Akademie HUSPOL

SCIENTIFIC PROGRESS: INNOVATIONS AND ACHIEVEMENTS

COLLECTION OF ABSTRACTS
International scientific-practical conference
(Kunovice, Czech Republic, June 29-30, 2023)

НАУКОВИЙ ПРОГРЕС: ІННОВАЦІЇ ТА ДОСЯГНЕННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ
Міжнародна науково-практична конференція
(Куновіце, Чеська Республіка, 29-30 червня 2023 року)

Kunovice 2023

Recommended for publication
by the Academic Council at
Akademie HUSPOL
June 30, 2023 (Protocol № 27)

Scientific progress: innovations ans achievements: collection of abstracts of International scientific-practical conference, Kunovice, Czech Republic, June 29-30, 2023. Kunovice : Akademie HUSPOL, 2023. 345 p.

Науковий прогрес: інновації та досягнення: зб. матеріалів Міжнар. наук.-практ. конф., м. Куновіце, Чеська Республіка 29-30 червня 2023 р. Куновіце : Академія ГУСПОЛ, 2023. 345 с.

ISBN 978-80-7314-412-8
ISBN 978-617-8094-11-9

The collection of abstracts contains the reports of participants of the International scientific-practical conference "Scientific progress: innovations and achievements", which was held by the Akademie HUSPOL (Czech Republic) with the assistance of the NGO "European Institute for Further Education" on June 29-30, 2023. The conference is dedicated to solving current problems in ensuring innovative development and finding ways to improve the legal practice of Ukraine and the Czech Republic.

Sborník abstraktů obsahuje zprávy účastníků Mezinárodní vědecko-praktické konference "Vědecký pokrok: inovace a úspěchy", kterou pořádala Akademie HUSPOL (Česká republika) za asistence nevládní organizace „Evropský institut postgraduálního vzdělávání“ 29-30.6.2023. Konference je věnována řešení aktuálních problémů při zajišťování inovativního rozvoje a hledání cest ke zlepšení právní praxe Ukrajiny a České republiky.

Збірник містить матеріали доповідей учасників Міжнародної науково-практичної конференції «Науковий прогрес: інновації та досягнення», яка була проведена Академією ГУСПОЛ (Чеська Республіка) за сприянням ГО «Європейський інститут післядипломної освіти» 29-30 червня 2023 року. Конференцію присвячено розв’язанню актуальних проблем в забезпеченні інноваційного розвитку та пошуку шляхів удосконалення правової практики України та Чехії.

ISBN 978-80-7314-412-8
ISBN 978-617-8094-11-9

©Akademie HUSPOL, 2023
© I. Kopotun, 2023
© S. Petkov, 2023

Mgr. Pavel Polián
Jednatel, statutární zástupce Akademie Huspol

Уважаемые коллеги!

Искренне поздравляю Вас с началом работы Международной научно-практической конференции!

Мне приятно, что организаторами конференции выступили Академия ГУСПОЛ и Общественная организация «Европейский институт последипломного образования», ведь мы выпускаем будущих юристов и повышаем квалификацию высококвалифицированных специалистов.

Сегодня в современном мире существует множество проблем, которые должны затрагивать мысли всех тех, кто имеет отношение к научным исследованиям. Реальные проблемы, которые возникают перед человечеством, куда более сложные, чем научные. Современная наука не в состоянии их кардинально решить. Важной причиной этому является разобщенность научных дисциплин. Элементарная синхронизация научных исследований дала бы действующий эффект.

Целью нашей конференции является именно разработка теоретических и практических аспектов обеспечения междисциплинарности научных исследований в контексте глобального развития и выделение конкретных мер обеспечения таких исследований на базе существующего международного опыта.

Вместе с Вами, дорогие коллеги, мы обоснуем основные теоретико-методологические подходы к развитию междисциплинарных научных исследований в условиях глобальных опасностей и угроз.

Учитывая то, что научная конференция является не только возможностью для обмена мыслями и апробирования своих теоретических наработок её участниками, но и прекрасным поводом для новых знакомств, надеюсь, что у Вас будет возможность для неформального общения с целью обмена опытом для решения в дальнейшем существующих проблем.

Радует то, что к работе на конференции откликнулись как отечественные, так и зарубежные ученые. Важно, чтоб научная дискуссия стала плодотворной для ученых, преподавателей, докторантов, аспирантов, магистров, а её результаты имели реальную общественно-политическую пользу.

Ігор Копотун
Доктор юридичних наук, професор, Заслужений юрист України,
Проректор з міжнародних зв'язків Akademie HUSPOL

Шановні колеги!

Сьогодні світ загалом переживає непрості часи. У сучасних умовах, наповнених суспільно значущими, а іноді й трагічними подіями, проведення Міжнародної науково-практичної конференції є знаковою подією міжнародного права, управління, філософії, педагогіки та інших дисциплін.

Міждисциплінарні дослідження стають сучасною науковою областю, що активно зростає. Як правило, під цим поняттям ховається вирішення наукових проблем шляхом інтеграції знань та методів із різних наукових галузей. Саме такі дослідження розглядаються як одна з можливостей для здійснення наукових проривів та розробки принципово нових способів вирішення найважливіших проблем сучасності.

Загальносвітовий досвід демонструє, що без тісної співпраці між вченими різних напрямів розвиток сучасної науки є практично неможливим. Дискусії та переговори з європейськими, вітчизняними та американськими колегами показують, що так звані «чисті науки» не мають жодних шансів отримати фінансування з боку наукових фондів тощо. Разом з традиційними небезпеками та загрозами – війнами, політичною нестабільністю, природними катаклізмами – з'явилися нові у вигляді поширення міжнародного тероризму та злочинності, пандемії коронавірусної інфекції COVID-19, значного погіршення екологічного стану довкілля людини, наркоманізації та алкоголізації населення багатьох країн, масштабних техногенних катастроф та аварій, зміни клімату на Землі, вичерпання природних ресурсів тощо.

Метою нашої конференції є пошук, а також аналіз можливих шляхів та нових підходів до вирішення глобальних та національних проблем в умовах сучасного світу шляхом міждисциплінарних досліджень.

Саме проведення нашої Міжнародної науково-практичної конференції, у якій взяли участь міжнародні представники академічної та вузівської науки, говорить про значний потенціал науки та освіти. Очевидно, що вирішення більшості важливих та складних питань можна досягти лише спільними зусиллями представників міжнародних наукових шкіл. Давайте разом прагнути досягнення нашої спільної мети.

Бажаю учасникам конференції активної та плідної роботи!

КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНЕ-ВИКОНАВЧЕ ПРАВО; КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

Mgr. Pavel Polián
Jednatel, statutární zástupce Akademie HUSPOL
Kunovice, Czech Republic

THE CHARACTERISTIC OF EXEMPTION FROM CRIMINAL LIABILITY FOR CORRUPTION CRIMES

Institutes of criminal law have come a long way of their historical formation. They did not occur simultaneously, but are the result of the adaptation of this branch of law to the conditions of a social situation that is constantly changing. It should be noted that the institute of exemption from criminal liability does not commit the decriminalization, but frees certain persons from liability for the crime, that they committed. Therefore, the exemption from criminal liability does not mean justification of a person or recognition of her innocent. Some grounds for exemption from criminal liability are not rehabilitated certain in the CC of Ukraine. The forms and types of positive behaviour are legally enshrined and in case of execution it by person in full, it should be a "incentive" reaction from the state as an exemption from criminal liability.

The analysis of modern criminal law and other legal, social and political processes in Ukraine gives grounds for the conclusion that the process of formation and development of criminal-law institutes passes one of its active phases.

The general ground for the exemption of a person who committed a crime from criminal liability for corruption crimes under the norms of the Special part of the CC of Ukraine is the inappropriate involvement of him in court liability and the enforcement of coercive measures of criminal-law influence to him. In resolving the issue of exemption from criminal liability, not only a criminal act and a number of legally significant circumstances related to its implementation, but also the characteristics of the guilty person and his conduct before or after the commission of the crime shall be assessed.

In the theory of criminal law, the following scientists paid much attention to studying the problem of exemption from criminal liability: Yu. V. Baulin, A. I. Boitsov, Ya. M. Brainin, K. K. Vavylov, B. Vittenberg, L. V. Golovko, T. T. Dubinin, S. Kelina, N. F. Kuznyetsova, S. N. Sabanin, V. V. Skibitskyi and others. Recently, some types of exemption from criminal liability at the level of the dissertation were investigated by M. Ye. Grigorieva, A. A. Zhitniy, P. V. Khryapinskyi and others.

The criminal-law institute is a normative decorated structural element of the criminal law field. The signs of this institution should be the considered idea-normative and appropriate to him social meaning. The second sign of the institute is the plurality of norms that make up it. The third sign of the criminal law institute is its focus on solving detailed intra-industry problems and external social tasks for the indicated sphere of policy.

Today one of the trends of criminal legislation can be called the rationing of cross-sectoral institutes. This is due to the fact that the individual elements of the criminal-law methods of management are "superimposed" on the subject of another branch of law or are the result of applying to the regulation of criminal law relations methods of other branches of law.

Despite the use of blanket dispositions in criminal law, in many cases we precisely can talk about inter-branch institutions. One of the most striking examples is the institute of criminal liability for corruption crimes. This institute can and should, in our opinion, be considered cross-sectoral. In V. M. Kyrychka's opinion, two groups of features are characteristic of corruption crimes: a) the composition of the crime provided for by the CC; b) the signs of a corruption offense are stipulated in art. 1 of the Law of Ukraine "On prevention of corruption" of October 14, 2014. Similarly is opinion of V. M. Kuts, who points out that a corruption crime is a socially dangerous act that contains signs of corruption and corruption offence, what is envisaged in the special part of the Criminal Code of Ukraine. I. Ye. Mezentseva defends the same position.

In addition, the cross-sectoral nature of the specified institute is due to the relationship with the criminal-procedural norms, which in many respects determine the direct practical implementation of special types of exemption from criminal liability for corruption crimes. The procedural ground for termination of a criminal prosecution is the execution of a guilty set of necessary and sufficient conditions (or the form and type of positive behaviour of the perpetrator, or the circumstance were preceding the commission of a crime) included in the construction of relevant norm of exemption. Taken together, they testify to the lack of expediency to lay the claiming all legal arising for the perpetrator from the criminal acts committed the official condemnation of a person and recognition him to be a criminal, his appointment of a punishment, the availability of criminal record. The procedural form of wrapping a similar ground is the decision of the authorized authority contained in the resolution (adopting) on the termination of criminal prosecution. The issue of exemption a person from criminal liability in special cases can be resolved both at pre-trial stages and in the order of preliminary hearing of materials of criminal proceedings and in court proceedings.

One of the most urgent reasons for application of the institute to exempt from criminal liability for corruption crimes is the subject's voluntary notification of a crime committed by him to the relevant official.

A number of articles of the CPC provides answers to questions about an authority whose servant is endowed with the right to report suspicion. In particular,

according to part 4 of art. 22 CPC the prosecutor reports to a person about suspicion of committing a criminal offense. In cases provided for by the CPC, a person may be informed of a suspicion of committing a criminal offense by an investigator in agreement with the prosecutor. Consequently, the authorities from whose official is entitled to report suspicion under the law are the Procuracy (article 11 (2), 36 of the CPC), Interior, Security, bodies supervising the observance of tax legislation, state investigation bureau, investigating officers of investigative units of performing preliminary inquiries and carrying out pre-trial investigation (art. 38 CPC), and authorized to notify the person, in agreement with the prosecutor, of suspicion (paragraph 6 of article 2, 40 of the CPC).

That is, the addressee of the voluntary notification should be the inquiry authority, investigator, prosecutor, judge or court (including special anti-corruption bodies such as the National Anti-Corruption Bureau of Ukraine, the Specialized Anti-Corruption Prosecutor's Office, etc.), and the content of the notification should include information about crime.

It should be clarified within what much time a person should report a crime committed by this person − given bribery of an employee of an enterprise, institution or organization − in order to be exempted from criminal liability. According to art. 214 of the CPC of Ukraine, the investigator, the prosecutor immediately, but not later than 24 hours after the submission of the application, the notification of a criminal offense committed or, after an self-identification of him from any source of circumstances that may indicate the commission of a criminal crime, is obliged to make the relevant information to the a single register of pre-trial investigations and initiate an investigation (part 1). Pre-trial investigation commences from the moment of entering information into the Unified Register of pre-trial investigations. The provisions about the Unified Register of Pre-trial Investigations, the procedure for its formation and maintenance are approved by the General Prosecutor's Office of Ukraine, with the consent of the Ministry of Internal Affairs of Ukraine, the SBU, the body, that supervising the compliance with tax legislation (part 2). The carrying out pre-trial investigation before the entering of information in the register or without such an entering is not allowed and entails the liability established by law (part 3).

Consequently, information about the crime should be made immediately, but not later than 24 hours, into the Unified Register of Pre-trial Investigations. This register is in accordance with the Regulation on the procedure for conducting the Uniform Register of Pre-trial Investigations, approved by the order of the General Prosecutor of Ukraine № 69 dated August 17, 2012 (with the changes approved by the orders of the General Prosecutor of Ukraine dated November 14, 2012, № 113, dd. 25.01.2013, № 13, dated 25.04.2013 № 54, 09.09.2014 № 95) and is created, in particular, with the purpose of providing a uniform record of criminal offenses.

In other words, only the data of this Register document the fact of the committed crime.

Consequently, the development of a dismissal institution, which is rooted in on the mechanisms of customary law, procedures and principles of complex social technology will, moreover, allow reduce the costs of prosecution for minor acts and minor crimes, which are necessary for the organization of the fight against serious corruption crimes, as well as to reduce extremely high overload of courts and investigation. In connection with this, it is proposed to provide for the following general conditions: the voluntary notification; an active assistance in the disclosure of crimes (including detection, prevention for and investigation); the first committing a corruption crime; the compensation for damages (if any). The specified conditions only in the complex form are the basis for exemption from criminal liability. Therefore, the release from criminal liability does not mean justification of a person or recognition of him innocent.

The article argues that the institute of exemption from criminal liability for corruption crimes refers to intersectoral. Such a classification determines the mechanism of application, which certainly is related to the norms of criminal-procedural and anti-corruption legislative acts.

The analysis of modern criminal law and other legal, social and political processes in Ukraine gives grounds for the conclusion that the process of formation and development of criminal-law institutes passes one of its active phases.

A detailed characteristic of the conditions for exemption from criminal liability for corruption crimes allowed focusing on the practical application of these norms by the judicial-investigative bodies. The voluntariness of notification of a corruption crime (stipulated by articles 354, 368-3, 368-4, 369, 369-2 of the CC of Ukraine) is a primary condition for the exemption of a person from criminal liability. This requires the establishment of the fact of voluntariness, with separating motives that play a minor role and may be different.

In determining active assistance for the disclosure of a corruption crime, a guilty person needs to commit actions that would confirm this fact. The actions can be different and objectively depend on the circumstances of the crime, for example, a notification about the place of storage of the subject of the crime (unlawful benefit) or about other participants who were involved in its commission, the finding of property and other values obtained in a criminal way.

For the saving of the forces and means of criminal justice, we recommend to set forth such explanations in the resolution of the Plenum of the Supreme Court of Ukraine to have the same understanding and application of a special exemption from criminal liability for corruption crimes.

It is useful to extend the possibility of applying a special exemption by establishment a single incentive norm in the CC of Ukraine, which would be extended to a more numerous group of corruption crimes.

References:

1. Lykhova S. Ya. Rozvytok kryminalno-pravovykh instytutiv v Ukraini na suchasnomu etapi. URL : http://conference.nau.edu.ua/index.php/TL/PRAVVYMIR/paper/ viewFile/1498/879

2. Kyrychko V. M. Kryminalna vidpovidalnist za koruptsiiu. Kharkiv : Pravo, 2013. S. 14.

3. Pro zapobihannia koruptsii : Zakon Ukrainy vid 14 zhovt. 2014. URL : http://zakon0.rada.gov.ua/ laws/show/1700-18

4. Kurs uholovnoho prava. Obshchaia chast. T. 2. Uchenye o nakazanyy : uchebnyk dlia vuzov / pod red. d-ra yuryd. nauk, prof. N. F. Kuznetsovoi y dr. Moskva : ZERTsALO, 1999. S. 35.

5. Mezentseva I. Vyznachennia predmeta koruptsiinykh zlochyniv. Visnyk Natsionalnoi akademii prokuratury Ukrainy. 2014. № 5. S. 76−81. URL : http://nbuv.gov.ua/UJRN/Vnapu_2014_5_13

6. Osadchyi V. I. Kryminalno-pravova kharakterystyka ta kvalifikatsiia pidkupu pratsivnyka pidpryiemstva, ustanovy chy orhanizatsii (st. 354 KK Ukrainy). Yurydychnyi visnyk. 2015. № 2 (35). S. 147.

7. Postanovlenye Plenuma Verkhovnoho Suda Rossyiskoi Federatsyy ot 9 yiulia 2013 h. № 24 "O sudebnoi praktyke po delam o vziatochnychestve y ob ynykh korruptsyonnykh prestuplenyiakh". URL : http://www. rg.ru/2013/07/17/verhovny-sud-dok.html

8. Sabanyn S. N. Nekotorye problemy zakonodatelnoi rehlamentatsyy spetsyalnykh vydov osvobozhdenyia ot uholovnoi otvetstvennosty. Yurydycheskaia nauka y pravookhranytelnaia praktyka. 2012. № 2. S. 59−66.

9. Ozhehov S. Y. Tolkovyi slovar russkoho yazyka. Moskva : [b. y.], 1995. S. 647.

10. Antonov A. H. Deiatelnoe raskaianye kak osnovanye osvobozhdenyia ot uholovnoi otvetstvennosty : avtoref. dys. … kand. yuryd. nauk / Antonov A. H. Tomsk, 2000. S. 17

Копотун І. М.

Доктор юридичних наук, професор, Заслужений юрист України,
Проректор з міжнародних зв'язків, Akademie HUSPOL,
м. Куновіце, Чеська Республіка

ОСОБЛИВОСТІ НАДЗВИЧАЙНИХ ПОДІЙ КРИМІНАЛЬНОГО ХАРАКТЕРУ У КРИМІНАЛЬНО-ВИКОНАВЧИХ УСТАНОВАХ

Варто зазначити, що надзвичайні події кримінального характеру у кримінально-виконавчих установах (втечі, захоплення заручників, масові заворушення, умисні вбивства) завжди були актуальною проблемою. Навіть сучасні системи ізоляції, охорони та нагляду за засудженими не можуть забезпечити виняткову безпеку у кримінально-виконавчих установах. Це, на нашу думку, пояснюється існуванням специфічних факторів, які пов'язані з діяльністю кримінально-виконавчих установ.

Справа в тому, що вивчення злочинної поведінки та її джерел здійснюється на трьох рівнях – загальному, особливому і одиничному. При вивченні походження злочинного на загальному (на рівні злочинності взагалі) і особливому рівнях (на рівні окремих видів, груп злочинів) у спеціальній літературі виділяють криміногенні фактори (детермінанти, обставини), а на рівні одиничного (на рівні конкретних злочинних діянь окремих людей) – причинно-наслідкові комплекси.

Вагомий внесок у наукове дослідження кримінально-правових, кримінологічних та кримінально-виконавчих засад надзвичайних подій кримінального характеру у кримінально-виконавчих установах зробили Г. А. Аванесов, Ю. М. Антонян, Ю. В. Баулін, О. М. Бандурка, В. Т. Білоус, І. Г. Богатирьов, В. В. Василевич, В. Б. Василець, В. В. Голіна, О. М. Джужа, В. М. Дрьомін, А. Ф. Зелінський, О. Г. Кальман, В. Є. Квашис, А. В. Кирилюк, О. Г. Колб, В. Я. Тацій, П. Л. Фріс, Ю. С. Шемшученко, В. І. Шакун та ін.

Метою статті є дослідження наукових засад визначення факторів, що обумовлюють виникнення у кримінально-виконавчих установах надзвичайних подій кримінального характеру.

Приступаючи до аналізу зазначених підходів, слід зазначити, що Г. Г. Зуйков у сукупності причин і умов, що сприяють вчиненню злочину, виділяє: а) безпосередню причину вчинення злочину; б) умови, що сприяли дії безпосередньої причини в конкретному злочинному посяганні; в) обставини, що сформували безпосередню причину і що є, таким чином, причинами безпосередньої причини [1, с. 3–18].

Однією з ключових проблем кримінології, що має важливе теоретичне і практичне значення, було і залишається вивчення причин злочинності як у цілому, так і окремих її видів. Без такого вчення було б безглуздим

дослідження не тільки даного явища, але і особи злочинця, проблем запобігання злочинності.

Теорія причинності у кримінології має методологічне значення і значною мірою визначає сенс і зміст правової природи злочинності, соціальної сутності особи злочинця, сприяє розробленню заходів запобігання вчиненню злочинів і вирішенню інших кримінологічних проблем. Причини та умови злочинності, як відомо, являють собою систему соціально-негативних явищ і процесів, що детермінують злочинність як свій наслідок. Причини злочинності визначаються реальними умовами життя людей, в основі яких – суперечності суспільства.

Раніше існувало механістичне уявлення про діючу і недіючу причини. Але тільки діюча причина в концепції діалектичного детермінізму і є причиною, хоча Г. В. Ф. Гегель зазначав, що причина є причиною остільки, оскільки вона породжує певну дію і якщо «причина згасає в своїй дії, так само згасає і дія, бо вона є лише виявленням причини» [2, с. 216].

Під впливом однакових причин існує велика кількість різних умов, що породжує неоднакову поведінку різних людей. Це ускладнює передбачення подальшої поведінки засуджених, які схильні до вчинення різного роду надзвичайних подій кримінального характеру у кримінально-виконавчих установах. У розрізі дослідження, це виявляється у тому, що існують різні форми злочинної діяльності, хоча причини можуть бути однаковими.

До характеристик причинності В. М. Кудрявцев відносить всезагальність, незворотність, просторову та часову безперервність. Причини та умови можна співвідносити таким чином: причина створює реальну можливість визначених наслідків, для настання яких необхідні ще певні умови. Самі по собі умови породжувати наслідки, призводити до них не можуть, але у відповідній ситуації сприяють реалізації дії причини.

Причини злочинності коріняться в соціальному ладі суспільства й обумовлені матеріальними й ідеологічними умовами життя людей. Людина не з’являється на цей світ із вродженими біологічними, расовими чи іншими ознаками злочинця, а стає ним через збіг несприятливих обставин, що, однак, не знімає з неї відповідальності за антигромадську поведінку. Слід враховувати особливості психології конкретної особи, які формуються й змінюються під впливом умов життя та виховання. Зміни структури та характеру злочинності залежать від різних соціальних умов, явищ і процесів (наприклад, від міграції й вікового складу населення, рівня освіти, культури й виховання людей, від економічної характеристики конкретних територій, від сформованих національних традицій, моралі, звичок, звичаїв) [3, с. 294].

При вивченні питання про виявлення причин і умов надзвичайних подій кримінального характеру у кримінально-виконавчих установах необхідно враховувати, що останнє складає основу перевірки заходів запобіжного впливу. Цілком справедливо у літературі підкреслюється, що причини злочинності виступають найвищим рівнем широкої системи джерел

антисоціальної поведінки. Відповідно до цього, процес запобіжного впливу має спрямовуватися на джерела і причини злочинності, причини і умови конкретних злочинів та фактори, що сприяють формуванню особистості.

Слід зазначити, що виявлення та вплив на причини і умови надзвичайних подій кримінального характеру – це складна система організаційних дій різних підрозділів і служб кримінально-виконавчих установах.

На початковому етапі дослідження причин і умов надзвичайних подій кримінального характеру у кримінально-виконавчих установах необхідно підкреслити, що істотне значення для з'ясування об'єктів запобіжного впливу має визначення і конкретизація самих понять причин злочинів і умов, що сприяють їх вчиненню. За наявності єдиної методологічної основи пояснення загальних причин злочинності, і, отже, успішного впливу на них необхідний більш предметний аналіз криміногенних факторів, які сприяють надзвичайним подіям кримінального характеру у кримінально-виконавчих установах, у певних регіонах, при певних обставинах і т. ін. Саме такий підхід, відповідно до якого групується сукупність злочинів за об'єктом посягання, дозволяє досягти найбільшої «відчутності» досліджуваних явищ, цілеспрямовано впливати на конкретні злочини та їх суб'єктів, вживати заходів, що перешкоджають самодетермінації злочинності.

Разом із тим, при аналізі причин і умов злочинності в цілому та надзвичайних подій кримінального характеру у кримінально-виконавчих установах зокрема, як об'єкта запобіжного впливу, ми з'ясували, що вони перебувають у тісному взаємозв'язку.

Насправді, деколи вельми складно установити причинно-наслідковий механізм і відокремити причини від умов як самостійні елементи цього механізму. Більш детальну конкретизацію об'єктів запобіжного впливу можна провести шляхом аналізу умов, що сприяють учиненню конкретних видів злочинів і причин їх вчинення. Тут варто враховувати, що однорідність злочинів веде до схожості об'єктів запобіжного впливу. Більше того, при аналізі причин і умов, що сприяють вчиненню конкретних видів злочинів, які належать до родового поняття «надзвичайні події кримінального характеру у кримінально-виконавчих установах», враховуються не тільки об'єктивні явища, але і суб'єктивна мотивація вчинення того або іншого злочину.

Отже, умови вчинення конкретних видів злочинів носять об'єктивний характер. І хоча вони самі по собі не викликають злочинну діяльність, проте здійснюють певний вплив на кількісні і якісні показники злочинності. Причини ж вчинення конкретного злочину (у нашому випадку – різні злочинні прояви надзвичайних подій кримінального характеру у кримінально-виконавчих установах) за своїм змістом носять суб'єктивний характер, виявляються через вольову поведінку людей. Це означає, що причини є внутрішньою силою, що виникає не тільки під впливом криміногенних факторів, але і з урахуванням індивідуальної свідомості

людини, її моралі, ставлення до існуючого порядку, норм співжиття. Вважаємо, що не менше значення мають і особистісні риси засудженого, який вчиняє конкретний злочин: рівень інтелектуального розвитку, психологічна стійкість, емоційність і т. ін.

Необхідність розмежовувати причини надзвичайних подій кримінального характеру у кримінально-виконавчих установах і умови, що сприяють цим злочинам, безперечна. Дослідження причин і умов надзвичайних подій кримінального характеру у кримінально-виконавчих установах розкриває природу цих злочинів, пояснює їх походження, показує, від чого вони залежать, що сприяє їх розповсюдженню. Тільки на основі подібних знань можна забезпечити ефективну боротьбу з цим видом пенітенціарних злочинів, передбачати можливі зміни, визначати і здійснювати необхідні заходи запобігання надзвичайним подіям кримінального характеру у кримінально-виконавчих установах.

Ми дотримуємося позиції кримінологів, які вважають, що різне розуміння детермінант злочинності веде до плутанини і виникнення у свідомості практичних працівників нігілізму до подібного роду суджень. Це викликає не завжди обґрунтовані судження, пов'язані з приниженням ролі науки кримінології і виконуваних нею відповідних функціональних суспільно важливих ролей [4, с. 54].

У зв'язку з викладеним вище, виявляється цілком обґрунтованим використання альтернативного терміну «фактор» [5, с. 109]. Саме тому у нашому дослідженні ми використовуємо поняття «фактори, що обумовлюють виникнення у кримінально-виконавчих установах надзвичайних подій кримінального характеру».

Список використаних джерел:

1. *Зуйков Г. Г. К вопросу о понятии причин преступления и условий, способствующих его совершению : Вопр. Предупреждения преступности, 1965. С. 3-18. Вып. 2.*
2. *Криминология. Словарь-справочник / сост. Х. Ю. Кернер; пер. с нем. В. Н. Кигас; отв. ред. пер. А. И. Долгова. : 4-е полн. перераб. изд. справочника Эгона Рессмана по криминологии для практикующих криминалистов. М.: Норма, 1998. 391 с.*
3. *Юридический энциклопедический словарь / ред.-упоряд. А. Я. Сухарев. М.: Норма, 1984. 294 с.*
4. *Кириллов С. И. Несовершеннолетние преступники: повторные грабежи и разбои. Учебное пособие. Коломна: Коломенский государственный педагогический институт, 1998.*
5. *Аванесов Г. А. Криминология и социальная профілактика. М.: Академия МВД СССР, 1980. 526 с.*

Агаркова О. І.

кандидат юридичних наук,
доцент кафедри поліцейської діяльності факультету
підготовки фахівців для підрозділів поліції
Луганського навчально-наукового інституту імені Е. О. Дідоренка
Донецького державного університету внутрішніх справ
м. Івано-Франківськ, Україна

ТАКТИКА ОГЛЯДУ МІСЦЯ ПОДІЇ ПІД ЧАС РОЗСЛІДУВАННЯ НЕЗАКОННОЇ ПОРУБКИ АБО НЕЗАКОННОГО ПЕРЕВЕЗЕННЯ, ЗБЕРІГАННЯ, ЗБУТУ ЛІСУ В УКРАЇНІ

Наразі забезпечення національної безпеки і оборони України, відсіч і стримування збройної агресії Російської Федерації, також вносить суттєві корективи до роботи лісової галузі нашої держави. Практично з перших днів війни виникли величезні потреби у деревині для оборонного сектору – облаштування фортифікаційних споруд, оборонних укріплень, дров для опалення та приготування їжі. Масова вирубка лісів, у тому числі незаконна, призводить до ерозії ґрунтів, виснаження річок, негативних змін клімату, що погіршує життя людей. У 2022 р. зареєстровано 4018 кримінальних правопорушень проти довкілля, з-поміж яких стабільним лідером за ключовими показниками є незаконна порубка лісу, а саме обліковано 2454 кримінальних правопорушень [1]. Тобто, одним із основних завдань держави є вдосконалення заходів щодо охорони лісового фонду, запобігання завдання йому шкоди та вчиненню правопорушень у сфері використання лісових ресурсів.

В умовах погіршення криміногенної ситуації, воєнного стану, докорінних змін кримінального процесуального законодавства та правозастосовної практики, науково обґрунтовані пропозиції науковців (С. О. Книженко, А. О. Новицький, В. О. Одерій, О. М. Пилипенко та ін.) потребують окремого дослідження особливостей проведення огляду під час розслідування незаконної порубки або незаконного перевезення, зберігання, збуту лісу.

Слідчий огляд при розслідуванні злочину, передбаченого ст. 246 КК України, є найбільш важливою й трудомісткою слідчою (розшуковою) дією.

Під час загального огляду, коли слідчий здійснює обхід території, де виявлено розкрадання лісодеревини, особлива увага приділяється забезпеченню збереження навколишньої обстановки, об’єктів та слідів, що знаходяться на місці кримінального правопорушення.

Коли межі огляду місця розкрадання лісодеревини встановлено, слідчому необхідно враховувати, що вони можуть розширюватись або

звужуватися залежно від встановлених обставин й отриманої інформації. Межі огляду повинні включати: територію, де вчинено кримінальне правопорушення або виявлені сліди, предмети, які в подальшому будуть визнані речовими доказами; ділянка місцевості, транспортні засоби, де злочинець перебував безпосередньо перед вчиненням кримінального правопорушення; інші ділянки місцевості, житла, дворові будівлі, склади, сховища, транспортні засоби, де можуть бути сліди і предмети, що мають відношення до розслідуваної події; імовірні шляхи підходу та відходу злочинців тощо.

У зв'язку з тим, що площа розкрадання лісодеревини є великою, то територію огляду доцільно поділити на невеликі сектори (що мають форму квадратів) та використовувати фронтальний спосіб огляду [4, с. 169].

Зважаючи на можливості сучасних техніко-криміналістичних засобів, вони застосовуються при проведенні огляду в ході розслідування розкрадання лісодеревини:

1). Під час виникнення труднощі, пов'язаних із прив'язкою до місцевості виявлених слідів – є доцільним запровадження в практику розслідування супутникових GPS/GLONASS-приймачів, що входять до системи глобальної супутникової навігації. За відсутності GPS-навігаторів слідчий повинен робити прив'язку до постійних орієнтирів: доріг, відгалуження річок або струмків з обов'язковим прив'язуванням до сторін світу, що має бути зафіксовано на схемі місця події та відображено у фототаблиці [3, с. 127] або кадастрового номеру земельної ділянки.

2). Під час загального огляду необхідно проводити фото- або відеофіксацію місця події без внесення змін до його обстановки, доцільно застосовувати фото- або відеозйомку з використанням квадрокоптера.

Особливістю техніко-криміналістичного забезпечення розслідування розкрадання лісодеревини є те, що під час проведення слідчих (розшукових) дій, зокрема під час огляду місця події, слідчий, прокурор не завжди може забезпечити повноту вилучення носіїв інформації, надати попередню оцінку інформативної значущості вилучених програмних і апаратних засобів, вжити заходів для максимального збереження інформаційних слідів. У таких випадках виникає потреба у спеціальному обладнанні, залученні відповідних профільних фахівців.

Під час детального огляду слідчий повинен спрямовувати свої дії на виявлення та вилучення наступних слідів кримінального правопорушення:

1). Слідів, що пов'язані з предметом посягання (пеньки, зрубані дерева (чагарники), а також їх частини). Саме це дасть змогу слідчому встановити об'єм порубки, її різновид, тривалість і періодичність, а також визначити кількість осіб, яких залучали до її проведення.

2). Слідів знарядь і засобів учинення злочину. Детальне дослідження слідів, що залишилися на предметі злочинного посягання, може з великою долею вірогідності вказати на знаряддя, якими було виконано відділення

стовбура дерева від кореня, його розкряжування та трелювання (сокирою, ручною пилою, електро- або бензопилою тощо).

3). Слідів взуття та транспортних засобів. Місцем виявлення слідів є оголений ґрунт: узбережжя рік та озер, дороги, стежки та інші місця, де за різних обставин (унаслідок руху транспортних засобів або трелювання деревини) було здерто шар лісової підстилки. Також сліди взуття злочинців і частки ґрунту можна виявити на килимках наявного на місці події автотранспорту. За виявленими слідами взуття слідчий має можливість установити дані щодо кількості залучених до незаконної порубки осіб, шляхів їхнього підходу та відходу, а також ідентифікувати конкретне взуття за залишеними ним слідами, що належить певним особам. Сліди транспортних засобів дають змогу встановити модель, напрям руху, ступінь навантаження, а також ідентифікувати конкретний транспортний засіб.

4). Біологічні сліди людини (кров, слина, піт, виділення з носа тощо), за допомогою яких слідчий отримує орієнтувальну інформацію щодо кількості осіб, які здійснювали порубку; наявність у злочинців ушкоджень, особливостей будови щелепи тощо, а за допомогою проведення відповідних експертиз може довести факт знаходження конкретних осіб на місці незаконної порубки лісу або їх безпосередню участь у її вчиненні.

Оглядаючи технічні засоби, знаряддя та пристосування незаконної порубки лісу, у протоколі огляду потрібно відобразити номери основних вузлів і агрегатів, зафіксувати, у якому стані перебувають ці засоби (увімкнені або вимкнені двигуни, чи придатні до роботи тощо).

Не менш важливим завданням під час проведення огляду є правильне вилучення виявлених та упакування слідів злочину та зразків, саме тому поряд із слідами правопорушення обов'язково необхідно відбирати та упаковувати зразки ґрунту, фрагменти деревини шляхом здійснення поперечних зрізів (спилів) тощо. Проведення вказаних дій краще доручити залученим спеціалістам.

Під час організації та проведення слідчих (розшукових) дій у кримінальних провадженнях щодо незаконної порубки, перевезення, зберігання, збуту лісу, необхідно враховувати надзвичайний правовий режим, який поширюється на територію де відбувається досудове розслідування. Тобто, проведення досудового розслідування в умовах воєнного стану має відповідну процедуру, визначену законодавством, і територію поширення. Це відповідно впливає на дію кримінального процесуального законодавства у просторі та часі.

Необхідно також зазначити, що виявлені під час огляду певні речі, які не вилучені законом з обігу (у нашому випадку незаконно добута деревина, автомобільна техніка, знаряддя і пристосування для незаконної порубки лісу тощо), вони автоматично набувають статусу «тимчасово вилучених» (ч. 2 ст. 168 КПК України). Відповідно до ч. 5 ст. 171 КПК України, на вилучене майно накладається арешт.

Отже, врахування таких особливостей проведення окремих слідчих (розшукових) дій і заходів забезпечення кримінального провадження під час розслідування, дозволить зібрати максимально повну інформацію про кримінальне правопорушення, передбачене ст. 246 КК України, надасть можливість оцінити зібрані докази в сукупності, уникнути неповноти досудового розслідування.

Список використаних джерел:

1. Карчевський М. В. Протидія злочинності в Україні: інфографіка. URL: https://ioyfgl-nikolay-karchevskiy.shinyapps.io/ukraine2022/_w_b03305a2/#tab-7463-1

2. Кримінальний процесуальний кодекс України: закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

3. Пилипенко О. М. Основи методики розслідування незаконної порубки лісу: дис. … канд. юрид. наук. Харків, 2018. 199 с.

4. Федорко Д. Є. Розслідування незаконної порубки або незаконного перевезення, зберігання, збуту лісу в Україні: дис. … канд. юрид. наук. Київ, 2022. 272 с.

Акімов М. О.

кандидат юридичних наук, доцент,
доцент кафедри кримінального права,
Національної академії внутрішніх справ

ЧИ ВДОСКОНАЛЕНА КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КАТУВАННЯ: АБО ДЕЯКІ ПРОБЛЕМИ ЗАКОНУ УКРАЇНИ ВІД 01 ГРУДНЯ 2022 РОКУ № 2812-IX

За шістнадцять місяців активної фази збройної агресії проти нашої держави прийняті та набули чинності двадцять законів про внесення змін та доповнень до Кримінального кодексу (далі – КК) України [1]. Відповідно до них у вітчизняному законодавстві про кримінальну відповідальність з'явилось вісім нових статей, ще двадцять дев'ять зазнали змін (причому деякі – неодноразово). Наскільки виправдана подібна динаміка – питання риторичне; у будь-якому разі прийняті новели викликають обґрунтовану зацікавленість щодо доцільності їх запровадження та можливості практичного застосування.

Закон України № 2812-IX «Про внесення змін до Кримінального кодексу України щодо кримінальної відповідальності за катування» [2], далі – Закон № 2812-IX, був прийнятий Верховною Радою 01 грудня, підписаний Президентом України 24 грудня та набув чинності 29 грудня 2022 року. Зауважимо, що відповідний законопроєкт (реєстр. № 5356) був поданий ще 05 квітня 2021 року та отримав при опрацюванні критичні зауваження як від апарату Верховної Ради України (Головного науково-експертного управління та Головного юридичного управління), так і від фахівців низки провідних вищих юридичних закладів освіти та науково-дослідних установ, до яких профільний парламентський комітет надіслав його на опрацювання.

Закон № 2812-IX має на меті, як стверджується у пояснювальній записці, приведення КК України у відповідність до положень Конвенції ООН проти катувань та інших жорстоких, нелюдських чи таких, що принижують гідність видів поводження та покарання від 10 грудня 1984 року [3], далі – Конвенція.

З цією метою статтю 127 КК України викладено у новій редакції. Зокрема, по-іншому сформульовано таку кваліфікуючу ознаку катування як вчинення його з мотивів расової, національної чи релігійної нетерпимості (відтепер воно є різновидом катування з метою дискримінації). Попередня редакція статті, що розглядається, дійсно передбачала мету дискримінації як обов'язкову ознаку простого складу цього кримінального правопорушення (частина перша статті 127 КК України), а мотив расової, національної чи релігійної нетерпимості – як кваліфікуючу ознаку (частина друга статті 127

КК України). Подібне рішення законодавця виглядає вельми сумнівним, адже одне посягання на рівноправність не повинно бути більш небезпечним за інше, інакше це означатиме неоднаковий кримінально-правовий захист рівноправності.

Заслуговує на схвалення і заміна передбаченого Конвенцією терміну «визнання» на «зізнання» при характеристиці мети примушування при катуванні, позаяк значення цих термінів істотно відрізняється, що впливає на сутність того, на що саме спрямоване примушування при катуванні.

Водночас аналіз інших положень Закону 2812-IX свідчить про їх дискусійний, а іноді суперечливий характер. Так, змінами, внесеними до частини п'ятої статті 49 та частини шостої статті 80 КК України, передбачається незастосування звільнення від кримінальної відповідальності у зв'язку із закінченням строків давності та звільнення від відбування покарання у зв'язку із закінченням строків давності виконання обвинувального вироку до кримінального правопорушення, передбаченого частиною третьою статті 127 КК України (тобто до вчинення катування представником держави, в тому числі іноземної). Стверджується, що це буцімто відповідає частині другій статті 4 Конвенції, а також Загальній Декларації прав людини, Конвенції про захист прав людини і основоположних свобод та Конституції України.

Проте поза увагою залишилось те, що вчинення катування представниками держави, в тому числі іноземної, може відбуватись (як-от наразі) під час збройного конфлікту (чи у зв'язку із збройним конфліктом). За таких умов катування, вчинене зазначеними особами, є порушенням законів та звичаїв війни і повинно бути кваліфіковане за частиною першою статтею 438 КК України. Пропозиція ж давати кримінально-правову оцінку вчиненому із застосуванням статті 127 КК України призведе, на нашу думку, лише до штучної конкуренції кримінально-правових норм, а відтак є неприйнятною. До того ж при прийнятті Закону 2812-IX жодним чином не була роз'яснена потреба прирівняти катування (причому лише його особливо кваліфікований склад) до злочинів проти основ національної безпеки України, передбачених у статтях 109–114-1, та злочинів проти миру та безпеки людства, передбачених у статтях 437–439 і частині першій статті 442 КК України.

Далі, у нинішній редакції статті 127 КК України склад катування сформульований як усічений («будь-яке умисне діяння, спрямоване на заподіяння особі сильного фізичного болю чи морального страждання, вчинене з метою примусити її чи іншу особу вчинити дії, що суперечать їх волі, у тому числі отримати інформацію чи зізнання, або з метою покарати її чи іншу особу за дії, вчинені нею або іншою особою чи у вчиненні яких вона або інша особа підозрюється, або з метою залякування її або інших осіб») замість формального («умисне заподіяння сильного фізичного болю

або фізичного чи морального страждання шляхом нанесення побоїв, мучення або інших насильницьких дій з метою примусити потерпілого чи іншу особу вчинити дії, що суперечать їх волі, у тому числі отримати від нього або іншої особи відомості чи визнання, або з метою покарати його чи іншу особу за дії, скоєні ним або іншою особою чи у скоєнні яких він або інша особа підозрюється, а також з метою залякування чи дискримінації його або інших осіб») у попередній редакції. Але нова редакція не відповідає меті прийняття Закону 2812-IX. Згідно частини першої статті 1 Конвенції «катування» означає «будь-яку дію, якою будь-якій особі навмисне заподіюються сильний біль або страждання, фізичне чи моральне, щоб отримати від неї або від третьої особи відомості чи визнання, покарати її за дії, які вчинила вона або третя особа чи у вчиненні яких вона підозрюється, а також залякати чи примусити її або третю особу, чи з будь-якої причини, що ґрунтується на дискримінації будь-якого виду, коли такий біль або страждання заподіюються державними посадовими особами чи іншими особами, які виступають як офіційні, чи з їх підбурювання, чи з їх відома, чи за їх мовчазної згоди».

Нарешті, якщо суб'єкт за частиною третьою статті 127 КК України – спеціальний (представник держави, в тому числі іноземної), незрозуміло:

- як під «представником держави» можна розуміти «групу осіб»;
- чому поняття «представники іноземної держави» сформульовано у множині (і яку кримінально-правову оцінку слід давати діянню у разі вчинення його одним представником іноземної держави);
- як саме прагнення привести положення цієї статті у відповідність із Конвенцією узгоджується з іншими положеннями вітчизняного законодавства про кримінальну відповідальність (а саме із нормами інституту співучасті) в частині визначення особи або групи осіб, які діють з підбурювання, з відома чи мовчазної згоди держави, як суб'єкта (суб'єктів) даного посягання (у тому числі тоді, коли йдеться про іноземну державу);
- яким чином передбачається виконувати передбачене цією частиною статті, що розглядається, додаткове покарання у виді позбавлення права обіймати певні посади або займатися певною діяльністю щодо представників іноземної держави.

Підбиваючи підсумки, зазначимо, що наведених вище недоліків цілком достатньо, аби істотно ускладнити правозастосування. Відтак залишається сподіватись на те, що українському законодавцю вистачить часу та здорового глузду, аби їх виправити.

Список використаних джерел:

1. Кримінальний кодекс України : Закон України від 05 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 22.04.2023).

2. Про внесення змін до Кримінального кодексу України щодо кримінальної відповідальності за катування : Закон України від 01 грудня 2022 року № 2812-IX. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/26194 (дата звернення 22.04.2023).

3. Конвенція про проти катувань та інших жорстоких, нелюдських чи таких, що принижують гідність видів поводження та покарання: прийнята 10 грудня 1984 року, набула чинності для України 24 лютого 1987 року. URL: https://zakon.rada.gov.ua/laws/show/995_085#Text (дата звернення: 22.04.2023).

Рудик М. М.

кандидат юридичних наук,
викладач кафедри поліцейського права
Національної академії внутрішніх справ, м. Київ

МЕХАНІЗМ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ КРИМІНОЛОГІЧНОЇ ПОЛІТИКИ У СФЕРІ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ ТА ЕКСПЛУАТАЦІЇ АВТОМОБІЛЬНОГО ТРАНСПОРТУ

На сьогодні правові засади забезпечення БДР та експлуатації автомобільного транспорту становлять значний масив нормативно-правових актів різної ієрархічної належності, починаючи від міжнародних договорів і закінчуючи національними підзаконними документами вищих та центральних органів влади. У цьому контексті ситуацію в означеній сфері можна визначити як позитивну, адже робота суб'єктів забезпечення безпеки на автомобільному транспорті не тільки вичерпно регламентована, а й постійно вдосконалюється відповідно до перспективних напрямів розвитку, що виражається в стратегічно спрямованих нормах різних концепцій, програм та інших аналогічних актів. Водночас, на сьогоднішній день в Україні увесь такий масив нормативно-правових актів, на жаль, не відображає основні принципи та засади актів права ООН та ЄС, а саме, те, що громадянин і його безпека має стати центром державної політики України у сфері БДР. Міжнародний досвід свідчить, що основою системи БДР розвинених країн є *національні концепції безпеки руху*, що забезпечують системний підхід до вирішення проблем указаної сфери. Використання наявного та практично перевіреного досвіду інших країн для України є найбільш ефективним, швидким та маловитратним шляхом розв'язання проблеми, особливо в умовах сьогоднішньої економічної кризи. У повній мірі такий підхід стосується як реалізації конкретних практичних заходів, так і вироблення принципів та побудови національної системи забезпечення БДР. Основою такої системи має бути принцип спільної відповідальності всіх складових суспільства.

Виходячи з цього, вважаємо доречним схвалити *Стратегію забезпечення безпеки дорожнього руху та експлуатації транспорту на період до 2030 року*, в якій виділити такі напрями державної політики у сфері БДР та експлуатації автомобільного транспорту:

– розвиток та вдосконалення вітчизняного законодавства про безпеку дорожнього руху. Як відомо, від якості нормативно-правових актів напряму залежить ефективність організації правовідносин, забезпечення законності та правопорядку, динамічний розвиток відповідних галузей і сфер соціального життя, авторитет органів державної влади. На жаль, сучасний стан

нормативно-правової регламентації суспільних відносин у сфері дорожнього руху (зокрема, в частині забезпечення його безпеки) не дає підстав розраховувати на позитивний соціально-економічний результат. Відсутність «стрижневого» закону з питань БДР; розпорошеність кореспондуючих норм по величезному масиву галузевих нормативно-правових актів; фрагментарність правового регулювання; застарілість та неузгодженість нормативного матеріалу; логіко-юридичні погрішності змісту законодавчих положень; безсистемність нормотворення – ці та інші проблеми, з одного боку, змушують констатувати недосконалість нормативно-правової бази, а з іншого – дозволяють убачати в окресленому напрямі державної політики стратегічний ресурс для оптимізації правовідносин та покращення основних показників БДР;

– модернізація системи управління БДР. За загальним визнанням, вітчизняна система забезпечення БДР перебуває в надзвичайно розбалансованому стані, що вкрай негативно позначається на її ефективності [29]. Практично відсутня координація управлінської діяльності на міжгалузевому та міжрегіональному рівнях. Центральні органи виконавчої влади у сфері БДР провадять «свою» відомчу політику, всіляко відхрещуючись від відповідальності за загальний стан справ. Місцеві державні адміністрації та органи самоврядування часто-густо не можуть дійти згоди щодо розподілу сфер адміністративного впливу (причому, зазвичай, має місце не перетягування повноважень, а, навпаки – їх взаємне перекладання). Функції щодо управління безпекою дорожнього руху та контроль за здійсненням відповідного напряму управлінської діяльності виконує по суті один і той самий орган – Міністерство внутрішніх справ України (думається, питання про відомчу «ангажованість» цього контролю є риторичним). Тому, для забезпечення сучасного рівня БДР в Україні пропонується, в першу чергу, створити окреме управління (як це вже зроблено в багатьох країна Європи), наприклад, національне управління (агенція) БДР, яке буде координувати міжгалузеві співвідношення у цій сфері. Тому що без єдиного координаційного управління та належного закону до нього, не можливо якісно і ефективно захищати громадян від небезпеки на дорогах країни. Регулювання з боку правової системи слід вважати найважливішим компонентом державного управління у сфері забезпечення БДР [30];

– поліпшення технічного стану, експлуатаційних характеристик та пропускної спроможності автомобільних доріг. Невпинне збільшення кількості транспортних засобів та критична зношеність дорожньої інфраструктури з особливою гостротою ставлять питання про активізацію будівництва, ремонту й реконструкції автомобільних доріг. На жаль, сьогодні це питання вирішується дуже повільно. За останні дев’ять років протяжність доріг загального користування збільшилась лише на 10 кілометрів (тобто на 0,005%), тоді як автопарк країни зріс щонайменше вдвічі. Переважна

більшість вітчизняних доріг не відповідають технічним правилам, нормам і стандартам. З огляду на хронічне бюджетне недофінансування, темпи реконструкції вулично-дорожньої мережі впали майже до мінімуму [31]. Величезну проблему становить брак технічних засобів організації руху. Загалом на українських дорогах «не вистачає» близько 70 тис. дорожніх знаків. У деяких містах працюють менше половини світлофорів. Далекими від оптимальних параметрів залишаються обсяги покриття та якість дорожньої розмітки;

– забезпечення високої якості підготовки водіїв. У соціотехнологічній макроструктурі «водій – транспортний засіб – дорога» найменш надійною ланкою є водій. За інформацією Департаменту патрульної поліції України, водії механічних транспортних засобів вчиняють 3,5 млн. порушень правил дорожнього руху на рік. З їх вини трапляються 65-75% усіх ДТП [32];

– підвищення дорожньо-транспортної культури населення. Величезна кількість правопорушень на автомобільному транспорті пояснюється не лише браком водійської майстерності, а й тотальним нігілізмом в питаннях дисципліни руху, вирішення спірних дорожніх ситуацій, соціальних стандартів поведінки водіїв і пішоходів. Як показують останні соціологічні дослідження, третина вітчизняних водіїв не співвідносять власні дії з інтересами інших учасників дорожнього руху, в усьому керуючись особистісними та егоїстичними міркуваннями. Кожний четвертий водій вважає нинішній рівень порядку й дисципліни на дорогах незадовільним. Причому визнання цього факту зовсім не свідчить про шанобливе ставлення до правил дорожнього руху: практично всі респонденти допускають можливість їх порушення за певних «сприятливих» умов (як-то: неконтрольованість дорожньої ділянки, відсутність поблизу транспортних засобів тощо). Що ж стосується пішоходів, то лише чверть з них при перетинанні проїзної частини послуговуються сигналами світлофора. Приблизно стільки ж – взагалі переходять дорогу не там, де це дозволено, а там, де їм зручно. Результат подібної легковажності закономірний: протягом 2016–2022 років в Україні зафіксовано 223743 ДТП за участю пішоходів;

– підвищення надійності та безпечності транспортних засобів. Аналіз причин аварійності на автомобільному транспорті дозволяє констатувати відсутність тенденції щодо збільшення кількості ДТП, обумовлених незадовільним технічним станом рухомого складу. Через несправності транспортних засобів трапляються близько 1 тис. аварій на рік, тобто 2,5-3% всіх ДТП. За світовими мірками це далеко не критичний показник. Але він повністю нівелюється надвисоким рівнем смертності й травматизму: на кожні 100 ДТП, спричинених технічними несправностями автомобілів (мотоциклів, автобусів), припадають 25 загиблих і 100 поранених осіб. Загрозлива віктимологічна ситуація вимагає від держави вжиття комплексу невідкладних заходів, спрямованих на: підвищення вимог до конструкції транспортних засобів у частині забезпечення їх пасивної та активної безпеки;

удосконалення контролю за технічним станом засобів пересування; посилення відповідальності за керування транспортними засобами із серйозними несправностями (дефектами рульового управління, гальмівної системи, тягово-зчіпного механізму автопоїзда тощо) [33];

– удосконалення медичного забезпечення БДР. Істотний вплив на стан аварійності та тяжкість наслідків ДТП здійснює система медичного забезпечення. Від того, наскільки добре ця система організована, наскільки злагоджено функціонують її компоненти, наскільки повно вона відповідає об'єктивним соціально-економічним і дорожньо-транспортним умовам, залежать такі показники БДР, як загальна кількість автомобільних аварій, обсяг спричинених ними матеріальних збитків, питома вага загиблих і поранених внаслідок ДТП.

Ось лише декілька показових викладок статистики: незадовільний психофізіологічний стан водія є причиною 9-12% ДТП, в яких щороку гинуть до 1 тис. чоловік; через несвоєчасне або неналежне надання медичної допомоги передчасно йдуть з життя 13% постраждалих у ДТП; надання першої допомоги протягом 9 хвилин після аварії дозволяє врятувати 90% важкопоранених, після 18 хвилин – шанси на порятунок зменшуються в 6 разів (до 15%); 91% жертв ДТП доправляються в медичні заклади попутним транспортом, при цьому ймовірність летального випадку становить 86,2% (при транспортуванні штатним автомобілем швидкої допомоги відповідний показник дорівнює 66,3%, бригадою реанімації – 17,4%).

Список використаних джерел:

1. *Національна транспортна стратегія України на період до 2030 року : розпорядження Кабінету Міністрів України від 30 трав. 2018 р. № 430-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/430-2018-%D1%80#Text*
2. *Голина В. В. Кримінологічна політика в Україні: деякі теоретико-прикладні проблеми. Вісн. Акад. прав. наук України. 2008. № 2. С. 182–190; Голина В. В. Кримінологічна політика України. Правова доктрина України: учебник. У 5 т. / В. Я. Тацій, В. І. Борисов, В. С. Батиргареєва та ін.; за заг. ред. В. Я. Тація, В. І. Борисова. Т. 5: Кримінально-правові науки в Україні: стан, проблеми та шляхи розвитку. Харків: Право, 2013. 640 с.*
3. *Голина В. В. Кримінологічна політика України як ресурс у протидії злочинності (реалії і можливості). Вісник Нац. акад. правових наук України. 2013. № 2 (73). С. 193–201; Василевич В. В. Поняття кримінологічної політики. Науковий вісник Ужгородського національного університету. Серія Право. 2013. Спецвипуск. Т. 2. С. 120–125.*
4. *Кузнецов А. П. Проблема определения смежных понятий в уголовной и криминологической науке. Законодательная дефиниция: логико-гносеологические, политико-юридические, морально- психологические и практические проблемы: материалы междунар. кругл. стола (Черновцы, 21–23 сент. 2006 г.) / под ред. В. М. Баранова, П. С. Пацуркивского. Нижний Новгород, 2007. С. 1125–1127. С. 1125.*
5. *Голіна В. В. Запобігання злочинності (теорія і практика): навч. посіб. Харків: Нац. юрид. акад. України, 2011. 120 с. С. 8.*
6. *Даньшин І. М., Зелінський А. Ф. Кримінальна політика: за і протии. Право України. 1992. № 8. С. 29–36. С. 34.*

Моісеєв М. Г.

аспірант заочної форми навчання відділу
докторантури та ад'юнктури
кафедри кримінального процесу
Національної академії внутрішніх справ

ЗАГАЛЬНІ АСПЕКТИ ОСОБИ ЗЛОЧИНЦЯ ПРИ НЕЗАКОННОМУ ВТРУЧАННІ В РОБОТУ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ І УСТАНОВАХ СИСТЕМИ ПРАВОСУДДЯ

На сьогодні все більш важливим напрямком науки криміналістики є вивчення осіб, які вчинили кримінальне правопорушення, в данному випадку нас цікавить саме незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, яке передбачено статтею 376-1 Кримінального кодексу України, оскільки розслідування такого діяння є ускладненим, враховуючи способи, знаряддя та предмет вчинення такого незаконного втручання.

Враховуючи специфіку саме способів незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, окремі аспекти такого кримінального правопорушення можна віднести і до службового кримінального правопорушення, і до кримінального правопорушення у сфері правосуддя, і до комп'ютерного кримінального правопорушення.

Категорія «особа злочинця» поєднує в собі соціологічне поняття «особа» та юридичне – «злочинець». Криміналістична характеристика особистості злочинця - це криміналістично значуща інформація про злочинця, його анатомічні, біологічні, психологічні та соціальні особливості. Тобто це сукупність відомостей щодо фізичних, соціальних, морально-психологічних та інших ознак та властивостей, характерних для осіб, що вчинили кримінальне правопорушення певного виду. Ця інформація насамперед потрібна для ідентифікації особистості, вирішення тактичних завдань та встановлення фактичної картини події кримінального правопорушнння у процесі його розкриття та розслідування.

Основним завданням криміналістичного встановлення особи злочинця є використання інформації для розробки тактики слідства. Саме знання типових рис особистості злочинця дозволяє оптимізувати процес розслідування кримінальних правопорушень.

Досить широку структура особи злочинця виокремлюють такі автори як Сергєєва Д. Б., Ткач О. В. виділяючи п'ять підструктур, що містять певні ознаки:

1) ознаки, які безпосередньо характеризують суспільну небезпеку особи злочинця (характер вчиненого кримінального правопорушення, його тяжкість і злочинні наслідки; форма вини, мотив і мета кримінального правопорушення; спосіб вчинення кримінального правопорушення; привід і ситуація вчинення кримінального правопорушення; вчинення кримінального правопорушення вперше, повторно, систематично або рецидивістом; наявність або відсутність інших правопорушень та інших антигромадських вчинків; інші обтяжуючі абопом'якшуючі відповідальність обставини; ставлення злочинця до вчиненного кримінального правопорушення; поведінку під час відбування покарання);

2) ознаки, що розкривають соціальні (й антисоціальні) відносини особи в різних сферах суспільного життя (загально-громадянські відносини; трудові відносини; участь в різних формах навчання і його результати; сімейні відносини; побутові відносини з найближчим безпосереднім оточенням; участь в громадських організаціях; зв'язку з злочинними та іншими антигромадськими елементами);

3) ознаки, що дають морально-психологічну характеристику особи (спрямованість особи; світогляд особи; інтереси особи; стійка система мотивів поведінки; моральні принципи, цінності та норми, якими особа практично керується в своїй діяльності; моральні навички і звички особи; характер і рівень потреб особи);

4) ознаки, що характеризують психологічний стан особи та її психічні особливості (особливості відчуттів, сприйняття, пам'яті; особливості протікання інтелектуальних, вольових і емоційних процесів й відповідні властивості особистості; темперамент; здатності; наявність або відсутність психічних аномалій; вікові особливості психіки);

5) ознаки, що характеризують фізичні (біологічні) властивості особи (стать; вік; особливості фізичної конституції; фізіологічні особливості, стан здоров'я; інстинкти, потяги, фізіологічні потреби) [1, с. 110].

Незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, що передбачене статтею 376-1 Кримінального кодексу України [2] відноситься до корисливих кримінальних правопорушень, та може мати як загального суб'єкта кримінального правопорушення (наприклад при зламувані паролів чи несанкціонованого входу до Єдиної судової інформаційно-телекомунікаційної системи, іншої автоматизованої системи, що функціонує в суді, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів, Державній судовій адміністрації України, їх органах, несанкціоновані дії з інформацією, що міститься в таких системах, чи інше несанкціонованого втручання в роботу таких систем), так і спеціального суб'єкта, що має доступ входу до Єдиної судової інформаційно-телекомунікаційної системи, іншої автоматизованої системи, що функціонує в суді, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів, Державній судовій

адміністрації України, їх органах, несанкціоновані дії з інформацією, що міститься в таких системах.

До спеціальних належать службові особи, які мають право доступу до автоматизованої системи документообігу суду (суддя або працівник апарату суду згідно з їх функціональними обов'язками). Названі особи одержують право доступу до автоматизованої системи документообігу суду на підставі наказу голови відповідного суду. До загальних суб'єктів належать будь-які інші фізичні осудні особи, що досягли 16-річного віку та вчинили це кримінальне правопорушення шляхом несанкціонованого доступу до автоматизованої системи документообігу суду.

Тобто особа злочинця тут охоплює широкий спектр, оскільки це може бути як службова особа, так і звичайний громадянин.

Так, наприклад Мірошниченко С. С. найчастіше кримінальні правопорушення проти правосуддя вчиняються особами чоловічої статі, віком старше 29 років, та особами із середньою, середньо-спеціальною та вищою освітою [3, с. 415].

Даючи соціально-психологічну характеристику осіб, які вчинили кримінальне правопорушення проти правосуддя, варто погодитися з думкою Ахмедова В.А., що для них притаманне викривлене відчуття незалежності від нормативної системи, правовий нігілізм, орієнтація на задоволення своїх власних потреб та інтересів будь-якими засобами, чітке усвідомлення протиправності своїх діянь [4, с. 116].

Якщо говорити саме про спеціальних суб'єктів, то відповідно це особи, що мають доступ до відповідної системи, тому вчиняти даний вид кримінального правопорушення у системі правосуддя (як особа, яка уособлює представника системи правосуддя) може особа віком 30-65 років, яка має досить високий інтелектуальний і освітній рівень. Водночас національність, стать, соціальне походження, місце народження і проживання не мають значення.

Саме високі вимоги щодо освіти й інтелектуального рівня суддів, секретаря суду, керівника апарату суду тощо призводять до складності виявлення і запобігання проявам таких кримінальних прапорушень в системі правосуддя, тому що такі особи здатні дуже майстерно приховувати (маскувати) свою злочинну діяльність. Водночас такі особи мають високий рівень освіти (вища юридична освіта), інтелекту та культури, а перебування на відповідних посадах вимагає не лише такого рівня знань, а й постійного його вдосконалення, досить часто їх називають «білокомірцевими злочинцями» [5, с. 69].

У підсумку відзначимо, що за великим рахунком корислива мета є обов'язковою ознакою суб'єктивної сторони зазначених кримінальних правопорушень. Винний усвідомлює, що незаконно втручається у справи правосуддя на свою користь чи на користь інших осіб з метою отримання певної вигоди. Загалом можна визначити, що суб'єкт кримінальних

правопорушень проти правосуддя – це самовпевнений, корисливий, який прагне отримання влади, ігровий тип людини, не боящийся ризику.

Список використаних джерел:

1. Сергєєва Д. Б., Ткач О. В. Особа злочинця як елемент криміналістичної характеристики порушень недоторканності приватного життя». Вісник кримінальної юстиції No 1. 2018. С. 106-114.

2. Кримінальний кодекс України від 05 квітня 2001 року № 2341-III. Відомості Верховної Ради України. 2001. № 25. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 24.05.2023)

3. Мірошниченко С. С. Кримінологічна характеристика осіб, які вчинили злочини проти правосуддя». Науковий вісник Львівського державного університету внутрішніх справ. № 3. 2012. С. 412-422.

4. Ахмедов В. А. Роль особистості злочинця в системі факторів, що зумовлюють вчинення кримінальних правопорушень проти правосуддя». Судова апеляція № 2 (55). 2019. С. 114-121.

5. Мезенцева І. Кримінологічна характеристика особи корупційного злочинця. Науковий часопис Національної академії прокуратури України. № 3. 2014. С. 65–71.

ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА; ІСТОРІЯ ПОЛІТИЧНИХ І ПРАВОВИХ УЧЕНЬ; ДЕРЖАВНЕ УПРАВЛІННЯ; ПОЛІТОЛОГІЯ; ФІЛОСОФІЯ ПРАВА

Дорошенко Т. В.

Кандидат педагогічних наук, доцент,
науковий співробітник
Національної академії Служби безпеки України

ВПЛИВ ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ НА СУЧАСНІ КОНФЛІКТИ

У сучасному взаємопов’язаному світі інформаційно-психологічні операції стали потужним інструментом, який формує і впливає на сучасні конфлікти. У світлі зазначеної проблематики важливим аспектом стає необхідність розуміння сутності вказаних операцій та їхній глибокий вплив на перебіг сучасних глобальних і локальних кризових проявів. Вивчаючи використання основних механізмів, стратегій та наслідків, можливо виявити, як інформаційні та психологічні операції трансформували природу конфліктів і методи, що застосовуються суб’єктами реалізації інформаційно-психологічних операцій. Аналіз існуючих конфліктів підкреслює критичну важливість визначення і вирішення проблем, пов’язаних з відповідними операціями, для забезпечення стабільності та безпеки в умовах еволюції глобальних загроз.

Сучасні конфлікти підкреслюють зміну парадигми, коли інформаційно-психологічні операції стали ключовими компонентами стратегічного планування і виконання окремих дій у зазначених конфліктах. Виходячи з нагальних потреб реалізації відповідної державної внутрішньої та зовнішньої політики, важливим є дослідження впливу інформаційно-психологічних операцій на сучасні конфлікти та з’ясування їх ролі у формуванні сприйняття, маніпулюванні наративами та впливі на результати, різні інструменти і методи, що застосовуються, а також виклики і наслідки, пов'язані з такими операціями.

Інформаційні операції охоплюють широкий спектр діяльності, спрямованої на збір, аналіз, оброблення та поширення інформації з метою отримання конкурентної переваги у сучасному конфлікті [1]. Сюди може входити проведення кібервійні, пропаганди, дезінформаційні кампанії та використання платформ соціальних мереж. Доступність цифрового ландшафту підвищила ефективність і масштаби цих операцій, дозволивши державним і недержавним суб’єктам впливати на цільові аудиторії по всьому

світу. Противник використовує витончені методи для пошуку вразливостей в інформаційних системах і мережах.

Психологічні операції передбачають здійснення впливу на думки, емоції та поведінку окремих осіб, груп або суспільств. Зазначені операції використовують когнітивні упередження, емоційні тригери і соціальну динаміку для формування сприйняття та пригнічення морального духу противника. Психологічними операціями, під час яких поширюються спеціальні повідомлення, які створюють плутанину, здійснюється вплив на прийняття рішень цільовими групами населення. Психологічні операції можуть застосовуватися через різні канали, включаючи традиційні ЗМІ, соціальні мережі та міжособистісне спілкування.

Інформаційні та психологічні операції часто працюють у синергії, використовуючи сильні сторони одна одної для досягнення максимального ефекту. Поєднуючи дезінформаційні кампанії з психологічними маніпуляціями, противник може використовувати існуючі лінії розколу в суспільстві, загострювати напруженість і сіяти розбрат. Більше того, використання новітніх технологій (фейкові відео, контент, створений штучним інтелектом) ще більше розмиває межу між реальністю та неправдою, підвищуючи ефективність цих операцій. Безперешкодна інтеграція інформаційних і психологічних операцій створює значні виклики для стратегій оборони та безпеки.

Успішні інформаційно-психологічні операції вимагають ретельного планування та виконання. Для досягнення своїх цілей супротивники використовують такі стратегії, як «розділяй і володарюй», «фабрикація наративів». Вказані стратегії спрямовані на використання існуючих невдоволень, маніпулювання громадською думкою та підрив довіри до інституцій, що послаблює стійкість суспільства та сприяє нестабільності. Противники також використовують такі методи, як соціальна інженерія, управління сприйняттям і проникнення в мережі, щоб отримати доступ до конфіденційної інформації та маніпулювати процесами прийняття рішень.

Вплив інформаційно-психологічних операцій на сучасні конфлікти не можна недооцінювати [2]. Їх здатність створювати плутанину, поляризувати суспільство та маніпулювати громадськими настроями створює значні виклики для безпеки і стабільності. Вибори, соціальні рухи і геополітична динаміка – все це піддається маніпуляціям, змінюючи таким чином хід конфліктів і ставлячи під загрозу цілісність демократичних процесів. Широке розповсюдження неправдивої інформації та підрив довіри до медіа-джерел ще більше загострюють проблеми, з якими стикаються органи державної влади та суспільство.

Вирішення проблем, пов’язаних з інформаційно-психологічними операціями, вимагає багатогранного підходу. Держава, міжнародні організації та технологічні компанії повинні співпрацювати, щоб розробити надійний захист від дезінформації, інвестувати в програми медіаграмотності

та посилити заходи кібербезпеки. Підвищення стійкості суспільства, сприяння критичному мисленню та розвиток культури скептицизму також можуть пом'якшити наслідки таких операцій і посилити заходи інформаційного захисту. Підвищення стійкості суспільства, розвиток критичного мислення та виховання культури скептицизму також можуть мінімізувати наслідки від операцій.

Крім того, ефективні заходи протидії інформаційно-психологічним операціям передбачають проактивні зусилля з виявлення і викриття дезінформаційних кампаній. Держава та суб'єкти господарювання повинні інвестувати в передові технології та аналітичні інструменти, щоб виявляти і відстежувати поширення неправдивої інформації та визначати джерела, які за нею стоять. Спільні зусилля між технологічними компаніями, платформами соціальних мереж та організаціями, що займаються перевіркою фактів, мають вирішальне значення для боротьби зі швидким поширенням дезінформації.

Програми з медіаграмотності відіграють життєво важливу роль для формування у громадян необхідних навичок критичного оцінювання джерел інформації та виявлення оманливих тактик. Освітні системи повинні інтегрувати медіаграмотність у навчальні програми, пропагуючи відповідальне орієнтування в цифровому просторі та розпізнання ознак маніпуляцій і пропаганди.

Крім того, міжнародна співпраця має важливе значення для подолання транснаціонального характеру інформаційно-психологічних операцій. Уряди країн світу повинні створити механізми для обміну розвідувальними даними, передовим досвідом і стратегіями для ефективної протидії цим операціям. Міжнародні договори та угоди можуть допомогти встановити норми та правила для обмеження зловмисного використання інформації та захисту цілісності демократичних процесів. Додатково слід використовувати технологічний прогрес для розробки надійних заходів кібербезпеки. Інвестиції в безпечну комунікаційну інфраструктуру, технології шифрування та системи виявлення загроз можуть підвищити стійкість до кібератак і маніпуляцій з інформацією. Крім того, державно-приватне партнерство має вирішальне значення для подолання викликів, пов'язаних з інформаційно-психологічними операціями. Співпраця між державою, технологічними компаніями, організаціями громадянського суспільства та науковими установами може сприяти розробці комплексних стратегій та інструментів для ефективної боротьби з інформаційними та психологічними операціями.

Інформаційно-психологічні операції змінили ландшафт сучасних конфліктів. Їх здатність формувати наративи, маніпулювати сприйняттям і використовувати вразливі місця ставить нові виклики перед політиками, стратегами і фахівцями з безпеки. Розуміючи механізми, стратегії та наслідки цих операцій, актуалізується необхідність розроблення проактивних заходів для захисту від їх згубного впливу та збереження цілісності демократичних суспільств перед обличчям нових глобальних загроз. Вирішення проблем,

пов’язаних із інформаційно-психологічними операціями, вимагає комплексного підходу, який включає в себе технологічні досягнення, програми медіаграмотності, міжнародне співробітництво та інший дієвий інструментарій. Зміцнюючи захист, розвиваючи критичне мислення та культуру стійкості, суспільство може пом’якшити вплив вказаних операцій і відстоювати цінності прозорості, свободи слова та демократичного врядування в цифрову епоху.

Список використаних джерел:

1. Лікарчук Н. В., Лікарчук Д. С. Інформаційно-психологічні війни: міжнародно-політичний аналіз. Міжнародні відносини: теоретико-практичні аспекти. 2022. №. 9. С. 157-172.

2. Фещенко І. В. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. Філософія та політологія в контексті сучасної культури. 2021. №. 1(13). С. 96-103.

Лясота А. Є.

кандидат політичних наук,
Дніпровський національний університет
імені Олеся Гончара
м. Дніпро, Україна

ІНСТИТУЦІЙНІ ВИКЛИКИ ТРАНСФОРМАЦІЇ ПОЛІТИЧНОЇ СИСТЕМИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Широкомасштабна воєнна агресія РФ проти України та запровадження воєнного стану не могли не позначитися на політичних процесах у нашій країні. Цей вплив не лише передбачено Законом України «Про правовий режим воєнного стану» обмеженнями, як: припинення виборів до органів влади всіх рівнів; заборонено проведення референдумів, демонстрацій, мітингів тощо; утворення військових адміністрацій. Існує чимало інших важливих факторів, обумовлених війною, які вже сьогодні трансформують внутрішньополітичний простір України, створюючи різноманітні конфігурації політичної системи в майбутньому.

Перш за все, в умовах війни постає проблема функціонування політичних інститутів, поява нових суб'єктів громадянського впливу та загальна криза партійної системи. Війна переформовувала політичне та інформаційне поле України. З одного боку, принципових змін в системі управління державою не відбулося. В Україні продовжують функціонувати основні органи державної влади з розподілом повноважень відповідно до демократичних стандартів. Крім того, повсюдне запровадження Військових адміністрацій, на думку О. Їжака (завідувача відділу регіональної політики НІСД), по факту в короткостроковій перспективі суттєво залишилося на місцях й не змінилося [3].

З іншого боку, як зазначила В. Підгорна, «продовжується дискредитація парламентаризму, зменшується кількість парламенту, хоча ВР продовжила свою роботу і ухвалила на 15% законів більше, ніж у мирні роки. Рівень протесту довіри до парламенту становить, за соціологічними опитуваннями, мінус 19% у порівнянні з іншими структурами влади». На її основі з причин такої ситуації є серйозні канали зв'язку, після закінчення війни число таких каналів є природно обмеженим. Падіння довіри до вищого представницького органу країни стає викликом для демократії в Україні, особливо з урахуванням того, що це падіння відбувається на фоні зростання довіри населення до силових структур [1].

Відповіддю на це могла стати реформа парламенту з підвищення ефективності роботи ВР, підвищення якості законотворчої діяльності та покращення іміджу вищого представницького органу країни. Останнє

потребуватиме забезпечення норм етичної поведінки депутатів, боротьби із лобізмом у стінах ВР, проблем депутатської дисципліни. Вже сьогодні, не дивлячись на війну, розпочалася робота над реалізацією такої реформи. Проте, як не дивно, навіть серед деяких депутатів запанувало збільшення ролі Уряду. Дійсно, Кабміни в попередні роки складаються переважно з міністрів, не з числа депутатів із депутатського корпусу (які мають мандатні довіри від своїх виборців), а з найманих людей (так звані «технократичні» уряди). такі урядовці не несуть відповідальності перед своїми виборцями та партією, яка їх висунула. Природа їх відповідальності, скоріше, суто професійна. Це важливий аспект політичної відповідальності. Крім того, перевага виконавчих інститутів влади порушує баланс владних повноважень та компетенцій, що не сприяє стійкості політичної системи.

Криза довіри до парламенту є сумісною із кризою ключового політичного інституту України – партійної системи. Як зазначила І. Павленко, вже до війни в Україні спостерігалася криза партій. Соціологічні опитування фіксували низький рівень довіри громадян до партій, як до політичного інституту загалом. Все це супроводжувалося падінням популярності фактично всіх політичних партій і, у першу чергу – тих, що представлені в парламенті. Деякі з них опинилися в рейтингах популярності на межі, або навіть за межею прохідного 5% бар'єру. І це при тому, що серед парламентських партій також не може бути появи потужних і перспективних проектів, які гарантовано могли б скласти конкуренцію на найближчих парламентських виборах. Усі нові партійні проекти також знаходилися на критичних 5% популярності [2].

З початку війни більшість партій так і не знайшли свого місця в умовах дії нових викликів і зникли з інформаційного поля країни. Це відзначили всі учасники дискусії. Протест, говорячи про наслідки цієї партійної кризи, експерти розійшлися у своїх прогнозах майбутніх змін.

На думку В. Подгорної, війна спонукала до поляризації політичного простору, що може призвести до перспективи того, що в Україні з’являться дві основні групи партій, або умовно дві «партії» - «військових» та «цивільних». Вже сьогодні, за соціологічними опитуваннями, виділено блок довіри на складах ЗСУ, ДСНС, Національної гвардії та волонтерів, а також другий блок – це громадські організації, які, зокрема, працюють на дипломатичному фронті, мають вже серйозні структурні установи і стовідсотково мають своє представництво в парламенті, в тому числі – внаслідок зміни партійного фінансування, його деолігархізації [3].

Крім того, справедливо відзначимо, що послаблення можливих позицій олігархів, окрім нових позицій на медіаринку України, створить ще одне поле можливо – політичного представництва. Тобто, актуалізується перспектива організації та фінансування нових партійних проектів поза інтересами великих фінансово-промислових груп. Ідея залучення коштів громадян, неолігархічного бізнесу – може бути реалізована, але у тому, що це буде у

майбутньому, сьогодні буде важко спрогнозувати. Цілком імовірно, що політичне поле України виявиться ще більш фрагментованим, і нові, в тому числі – регіональні партії не наберуть достатньої потужності, щоб прийняти рішення про загальнонаціональні проекти.

Зазначимо що, одним з інституційних викликів політичної системи України є трансформація лінії соціально-політичних розмежувань.

На думку Г. Макарова, воєнні події складають нові ряди суспільних і політичних розмежувань, а також відповідних дискурсів, навколо яких формується партійна система. Це, зокрема:

– ступінь мілітаризації суспільства (виявляти, зокрема, у визначені переваги бюджетного фінансування армії та оборонно-промислового комплексу над іншими, соціальними статтями та видатками на економічний розвиток; ставлення суспільства до різних аспектів регулювання військового обов'язку);

– модель економічного розвитку: ліберальної економічної та податкової політики або соціально орієнтованої держави з жорсткою фіскальною політикою та елементами прямого державного втручання у роботу суб'єктів підприємницької діяльності. Останнє є можливим, наприклад, у межах політики зайнятості. Втрата значної частини економічного потенціалу країни суттєво ускладнює пошук балансу між цими двома моделями. Перша користуватиметься підтримкою підприємців, друга – категорії громадян, які залежать від державного фінансування (працівники бюджетної сфери, пенсіонери, безробітні тощо);

– міра відкритості/закритості громадянського суспільства для зовнішніх впливів. Розмежування може актуалізуватися в процесі європейської інтеграції України (а саме – адаптації законодавства та соціальної практики до норм ЄС) і остаточно витіснити поділ на прихильників прозахідної чи проросійської зовнішньої політики. В економічній сфері воно виявляється у боротьбі за відкриті відносини з європейським митним простором або за захисні заходи національного товаровиробника; у ціннісній – за пріоритет прав і свобод індивіда та захист різних категорій меншин (етнічних, релігійних, гендерних тощо) або традиційних цінностей (національних, релігійних, сімейних); у політичній – за повну інтеграцію до Європейського Союзу або за максимальне збереження суверенітету) [2].

Доцільно констатувати, також, зникнення запиту на проросійські сили. Значна кількість партій було заборонено за свою колабораціоністську діяльність. О.Гарань (науковий директор Фонду «Демократичні ініціативи» імені Ілька Кучеріва), наголошує: «може, в Україні і зникли проросійські сили, проте залишилося чимало людей, які були їхніми членами, і ці люди, можливо, відмовилися від проросійськості, але зберегли». далеко від демократичних стандартів політичної практики» [1].

На думку сучасної дослідниці Г. Зеленько «здатність до самоорганізації українців, разом із інституційною сприятливістю яку продемонструвала наша країна в момент кризи – це два кроки нашої держави. І сьогодні, в умовах війни, ці дві системи розвиваються прискорено». Разом із тим, вона звернула увагу на ще один важливий аспект, який впливає на політичні запити громадян. На її думку, «…суспільство матиме посттравматичний синдром, і це також варто хворіти. Це вплине на радикалізацію суспільства. Варто зазначити, в даному контексті, про санацію державної влади, якщо ми зараз цього не зробимо – старі негативні практики (як повернення олігархів у медіа та політику), безперечно, спровокує радикальний спротив з боку фронтовиків та суспільства. А це впливає на стабільність держави, на те, чи буде в українському політичному просторі нормальна конкуренція». Дійсно, створення в українському суспільстві запобіжників проти виступу на демократичні свободи та проти монополізації влади є досить актуальним. Доказом цього є історія українського внутрішньополітичного спротиву [1].

Досліджуючи лінії можливого глибинного розподілу та майбутнього протистояння, потрібно відштовхуватися не лише від політичних інститутів та їх стану, але й проаналізувати зміни, які сьогодні відбуваються у суспільстві: «війна як суспільно-політичне виявилося змінило багато людей. , пробудив в них відчуття патріотизму, гордості, багатьох інших емоцій. Ці люди будуть брати участь у політичному процесі і як політики, і як активісти, і як виборці. Небезпека криється в ще більшому поділі суспільства на активних (які знайшли себе в новій політичній реальності) та пасивних (найбільш соціально постраждалих) громадян. Тому ваше електоральне протистояння може бути за новим принципом – між електоральними м патріотизмом і патерналізмом» [3].

Підсумовуючи, варто виділити кілька, ключових аспектів змін щодо політичної системи в умовах військового стану.

По-перше, політична система України в кризовій ситуації широкомасштабного вторгнення РФ показала ефективність і стійкість. Разом з тим, найслабшою виявилася та ланка системи, яка загрожує політичним партіям, що так і не пропонують проявити себе, або «знайти своє місце» під час війни. Ця криза стала логічним наслідком ситуації, що склалася на партійному полі України напередодні війни, а саме – фактично зареєстрованих в Україні політичних партій, які відповідали вимогам тогочасного партійного законодавства та розумінню «партій», що склалося в політичній науці та демократичній практиці. У передвоєнний період політичніі партії в Україні по факту були партіями переважно клубного типу, або взагалі суто виборчими проектами, а не об'єднаннями громадян із широким представництвом у регіонах (тобто, загальнонаціональними).

По-друге, одним з потужних викликів політичної системи України періоду війни стала фактична деолігархізація суспільних відносин, що

створила широкий спектр негативних дій, можливих для змін як у політичному, так і в медійному просторі.

Саме інформаційне середовище також зазнало серйозних трансформацій. З одного боку, з безпекових міркувань був організований Єдиний телемарафон, внаслідок чого відбулася певна монополізація телепростору. З іншої – значної популярності набули новинні месенджери та інтернет-блогери. Сьогодні кількість користувачів цього інформаційного ринку скорочується на кількість людей, які відвідують новини з телебачення. У той самий час Інтернет-простір функціонує поза межами українського медійного законодавства.

Популярність месенджерів та блогерів як постачальників новин та їх трактів не лише створює фактор нового впливу на політичний простір України, а має потенціал для його видозміни та появи нових учасників політичного процесу. Це перше середовище, яке значною мірою може висунути нових гравців, які свою медійну популярність здатні перетворити в популярність політичну.

Список використаних джерел:

1. Політичні процеси сучасності: глобальний та регіональний виміри. URL: https://ipiend.gov.ua/novyny/iv-vseukrainska-naukovo-praktychna-konferentsiia-politychni-protsesy-suchasnosti-hlobalnyj-ta-rehionalnyj-vymiry/ . (дата звернення 28.04.23).

2. Політична система України в умовах війни. URL: https://niss.gov.ua/news/komentari-ekspertiv/politychna-systema-ukrayiny-v-umovakh-viyny (дата звернення 28.04.23).

3. Парламент України у воєнний час. URL: https://www.constjournal.com/pub/2 2022/parlament-ukrainy-voiennyi-chas/ . (дата звернення 28.04.23).

КОНСТИТУЦІЙНЕ ПРАВО; МУНІЦИПАЛЬНЕ ПРАВО; ЦИВІЛЬНЕ ПРАВО І ЦИВІЛЬНИЙ ПРОЦЕС; СІМЕЙНЕ ПРАВО; МІЖНАРОДНЕ ПРИВАТНЕ ПРАВО

Рижук І. В.

кандидат юридичних наук, доцент,
доцент кафедри конституційного, адміністративного та фінансового права
Хмельницького університету управління та права імені Леоніда Юзькова
м. Хмельницький, Україна

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНДИВІДУАЛЬНОЇ КОНСТИТУЦІЙНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ НАРОДНИХ ДЕПУТАТІВ

Закріплення конституційно-правової відповідальності народних депутатів розпочинається зі ст. 3 Конституції України, в якій передбачена відповідальність держави перед народом, оскільки народний депутат входить до складу органу державної влади – Верховної Ради України, то на нього також поширюється дана норма.

Відповідальність народних депутатів України перед народом обґрунтовується й тим, що на підставі виборів парламентарій одержує вільний мандат. Принцип вільного депутатського мандата прямо не закріплюється в Конституції України, але він випливає із аналізу норм законодавства та який отримав визнання в ст. 75 Конституції України. Цей принцип має визначальне значення та обумовлює характер мандата народного депутата України. Крім того, Конституція України не передбачає таких складових ознак імперативного мандата, як накази виборців та відкликання народного депутата України виборцями.

До прийняття Конституції України 1996 року в Україні діяв імперативний мандат, основою якого була можливість відкликання народного депутата в разі неналежного виконання покладених на нього обов’язків, а також можливість виборців давати депутату обов'язкові до виконання накази. З прийняттям Конституції України 1996 року положення імперативного мандата почали суперечити її нормам, зокрема ст. 81 закріпила вичерпний перелік підстав, за яких повноваження народного депутата України припиняються достроково. Серед таких підстав відкликання депутата виборцями не передбачено. Отже, Конституція унеможливила застосування раніше прийнятого Закону України «Про відкликання народного депутата України», чинність якого була остаточно скасована лише 22 березня 2001 р.

Так, Конституцією України у 1996 році фактично було запроваджено вільний мандат народного депутата України, хоча в Основному Законі нашої держави відсутня норма, в якій би безпосередньо говорилося про це. Вільність депутатського мандата випливає також із положень Закону «Про статус народного депутата України», в якому жодної відповідальності перед виборцями, а також можливості відкликання народного депутата не передбачено.

В наукових колах існує думка, що однією з форм реалізації конституційно-правової відповідальності народного депутата України є зняття депутатської недоторканості. Цілком погоджуємось з даною позицією, лише зауважимо, що в даному випадку вирішальне значення відіграє подвійна сутність конституційних норм, оскільки ними передбачається не лише конституційно-правова відповідальність, але й закладено основи кримінальної та адміністративної відповідальності парламентаріїв, що знаходить своє продовження в нормах вже відповідних галузей права.

Окрім парламентаріїв, індивідуальну конституційно-правову відповідальність несуть також органи та посадові особи Верховної Ради України [1, с. 209]. Згідно з Конституцією України, Верховна Рада України обирає зі свого складу Голову Верховної Ради України, Першого заступника і заступника Голови Верховної Ради України (ст. 88), затверджує перелік комітетів Верховної Ради та обирає голів цих комітетів, а також у межах своїх повноважень, може створювати тимчасові спеціальні комісії для підготовки і попереднього розгляду питань (ч. ч. 1. 3. ст. 89) [2].

Конституційно-правова відповідальність Голови Верховної Ради України полягає в тому, що він може бути відкликаний з цієї посади, що закріплено в Основному Законі та регламенті Верховної Ради України. (ч. 5 ст. 88 Конституції України; ст. 76 глави 15 Регламенту Верховної Ради України від 10 лютого 2010 р.)[2; 3].

Голова Верховної Ради України може бути в будь-який час відкликаний з посади Верховною Радою на його прохання, а також може бути відкликаний у зв'язку з незадовільною його роботою на цій посаді, в тому числі у разі відсторонення від ведення пленарних засідань три і більше разів протягом однієї чергової сесії Верховної Ради, або через інші обставини, що унеможливлюють виконання ним своїх обов'язків. Дострокове припинення депутатських повноважень Головою Верховної Ради України має наслідком припинення його повноважень як Голови Верховної Ради України.

Окремо у Регламенті передбачено конституційно-правову відповідальність головуючого на пленарному засіданні Верховної Ради України. Мається на увазі, що дані норми можуть бути застосовані в однаковій мірі як до Голови Верховної Ради України так і до Першого заступника і заступника Голови Верховної Ради України в залежності від того, хто з них в конкретному випадку головував на пленарному засіданні.

Ст. 29 Регламенту закріплено, що у разі порушення головуючим на пленарному засіданні вимог Регламенту народний депутат має право невідкладно або після закінчення розгляду питання порядку денного пленарного засідання Верховної Ради звернутися до головуючого на пленарному засіданні із зауваженням про допущені ним порушення для негайного їх усунення.

У разі грубого або систематичного порушення Регламенту головуючим на пленарному засіданні, за пропозицією, внесеною в паперовій формі на пленарному засіданні не менш як двома депутатськими фракціями (депутатськими групами), або не менш як однією третиною народних депутатів від конституційного складу Верховної Ради шляхом зібрання їх підписів, або комітету, до предмета відання якого належать питання регламенту, після скороченого обговорення Верховна Рада може прийняти рішення про відсторонення головуючого на пленарному засіданні від ведення пленарних засідань на строк до двох пленарних днів більшістю голосів народних депутатів від конституційного складу Верховної Ради, про що робиться запис у протоколі пленарного засідання Верховної Ради. На цей час за ним зберігаються виплати, пов'язані з виконанням депутатських повноважень та посадових обов'язків.

У разі відсторонення головуючого на пленарному засіданні від ведення пленарних засідань три і більше разів протягом однієї чергової сесії Верховної Ради, за висновком комітету, до предмета відання якого належать питання регламенту, Верховна Рада може розглянути питання про відкликання його з посади відповідно Голови Верховної Ради України, Першого заступника чи заступника Голови Верховної Ради України [3].

Щодо конституційно-правової відповідальності Голови, першого заступника голови, заступника голови та секретаря комітету, Регламент нас відсилає до Закону України «Про комітети Верховної Ради України», де зазначено, що вищезгадані посадові особи парламенту можуть бути у будь-який час за рішенням Верховної Ради України відкликані зі своїх посад:

1) за їх власною заявою;

2) у зв'язку з їх незадовільною роботою на посаді;

3) внаслідок інших обставин, що унеможливлюють виконання ними своїх обов'язків.

Пропозиція про відкликання може бути внесена Головою Верховної Ради України або відповідним комітетом. Рішення комітету щодо внесення пропозиції про відкликання голови, першого заступника голови, заступника голови, секретаря комітету приймається на засіданні комітету. Після відкликання народного депутата України з посади голови, першого заступника голови, заступника голови чи секретаря комітету він залишається членом цього комітету, якщо Верховною Радою України не прийнято іншого рішення [4].

У національному законодавстві, зокрема беремо до уваги Закон України «Про статус народного депутата України», Закон України «Про комітети Верховної Ради України», передбачено відповідальність насамперед за вчинення протиправних дій щодо депутатів, а не за порушення самими парламентаріями норм законодавства, невиконання ними своїх обов'язків. Таким чином, переважна більшість положень законів в частині роботи в комітетах парламенту, їх обов'язків, носить суто декларативний характер й не тягне будь якої відповідальності. Лише частково передбачена така відповідальність й Регламентом Верховної Ради України. У тих же випадках, коли відповідальність за порушення вимог зазначеного Закону передбачена, санкції є досить м'якими.

Наприклад, згідно із статтею 33 Закону «Про статус народного депутата України», якщо народний депутат протягом календарного місяця упродовж однієї чергової сесії Верховної Ради України без поважних причин, не бере особистої участі у більш як 30 відсотках голосувань при прийнятті рішень Верховної Ради України на пленарних засіданнях Верховної Ради України або у більш як 50 відсотках засідань комітету Верховної Ради України, до складу якого його обрано, такому народному депутату не відшкодовуються витрати, пов'язані з виконанням депутатських повноважень, за відповідний календарний місяць [5]. Водночас згідно із законодавством багатьох інших європейських країн неучасть депутата у пленарних засіданнях чи засіданнях комітету карається штрафом або ж навіть достроковим припиненням депутатських повноважень (повноважень члена комітету), а не лише утриманням виплати заробітної плати за дні відсутності. На нашу думку, відсутність чіткого переліку поважних причин для відсутності на засіданнях парламенту та комітетів, дієвих санкцій за неучасть у засіданнях є ключовими причинами поширеної у Верховній Раді практики пропуску депутатами засідань парламенту та комітетів.

Ще одним з недоліків Регламенту Верховної Ради України є те, що ним не передбачено проведення чіткого розмежування між різними типами правопорушень та санкціями, що застосовуються у випадку їх вчинення (наприклад, вживання депутатом у виступі образливих слів може тягнути як оголошення попередження, так і припинення виступу чи позбавлення парламентаря права участі у пленарних засіданнях), санкціями за порушення, вчинені вперше та порушення, вчинені повторно на тому ж чи іншому пленарному засіданні. Одним з недоліків Регламенту є досить вузький перелік санкцій за порушення норм дисципліни й етики. Наприклад, за окремі категорії діянь, зокрема – застосування фізичної сили до депутатів, голосування за відсутніх колег, передачу іншим особам карток для голосування, несанкціоноване розголошення інформації, що була предметом обговорення на закритих засіданнях комітетів тощо – взагалі не передбачено дисциплінарної відповідальності, хоча у ряді країн їх вчинення має наслідком позбавлення депутата права входження до приміщень парламенту на певний

строк чи заборону його участі у пленарних засіданнях, позбавлення права членства в комітеті тощо.

У цьому контексті орієнтиром у розширенні переліку санкцій може слугувати досвід окремих країн ЄС, де санкції за невиконання депутатами обов'язків чи порушення норм, які стосуються роботи парламентаріїв в комітетах варіюються від оголошення попередження до позбавлення права на входження до приміщень парламенту на певний строк до утримання заробітної плати та навіть дострокового припинення повноважень тощо.

Список використаних джерел:

1. Словська І. Є. Верховна Рада України як суб'єкт конституційно-правової відповідальності. Право України. 2011. №5. С. 204-210.

2. Конституція України : чинне законодавство зі зм. та доп., станом на 1 вересня 2018 р. : (офіц. текст). К. : ПИЛИВОДА, 2018. 64 с.

3. Про Регламент Верховної Ради України : Закон України від 10.02.2010 р. Відомості Верховної Ради України. Офіц. вид. 2010. № 14, / № 14-15; № 16-17. – Ст. 412.

4. Про комітети Верховної Ради України : Закон України від 04.04.1995р. Відомості Верховної Ради України. Офіц. вид. 1995. № 19. Ст. 134.

5. Про статус народного депутата України : Закон України від 17.11.1992 р. Відомості Верховної Ради України. Офіц. вид. 1993. № 3. Ст. 17.

ЗЕМЕЛЬНЕ ПРАВО; АГРАРНЕ ПРАВО; ЕКОЛОГІЧНЕ ПРАВО; ПРИРОДОРЕСУРСНЕ ПРАВО

Бєлєвцев Ю. В.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка
сертифікований інженер-землевпорядник, сертифікований інженер-геодезист,
член Асоціації Фахівців Землеустрою України

ЗЕМЕЛЬНЕ ПРАВО В СУЧАСНІЙ УКРАЇНІ

Земельна реформа в Україні розтягнулась вже більше ніж на 30 років.

Її можна розділити на такі етапи:

1. УСВІДОМЛЕННЯ 1991-2000 р. – цей етап характеризується переходом від колективної власності до приватної, усвідомленням поняття приватна власність і взагалі розумінням народу, що це таке і навіщо воно треба.
2. ОРГАНІЗАЦІЯ ЕЛЕКТРОННИХ РЕЄСТРІВ 2000-2012 р. – цей етап приніс перехід від паперових носіїв до електронної реєстрації земельних ділянок. Дуже важкий етап з багатьма корупційними складовими.
3. ОПАНУВАННЯ РЕЄСТРІВ 2012-2020 р. – запрацювали реєстри у зв'язці, бази даних почали синхронізуватися (наприклад: кадастрові данні після злиття почали автоматично відображатись в реєстрі на нерухоме майно).
4. ДЕЦЕНТРАЛІЗАЦІЯ 2020-2023 р. - відбулися глобальні зміни по боротьбі з корупційною складовою. Наразі, реєстрація всіх документацій на землю проводиться екстериторіально. Тобто перевірка документації і видача кінцевого документа проводиться по всій території України без можливості контакту між замовником та реєстратором або між виконавцем і реєстратором.

На сьогоднішній день реформа в Україні рухається «гігантськими» кроками. Інколи фахівці не встпівають освоїти безліч нововведень, зміни в законодавстві, перехідні положення на час військового стану і т. ін.

Для того щоб легше було розібратись в законодавстві фахівцями із землеустрою в Україні були створені безприбуткові спілки. До таких спілок почали долучатись і законотворці, між ними ,наразі, комунікація налагоджена на високому рівні. Виносяться на обговорення проекти постанов, стало можливим сформувати колективну думку фахівців і внести свої пропозиції.

Представники спілки почали отримувати місця в комісії на видачу та анулювання сертифікатів на землевпорядну діяльність. Це важливий крок в запобіганні корупції.

З останніх позитивних нововведень можна відмітити спрощену процедуру зміни цільового призначення. Наприклад, стало можливим змінити з землі під садівництво на землі під забудову, при наявності зонування в містобудівній документації. Раніше це вимагало розроблення та погодження землевпорядних документацій та затвердження містобудівних детальних планів. Така процедура вимагала багато часу і включала корупційну складову.

На сьогоднішній день , в Україні у зв'язку з військовим станом призупинено відведення землі в приватну власність. Це своєчасний крок влади також пов'язаний з запобіганням корупції. Але залишилась можливість формування земельних ділянок в державну або комунальну власність з подальшою передачею в оренду фізичним та юридичним особам.

Підсумовуючи вище наведене, можна зазначити що наразі реформа на кульмінаційному шляху. І Держава в цьому питанні рухається в вірному напрямку.

МІЖНАРОДНЕ ПРАВО

Рудецька П. А.

Здобувач вищої освіти
факультету судового та міжнародного права
Національного університету «Одеська юридична академія»

ДЕЯКІ ПИТАННЯ ЩОДО ДОМАШНЬОГО НАСИЛЬСТВА: ДОСВІД ЗАРУБІЖНИХ КРАЇН В НАЦІОНАЛЬНЕ ПОЛЕ УКРАЇНИ

Домашнє насильство має глибоке історичне коріння як в Україні, так і в зарубіжжі. Воно бере свій початок із давніх-давен, відтоді як почало існувати людство на Землі. Різноманіття його форм негативно віддзеркалилося на процесах життєдіяльності, що значною мірою вплинуло на дискримінаційне становище жінок, чоловіків та дітей у суспільстві в цілому в сім'ї [1]. Попри прийняття міжнародних та внутрішньодержавних актів, які повинні регулювати відповідальність за злочини домашнього насильства кількість жертв постійно зростає.

Протидіяти злочинам домашнього насильства можливо, але потрібно обрати комплексний підхід до вирішення даної проблеми. У зв'язку, з цим необхідно, щоб вітчизняний законодавець міг вирішити та протидіяти злочинам домашнього насильства, потрібно враховувати зарубіжний досвід.

Звертаючись до Стамбульської конвенції, вона сьогодні є одним із найбільш прогресивних міжнародних інструментів протидії різним проявам домашнього насильства яка визначає «… всі акти фізичного, сексуального, психологічного або економічного насильства, які відбуваються в лоні сім'ї чи в межах місця проживання або між колишніми чи теперішніми подружжями або партнерами, незалежно від того, чи проживає правопорушник у тому самому місці, що й жертва, чи ні або незалежно від того, чи проживав правопорушник у тому самому місці, що й жертва, чи ні …» [2].

Потрібно зауважити, що переважна більшість національного законодавства розробляється у відповідності до міжнародних актів, оскільки в Україні діє примат міжнародного права над національним, проте законодавець може вносити свої корективи в якому визначає специфічне поняття «домашнє насильство» так і вживає заходів щодо протидії та запобіганню домашньому насильству.

В даній публікації досліджений взаємозв'язок із різними правовими системами та законодавствами. Щодо держав англо-американського типу правової системи,пропонуємо розглянути на прикладі Сполучених Штатів Америки. Якщо розглядати досвіт Сполучених Штатів Америки то найбільш потрібно врахувати досвід у протидій домашньому насильстві. Досить цікава

практика видання ордерів, які видаються на базі судового засідання, їх існує три типи: надзвичайний, тимчасовий та постійний[3].

Надзвичайний ордер видається тоді коли потерпла особа звертається до поліції. Це дозволяє оперативно відреагувати на звернення та як метод оперативного реагування на протидію насильству [4, с. 162].

Тимчасовий ордер видається на термін від чотирнадцяти до двадцять одного дня. Ордер видається без попереднього повідомлення особі,що вчинила насильство [5].

Для запобіганню насильству в США реалізується програма обов'язково реагування. Медичний заклад, який виявляє факт підозри або факт домашнього насильства, обов'язково зобов'язаний повідомити до правоохоронних органів. Відповідно можна зробити висновок, що в Україні це також можна зробити, але потрібно врахувати різні аспекти життєдіяльності населення.

Щодо романо-германського типу більш детально хотілось би зосередитись на практиці Франції. У Франції домашнє насильство вважається серйозною проблемою, у зв'язку з цим уряд діє активно, щоб боротися з цим явищем. У 2019 році Франція прийняла закон, який зміцнює захист жертв домашнього насильства. Закон передбачає широкий спектр заходів, включаючи заборону контакту зі зловмисником, встановлення електронного нагляду, надання жертвам фінансової допомоги та доступу до житла.Франція має національну лінію підтримки для жертв домашнього насильства. Лінія працює цілодобово і надає консультації та підтримку жертвам, а також допомагає їм знайти безпечне місце для перебування. Також діють різні проекти з профілактики домашнього насильства, наприклад, освітні кампанії та тренінги для працівників органів правопорядку. Країна активно співпрацює з іншими країнами, щоб боротися з домашнім насильством на міжнародному рівні. Наприклад, вона є учасником Ради Європи та Організації Об'єднаних Націй і бере участь у роботі з питань захисту прав жінок та боротьби з насильством. В цілому, Франція діє рішуче, щоб боротися з домашнім насильством та забезпечити захист прав жертв. Однак, як і в інших країнах, це є складною проблемою, і багато роботи ще потрібно зробити.

Враховуючи досвід іноземних країн, вважаю потрібним перерахувати як в Україні можна покращити ситуацію з боротьби домашнього насильства:

1. Україна має прийняти закони, які забезпечують захист жертв насильства та покарання за злочини насильства в сім'ї. До таких заходів можуть належати заборона примусового шлюбу, заборона насильства в сім'ї, встановлення механізмів захисту жертв та покарання винних.

2. Навчання людей про насильство в сім'ї та його наслідки може допомогти зменшити число випадків насильства в сім'ї. Освіта повинна включати інформацію про права жертв насильства, відповідальність за насильство в сім'ї та механізми захисту.

3. Важливо змінити стереотипи та усвідомлення насильства в сім'ї, щоб зменшити його поширеність. Це може бути досягнуто через медіа-кампанії, освіту та інші культурні заходи.

Список використаних джерел:

1. Мануїлова К. В., Рудецька П. А. Злочини домашнього насильства в міжнародному праві: історія становлення відповідальності. Трансформація правових систем в умовах збройних конфліктів : матер. круглого столу (м. Одеса, 10 лютого, 2023 р.). 2023, С. 52 – 55. URL: http://dspace.onua.edu.ua/handle/11300/23629

2. Конвенція Ради Європи про запобігання насильству проти жінок і домашньому насильству та боротьбу з цими явищами (Стамбульська конвенція) 2011 року. URL:https://zakon.rada.gov.ua/laws/show/994_001-11

3. Довгунь К. Досвід США та Канади у сфері запобігання і протидії домашньому насильству. Підприємництво, господарство і право. 2020, №11. С. 111-114. URL:http://pgp-journal.kiev.ua/archive/2020/11/19.pdf

4. Горбова О., Галунько В. Адміністративно правове регулювання протидії насильству в сім'ї. Київ : Інститут публічного права, 2016. 226 с.

5. Міжнародний досвід попередження та протидії домашньому насильству / за заг. ред. А.О. Галая. Київ : КНТ, 2014. 160 с.

Shevchenko - Ledyan Cristina

student
Institute of Secondary Education
Roquetas de Mar, Spain

CURRENT ENVIRONMENTAL LAW IN THE EUROPEAN UNION: THE LEGAL ASPECT

The influence of the environmental agenda on global politics and economics has increased significantly at the beginning of the 21st century. Special legal acts aimed at creating a legal basis for the implementation of environmental policy began to appear in the countries. It should be noted that the European Union soon became the leader in this area. European institutions were among the first in the world that actively developed climate and environmental policy.

Furthermore, it is environmental protection and the climate agenda that have become one of the "calling cards" of the European Union.

There are many environmental issues in the world today, and five key ones stand out. These are: climate change, environmental pollution (air, water and soil), generation of waste, loss of biodiversity and vulnerability of both natural and man made ecosystems.

The environmental agenda became particularly relevant during the Covid-19 pandemic. The pandemic caused a sharp decline in international trade, virtually curtailed the activities of some of the largest companies in many parts of the world, significantly reduced the number of tourists, air travel, etc.

As a consequence, it has had an unpredictable effect on the environmental situation on all continents. "Gradually there has been a return to their habitats, such as the return of dolphins to the canals of Venice as a result of the clearing of the adjacent waters" [1]. The reduction in emissions has contributed to the disappearance of smog in Beijing [2].

As the world economy recovers, all of these processes will reverse in one way or another. However, the pandemic has demonstrated to humanity an extremely important pattern - the effects of human activities are reversible and the ecosystem is capable of regeneration.

The European Union, together with the European Commission, has developed and adopted a significant number of laws and initiatives in the field of environmental protection and ecology.

Let's try to analyze the legal framework of the key legal acts that underpin the environmental policy of the modern European Union.

"The EU Green Deal" (also known as the "European Green Deal")

On 11 December 2019, the European Commission adopted the European Green Deal (EGD) Communiqué. "The Green Deal" is the largest economic course

correction in EU history. It is an action program of the European Commission with the main objective of moving towards a climate-neutral Europe by 2050. Climate neutrality is the way of development in which greenhouse gas emissions are equal to their absorption and economic growth is not linked to increased resource use [3].

The goals of the EGD cannot be achieved by the EU alone, and cooperation extends beyond the EU's borders. Countries that set themselves ambitious targets to reduce emissions and increase the absorption of greenhouse gases must be energy independent, protect, and improve their technology. The target of emission reduction is a clear goal towards an energy efficient, low-carbon, green economy. "The European Green Deal is Europe's structural answer and a new growth strategy to transform the EU into a modern, resource efficient and competitive economy.

The EU REPowerEU plan

The documents were published on the EC website on 18 May 2022. The EU REPowerEU plan is one of the latest founding documents of the European Union climate policy, since the refusal to use non-renewable energy sources (oil, natural gas, coal, etc.) in the short term would be a step connected with the Green Deal and other European environmental regulations.

The plan came into force in spring 2022 due to Russia's special military operation in Ukraine. In August 2022, the EU stopped importing coal from Russia. The finalized REPowerEU plan, which includes a set of measures that would allow the EU to stop importing Russian oil, gas and coal in 2027. According to the REPower EU plan, EU countries must meet the following conditions: increase imports of LNG and gas pipelines by non-Russian corporations, increase their own production and imports of biomethane and renewable hydrogen [3].

All these measures would reduce the demand for Russian gas by two thirds by the end of this year. The European Commission sees great promise in the fact that ending the EU's dependence on Russian fossil fuels, which are used as economic and political weapons, will cut costs by nearly 100 billion euros a year.

The EU Action Plan "Towards Zero Air, Water and Soil Pollution"

The document was approved by the European Commission on 12 May 2021. It is a comprehensive vision for the year 2050. The vision envisages a world where pollution is reduced to levels that are not harmful to human health and natural ecosystems. The Plan defines the steps towards achieving these goals.

This Action Plan sets benchmarks for reducing pollution in each area compared to current levels. These benchmarks include:

- Improving air quality to reduce premature deaths by 55%.
- Improving water quality by reducing levels of waste and plastic debris in the sea by 50% and microplastics pollution in nature by 30%.
- Improving soil quality by reducing soil nutrient loss and pesticide use by 50%. - Reduction in the total amount of waste, and in the amount of residual urban waste by 50%.
- A 25% reduction in the number of EU ecosystems whose biodiversity is threatened by pollution [3].

The European Union has been able to coordinate joint actions by individual states to protect the environment, necessitating a study of their common policies and legislation in this area.

"European Parliament and Council Regulation 2021/1119" (known as the "European Climate Law")

The document was adopted on 30 June 2021. This document set a legally binding carbon neutrality target by 2050. In addition, it is expected to reduce net greenhouse gas emissions by 55% from 2050 levels by 2030. The process of agreeing on a common climate goal by 2040, including a carbon budget for 2030-2050, as well as targets for a negative emissions strategy after 2050, has been initiated among EU member states.

Eighth EU Environment Action Program 2030

The Environmental Action Program is the most important document in the climate field. It sets out the guidelines for the European Union's environmental policy. It calls for the active involvement of all stakeholders at all levels of government to ensure effective implementation of EU climate change and environmental legislation.

Conclusions: It can be concluded from the above that European legislation not only focuses on the prevention of environmental risks, but also on preventive measures which, in the long term, will ensure that production and consumption become environmentally neutral.

Today's key European Union environmental law documents, particularly those adopted in the last decade, are based on the progressive national experiences of its member states. It should be noted that European environmental law is a new and complex legal part of European integration. It is characterized by the search for optimal approaches to solving complex problems of natural resources management and nature conservation.

References:

1. *Machemer, T. (2021, April 5). Dolphins Spotted in Venice's Grand Canal-for Real This Time. Smithsonian Magazine. Retrieved from https://www.smithsonianmag.com/smart-news/dolphins-spotted-venices-grand-canal real-time-180977403/*

2. *Sommer, L. (2020,March 4).Why China's Air Has Been Cleaner During The Coronavirus Outbreak. NPR organization. Retrieved from https://www.npr.org/sections/goatsandsoda/ 2020/03/04/811019032/why-chinair-has-been-cleaner-during-the-coronavirus-outbreak*

3. *European Commission, official website commission. europa.eu*

Shevchenko - Ledyan Cristina

student
Institute of Secondary Education
Roquetas de Mar, Spain

STUDY OF THE LEGAL MEANS OF IMPLEMENTING ENVIRONMENTAL POLICY IN SPAIN

There is a huge number of environmental problems in today's world, among which five key ones can be highlighted. These are: climate change, environmental pollution (air, water and soil), waste generation, loss of biodiversity and vulnerability of both natural and man-made ecosystems.

In addition, the environmental situation is gradually becoming an increasingly significant development factor affecting the political and economic situation in individual states and in their economic unions. Since the foundation of the European Union (EU) in 1993, the member states of this community have taken up the protection of the global environment as a goal. The EU has succeeded in coordinating the joint efforts of individual countries to protect the environment.

At the time when Spain was preparing to join the European Economic Community (EEC), strict environmental requirements were imposed on the Kingdom of Spain. If these requirements had not been met, this could have been a real obstacle to Spain's membership of the Community. Spain needed to achieve an optimum balance between the economic development of the country and ensuring appropriate level of environmental protection. As early as in the 1980s, the development of the national program of pollution prevention began.

It should be noted, however, that real ecological barriers to new construction appeared in regions with an industrially overstretched infrastructure. The intensification of production and the first structural shifts in the economy, oriented towards 'quality' growth and the rational use of natural resources, became evident. Spain became a member of the EEC in 1985.

The right for a healthy environment was for the first time proclaimed in the Constitution of the Kingdom of Spain, adopted on 27 December 1978. Since then, Spain's experience in environmental legislation has been widely applied in the main national laws of other countries.

According to Art. 45 points 1, 2, 3 of the Constitution of Kingdom of Spain [1], all have the right to the environment that is favorable for human development and all are obliged to preserve it. The state authorities ensure the sustainable use of all natural resources in order to protect and improve the quality of life and protect and restore the environment, based on the requisite shared solidarity. People who violate the right to a favorable environment of others are liable, in accordance with the law, to criminal or administrative prosecution and are obliged to compensate the damage caused.

The Constitution of the Kingdom of Spain, article 149, paragraph 1, point 23 [1] states that the exclusive competence of the State includes such things as the legal framework for environmental protection, regardless of the powers of the autonomous communities to carry out additional protective measures. Legislative framework on the use of forests, woodlands and pastures.

Currently, Spain pursues an active environmental policy, which is reflected in its extensive legal framework for environmental protection, characterized by an elaborate and easily traceable hierarchy. There are more than 20 laws at the national level designed to protect the environment. Law 21/2013 of 9 December is considered fundamental and obliges each autonomy and province to take appropriate measures and adopt strategic plans and programs both at the national and local levels.

In April 2022, the Waste and Contaminated Soil Act came into force.

The government says the innovations should help to slow down the current rate of waste generation (by 13% in 2025 and 15% in 2030) and increase recycling (by 2023, at least 70% of plastic bottles available at the market should be recycled). The law includes separate collection of "at least" paper, metal, plastic and glass [2].

In the Kingdom, a new law came into force that obliged the country's retail establishments to accept customers' packaging. In particular, retailers selling food by weight and bottled drinks must pack goods in customers' packaging if they provide it. The main aim of the innovation is to discourage the use of plastic disposable packaging. Supermarkets have been given six months to adapt to the new law.

According to the Spanish Ministry of Agriculture, Fisheries and Food in 2020, Spanish households throw away 1.3 billion kilograms of food every year, an average of 31 kilograms per person [3].

Intending to stop this waste, the Spanish government has approved a draft law in the Council of Ministers on the reduction and rational use of food waste. The measures introduced by the law include informing customers by restaurants that they can take away leftovers, donating food to food banks, and forcing all participants in the food chain to develop a waste prevention plan.

The climate law, signed by the Spanish Parliament in May 2021, commits the country to reducing emissions by 23% by 2030 compared to 1990 levels. Since the law was signed, it has banned new permissions for the exploration and extraction of coal, gas and oil and has set a target of generating 74% of the country's electricity from renewable sources by 2030. In addition, the sale of vehicles powered by fossil fuels will be completely banned by 2040. The extraction of fossil fuels on Spanish territory, according to the law, is to be completely phased out by 31 December 2042.

The measures announced indicate the country's full commitment to expand the market for renewable energy sources (RES), which is attracting major international investors. The law notes that climate targets must be reviewed

periodically, and the first consultation is scheduled for 2023. The law requires all companies in the country to develop clear climate action plans with emission reduction targets which must be met within five years. This is the first such law in the history of Spain which has faced a climate emergency.

All these things force the industry to make fundamental changes, but the climate emergency leaves us no choice. It's not so much a question of changing our way of life as of finding ways and means of preserving much of it without destroying the planet [4].

In our opinion, an equally important reason for the current environmental situation in Spain is also the lack of environmental and legal culture, both of citizens and government representatives. This leads to the fact that citizens have insufficient understanding of their constitutional rights, and representatives of the authorities do not take measures to properly protect nature or make decisions on cases of environmental damage or the suspension of environmentally harmful economic activities not in favour of the society.

It is clear that the new environmental standards are paid for with taxpayers' money in relatively more developed European countries and increase the cost of the EU's final products for consumers all over the world. Higher prices for imported and domestic raw materials due to the application of environmental standards in cross-border trade also increase production costs. Hence, the increase in the cost of European goods and the decrease in the capacity to import raw materials are directly related to the strengthening of European environmental standards.

A great support for Spain's national environmental policy is provided by the key legal acts of the modern European Union, which include the eighth Environment Action Program (EAP) for the period 2021-2030, the EU Green Deal (also known as the European Green Deal), the Regulation 2021/1119 of the European Parliament and Council (known as the European Climate Law), the EU Action Plan Towards Zero Air, Water and Soil Pollution, and the REPowerEU Plan.

Perhaps it is thanks to the freedom of action which Law 34/2007 of 15 November grants to the autonomous communities that the Spanish are able to move forward in the "ecological" direction.

Taking into account the information mentioned above, we can conclude that Spain's environmental policy focuses not only on the prevention of environmental risks, but also on preventive measures that in the long term are capable of achieving production and consumption neutrality in relation to the environment.

References:

1. *https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf*
2. *https://how2spain.com/novosti/zakon-ob-otxodax-2022.html*
3. *https://russpain.com/news/potrebitel/ispaniya-podrobnosti-pro-zakon-o-pishhevyh-othodah4.*
4. *https://www.eurotopics.net/en/261187/new-climate-targets-in-europe-on-the-right-track.*

НАЦІОНАЛЬНА БЕЗПЕКА; ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА; ДЕРЖАВНА БЕЗПЕКА; ЕКОНОМІЧНА БЕЗПЕКА;

Абрамов А. В.

Студент, Akademie HUSPOL s.r.o.,
м. Куновіце, Чеська Республіка

РОЗВИТОК КВАНТОВИХ ОБЧИСЛЕНЬ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Відмінності класичної та кватнової комп'ютерних моделей

Класична комп'ютерна модель заснована на принципі бітів, які можуть бути у двох станах – 0 або 1. Це дозволяє проводити операції з логічними значеннями та зберігати інформацію в пам'яті. У класичних комп'ютерах інформація обробляється послідовно, крок за кроком, що забезпечує детерміновану поведінку комп'ютера.

У квантовій комп'ютерній моделі, використовується кубіти, які можуть бути в більш ніж двох станах. Це дозволяє використовувати принципи квантової механіки для обробки інформації та здійснювати операції зі значеннями, які можуть бути у декількох станах одночасно. Це дає можливість виконувати декілька операцій одночасно та зменшує кількість кроків, необхідних для вирішення складних задач.

Одна з найбільш значущих відмінностей між класичною та квантовою моделями полягає в тому, що в квантовому світі інформацію неможливо скопіювати, а це надає додаткової захисту від несанкціонованого доступу та злому даних. Крім того, з квантовими комп'ютерами можна вирішувати задачі, які класичні комп'ютери не можуть розв'язати в прийнятний час, наприклад, розкладання складних чисел на прості множники. Таким чином, квантові комп'ютери можуть відкривати нові можливості для обчислювальної науки та розв'язування складних проблем у різних галузях.

Загрози кватнової комп'ютерної моделі

В той же час, квантові обчислення несуть велику загрозу для захисту інформації, в тому числі національного рівня. Алгоритми шифрування та хешування даних, які законодавчо визнані стійкими до зламу класичними комп'ютерними моделями, можуть виявитись вразливими до алгоритмів квантового обчислення [1][2]. Прикладами таких алгоритмів є RSA, Diffie-Hellman та ECC.

В особливості це стосується алгоритмів асиметричного шифрування, таких як RSA та ECDSA, що використовують великі прості числа для створення криптографічних ключів. Проблема полягає в тому, що дані, зашифровані класичними алгоритмами шифрування, можуть бути

розшифровані з використанням факторизації числа на прості множники. А ця операція може бути виконана на квантовому комп'ютері за лінійний час.

На відмінку від класичних комп'ютерів, квантові здатні до виконання алгоритму Шора [3][4], який є квантовою версією алгоритму розкладання чисел на прості множники. Цей алгоритм здатний знайти прості множники надзвичайно великих чисел у значно менший термін, ніж класичний алгоритм розкладання чисел на прості множники. Таким чином, з використанням квантового комп'ютера можливо досить швидко розкрити ключі, що використовуються в алгоритмах асиметричного шифрування.

Також варто згадати квантовий алгоритм Гровера [5], який може бути використаний для пошуку значень функції шифрування, яка використовується в алгоритмах асиметричного шифрування. Це дозволяє зловмисникам швидко знайти приватний ключ, що відповідає публічному ключу, що використовується для шифрування повідомлень.

Отже, алгоритми асиметричного шифрування вразливі до квантових обчислень через можливість використання алгоритму Шора для розкриття криптографічних ключів та алгоритму Гровера для пошуку приватних ключів.

Вплив на національну безпеку України

Розвиток квантових обчислень може стати серйозною загрозою для національної безпеки України через здатність квантових комп'ютерів швидко розкривати шифри, які використовуються для захисту важливих даних. Сучасні шифри, які використовуються в банківській сфері, національній обороні та інших галузях, базуються на складних математичних алгоритмах, які важко зламати класичним комп'ютером. Однак, квантові комп'ютери можуть швидко знайти ключі, які використовуються в цих шифрах, що зробить їх легко зламуваними.

Крім того, інші країни матимуть квантові комп'ютери, які перевершують Україну за потужністю, вони зможуть швидше розв'язувати ці задачі та матимуть перевагу у вирішенні своїх геополітичних інтересів.

Також, існує загроза квантового шпигунства, коли квантові комп'ютери можуть використовуватися для швидкого розшифрування інформації, що передається через канали зв'язку. Це може стати серйозною загрозою для національної безпеки України, оскільки чутлива інформація, така як військова та дипломатична інформація, може бути викрадена іншими державами з допомогою квантових комп'ютерів.

Ще одною великою загрозою є так званий підхід "збирай зараз, розшифруй пізніше" (Harvest Now, Decrypt Later – HNDF). Його суть полягає в тому, що зловмисники збирають і зберігають інформацію для подальшого дешифрування у майбутньому, коли квантові обчислювальні засоби стануть потужнішими. Особливіть даної загрози в тому, що вже збережені зловмисниками дані неможливо наново перешифрувати алгоритмами стійкими до квантових обчислень оскільки власник цих даних не має до них

доступу. На відміну від, наприклад, даних фінансового сектору, де є більш актуальними поточні дані, дані національного масштабу, будь то військові чи політичні таємниці, можуть нести свій вплив на геополітичну картину світу у майбутньому

Таким чимом, квантові обчислення є серйозною загрозою для національної безпеки України, оскільки можуть призвести до розкриття секретної інформації, зашифрованої за допомогою алгоритмів шифрування, що використовуються в даний час. Наслідки такого розкриття можуть бути катастрофічними для різних сфер діяльності, таких як військова, економічна, політична, наукова тощо. Тому важливо вжити заходів щодо підвищення захисту даних та розробки кванто-стійких алгоритмів шифрування та інших заходів забезпечення кібербезпеки.

Список використаних джерел:

1. Robert Burns The cybersecurity implications of quantum computing. URL: https://www.securityinfowatch.com/cybersecurity/information-security/managed-network-security/article/53012965/the-cybersecurity-implications-of-quantum-computing

2. Ryan Arel Explore the impact of quantum computing on cryptography. URL: https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography

3. Feynman R. Simulating Physics with Computers // International Journal of Theoretical Physics. — 1982. — С. 467–488.

4. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. — 1994. — С. 124–134.

5. Lov K. Grover Quantum Computing. URL: https://cryptome.org/qc-grover.htm

6. Р. В. Олійников, І. Д. Горбенко, О. В. Казимиров, В. І. Руженцев, О. О. Кузнєцов, Ю. І. Горбенко, В. І. Долгов, О. В. Дирда Основні властивості нового національного стандарту блокового шифрування ДСТУ 7624:2014. URL: https://okazymyrov.github.io/assets/attachments/abstracts/2015/62ecf5f38d1a41bbdc35452c6fa17a.pdf

7. Наказ "Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації". URL: https://zakon.rada.gov.ua/laws/show/z0862-07#Text

8. Наказ "Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису". URL: https://czo.gov.ua/news-details?id=107

Биндич В. В.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ КЛАСИФІКАЦІЇ ДАНИХ В ХМАРНИХ СХОВИЩАХ

З кожним роком кількість інформації зростає з шаленою швидкістю. Важко собі уявити, що 10 років тому кількість усіх даних дорівнювала тому, що зараз створюється лише за один місяць. І за оцінками експертів їх кількість буде лише зростати, і що важливо, зростати дуже швидко. Так прогнозують, що за 2024 рік буде зібрано майже на чверть більше даних ніж у 2023, а у 2025 на чверть більше ніж у 2024 (Duarte, 2023). Тому навіть невеликі та середні компанії будуть стикатися з проблемами про які раніше знали лише великі корпорації. Так питання ефективного зберігання та обробки даних все частіше з'являєтеся на порядку денному.

Але це не єдина проблема. З появою державної регуляції зберігання та обробки персональних, та інших даних користувачів (найбільш відомим в цій сфері є "Загальний регламент про захист даних" або GDPR) з'явилася ще низка проблем, пов'язаних з правильною ідентифікацією, маркуванням, захистом та обробкою захищених даних. Це пов'язано із тим, що в разі порушення вимог регулятора, компанія буде вимушена заплатити немалий штраф, а також може понести репутаційні збитки. І якщо останні дуже важко виміряти, то кількість і суми штрафів зростають із року в рік. Так наприклад за порушення одного GDPR у 2019 році було зареєстровано 143 штрафи на загальну суму майже 72 мільярди Євро, а вже у 2022 зареєстровано 532 штрафи на загальну суму 841,5 мільярд Євро (GDPR Enforcement Tracker, n.d.).

Тому не дивно, що зараз з'явилося багато ініціатив які направлені на вирішення цих проблем. На мій погляд одним із перспективних напрямків може стати використання штучного інтелекту та систем машинного навчання, що за допомогою спеціальних алгоритмів можуть не лише ідентифікувати дані які вимагають особливих умов зберігання серед великої кількості інших даних, але й перевірити чи відповідають умови зберігання цих даних вимогам стандартів таких як GDPR, PCI-DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act) та інших. Такі рішення відносно прості у використанні, ефективні і можуть обробляти терабайти даних за відносно короткий час, а головне вартість таких рішень відносно невелика, що робить їх доступними навіть для середнього та малого бізнесу.

Розглянемо вартість такої системи на прикладі AWS Macie, хмарного сервісу від компанії Amazon на основі систем машинного навчання, який дозволяє автоматично ідентифікувати, класифікувати та захистити конфіденційні дані. Для прикладу візьмемо невеличку компанію яка обробляє на місяць 10 мільйонів документів різних даних загальним об'ємом приблизно 150 ГБ. Вартість такого сервісу буде становити всього 150 доларів на місяць (Amazon, n.d.). Натомість компанія отримає автоматичний інструмент для перевірки різних документів .doc, .docx, .pdf, .xls, .xlsx, .csv, .htm, .html та навіть файли повідомлень електронної пошти та специфічних форматів для Big Data (Amazon, 2020). Якщо порівняти ці витрати із потенційним штрафом у декілька десятків тисяч євро та потенційними репутаційними збитками, то витрати на систему виглядають мізерними. В свою чергу система легко масштабується і витрати в ній зростають лінійно до кількості оброблюваних даних.

Ще одним, на мою думку вирішальним критерієм є те, що модель вже «натренована», тобто готова до використання, і вимагає мінімальної кількості налаштувань та експертизи від користувача, при цьому вона зберігає свою ефективність. Той самий AWS Macie після початкових налаштувань може швидко визначати різні типи персональних даних, починаючи від імені та дати народження, та закінчуючи водійським посвідченням чи номерним знаком автомобіля більше ніж для 30 країн світу (Amazon). Але не дивлячись на те, що більшості користувачів буде достатньо такого рішення, AWS пропонує можливість легкого розширення своєї моделі додатковими правилами (Jing, Choung, & Reith, 2020), що робить її ще більш гнучкою.

Та на цьому потенціал можливостей подібних систем не обмежується. Оскільки система використовує стандартний набір протоколів та інтерфейсів, вона може бути легко інтегрована як частина більш складної системи контролю безпеки інформації. Наприклад, якщо поєднати систему баз даних із системою розпізнавання конфіденційних даних на основі штучного інтелекту, то можливо проаналізувати повідомлення користувачів або публічні пости чи інші фрагменти текстової інформації на предмет конфіденційних даних (Silveira & Pádua, 2021). Це в свою чергу дозволить підвищити рівень безпеки всієї організації. А інтеграція системи із корпоративним месенджером, дозволить своєчасно повідомити відповідального співробітника про можливі проблеми (Carvalho & Silveira, 2021). Загалом потенціал подібної системи майже безмежний, так якщо інтегрувати її із моделлю, що дозволяє розпізнавати зображення або звук, можливо розширити і без того широкий список підтримуваних форматів.

Звичайно після всього вище згаданого може скластися враження, що подібні системи можуть повністю замінити людину або вирішити всі проблеми безпеки конфіденційних даних, але це не так. Вони лише інструмент, який дозволяє більш ефективно аналізувати сховища даних та

підсвічувати проблеми в умовах невпинного зростання кількості даних та підвищення вимог до їх зберігання та обробки. Щоб правильно зрозуміти проблеми, які виявить система, а також своєчасно та якісно відреагувати на виклики, потрібні кваліфіковані спеціалісти в сфері безпеки інформації.

***Список використаних джерел**:*

1. *Amazon. (2020, August 08). Data Discovery and Classification. Retrieved from https://static.us-east-1.prod.workshops.aws/public/1776ed5b-4ad9-46c8-8d77-884903f8abcf/static/images/Macie-Workshop-Deck.pdf*
2. *Amazon. (n.d.). Amazon Macie Pricing. Retrieved May 14, 2023, from https://aws.amazon.com/ru/macie/pricing/*
3. *Amazon. (n.d.). Sensitive data types: Personal information – Personally identifiable information. Retrieved May 14, 2023, from https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html#managed-data-identifiers-pii*
4. *Carvalho, J., & Silveira, B. (2021, June 10). Creating a notification workflow from sensitive data discover with Amazon Macie, Amazon EventBridge, AWS Lambda, and Slack. Retrieved from https://aws.amazon.com/ru/blogs/security/creating-a-notification-workflow-from-sensitive-data-discover-with-amazon-macie-amazon-eventbridge-aws-lambda-and-slack/*
5. *Duarte, F. (2023, April 03). Amount of Data Created Daily. Retrieved from Exploding Topics: https://explodingtopics.com/blog/data-generated-per-day*
6. *GDPR Enforcement Tracker. (n.d.). List of GDPR fines. Retrieved May 14, 2023, from https://www.enforcementtracker.com/?insights*
7. *Jing, K., Choung, J., & Reith, L. (2020, August 26). Discover sensitive data by using custom data identifiers with Amazon Macie. Retrieved from https://aws.amazon.com/blogs/security/discover-sensitive-data-by-using-custom-data-identifiers-with-amazon-macie/*
8. *Silveira, B., & Pádua, T. (2021, October 05). Enabling data classification for Amazon RDS database with Macie. Retrieved from https://aws.amazon.com/ru/blogs/security/enabling-data-classification-for-amazon-rds-database-with-amazon-macie/*

Воробьев И. О.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ВЛИЯНИЕ КИБЕРАТАК НА БЕЗОПАСНОСТЬ ГОСУДАРСТВА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ КИБЕРВОЙНЕ

В эпоху быстрого развития информационных технологий и все более тесной связи между цифровым и реальным миром, кибербезопасность становится одним из наиболее важных аспектов безопасности государств и организаций. Вместе с ростом интернета и цифровизации сферы деятельности возникают новые угрозы, способные нанести серьезный ущерб геополитической стабильности и безопасности стран. Одной из таких угроз является кибервойна.

Кибервойна представляет собой конфликт, в котором государства используют кибератаки и кибероперации в качестве оружия для достижения своих целей. Это может включать нападения на критическую инфраструктуру, кибершпионаж, манипуляцию информацией и другие формы киберагрессии. Последствия таких атак могут быть катастрофическими, оказывая влияние на геополитическую обстановку, экономическую стабильность и национальную безопасность.

Одним из примеров кибервойны является кибератака на энергетическую систему, известная как атака на энергетическую инфраструктуру Украины в 2015 году. В течение нескольких часов неизвестные хакеры совершили серию скоординированных кибератак, которые привели к отключению электроэнергии для около 230 тысяч человек. Кибератака была направлена на системы управления энергетическими объектами, что вызвало серьезные нарушения в работе электроэнергетической инфраструктуры. Эта атака считается первым документированным случаем, когда кибератаки привели к физическому воздействию на реальную инфраструктуру.

Другим примером является кибершпионаж, связанный с международными отношениями. Один из таких случаев был связан с хакерской группой, известной как APT29. Эта группа была обвинена в кибершпионаже, в том числе в хакерских атаках на правительства и организации в разных странах. Наиболее заметной атакой, связанной с этой группой, стала атака на компьютерную сеть Демократической партии США в 2016 году. Эта атака стала объектом широкого внимания и вызвала серьезные политические последствия, повлиявшие на геополитическую обстановку и отношения между США и другими странами.

Эти примеры кибервойны демонстрируют, как кибератаки могут иметь глобальные последствия и повлиять на геополитическую ситуацию и безопасность стран. Кибератаки на энергетическую инфраструктуру могут нарушить экономику, безопасность и устойчивость государств, в то время как кибершпионаж может влиять на политические процессы, международные отношения и национальную безопасность. Эти случаи подчеркивают необходимость развития международного сотрудничества и улучшения кибербезопасности.

Улучшение кибербезопасности и сотрудничество на международном уровне становятся все более важными для предотвращения и противодействия кибервойне. Некоторые дополнительные аспекты, которые могут быть учтены в связи с примерами кибервойны, включают:

Развитие кибероборонны: Государства должны разрабатывать и укреплять свои кибероборонительные возможности для обнаружения, предотвращения и отражения кибератак. Это включает в себя создание и развитие центров кибербезопасности, тренировку специалистов по кибербезопасности и применение передовых технологий защиты.

Многоуровневая защита: Разработка и внедрение комплексных систем защиты, которые включают фаерволы, антивирусы, антишпионы, системы обнаружения вторжений и шифрование данных. Комбинированный подход к защите помогает предотвратить и обнаружить различные типы кибератак.

Мониторинг и обнаружение: Разработка и внедрение систем мониторинга и обнаружения аномального поведения в сети. Это позволяет оперативно обнаруживать и реагировать на потенциальные кибератаки, а также проводить анализ инцидентов для предотвращения повторного возникновения.

Исследования и инновации: Непрерывные исследования и инновации в области кибербезопасности помогают развивать новые методы обнаружения и защиты от кибератак. Использование искусственного интеллекта, машинного обучения и аналитики данных может помочь в прогнозировании и предотвращении киберугроз.

Улучшение общественной осведомленности: Общественность должна быть осведомлена о потенциальных угрозах кибервойны и принимать меры по защите своей кибербезопасности. Кампании по информированию, обучение и создание осведомленности о кибератаках и методах защиты помогут укрепить общественную готовность к киберугрозам.

Улучшение кибергигиены: Обучение пользователей базовым принципам кибербезопасности и практикам безопасного использования информационных систем. Это включает использование сложных паролей, регулярное обновление программного обеспечения, осторожность при открытии вредоносных ссылок и вложений, и регулярное создание резервных копий данных.

Юридические и политические меры: Государства должны разработать и применять соответствующие юридические и политические меры для предотвращения и пресечения кибератак. Это включает в себя ужесточение законодательства в области кибербезопасности, установление ответственности за кибератаки и содействие международным договорам и соглашениям в области кибербезопасности.

Развитие международных норм и правил: Государства должны продолжать работу над разработкой и согласованием международных норм и правил в киберпространстве. Это включает создание договоренностей о том, как государства должны вести себя в киберпространстве, и установление ответственности за нарушение этих норм.

Улучшение кибербезопасности и сотрудничество на международном уровне являются важными факторами в предотвращении и ограничении последствий кибервойны. Необходимо уделить должное внимание разработке и реализации эффективных стратегий и мер безопасности для защиты критической инфраструктуры и информационных систем от кибератак.

Кибератаки имеют значительное влияние на безопасность государства в эпоху цифровой трансформации. Они представляют серьезную угрозу для национальной безопасности, экономического развития и политической стабильности. В результате кибератак могут быть нанесены значительные ущербы критической инфраструктуре, включая энергетические системы, финансовые институты, транспортные сети и государственные коммуникации.

Противостоять кибервойне и защищать безопасность государства требует комплексного подхода и эффективных методов противодействия. Одним из ключевых аспектов является разработка и реализация превентивных мер, включая улучшение кибербезопасности, обновление и защиту информационных систем, обучение персонала и осведомленность об угрозах кибератак.

Понимание влияния кибератак на безопасность государства и эффективные методы противодействия кибервойне играют решающую роль в защите национальных интересов и обеспечении стабильности. Только путем совместных усилий, сотрудничества и постоянного развития в области кибербезопасности мы сможем достичь более безопасного и надежного цифрового будущего.

Список использованных источников:

1. Richard A. Clarke, Robert K. Knake "Cyber War: The Next Threat to National Security and What to Do About It" (Кибервойна: следующая угроза национальной безопасности и что с этим делать). HarperCollins, 2020. 320 с.

2. Jason Andress, Steve Winterfeld "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners" (Кибервойна: методы, тактика и инструменты для специалистов по безопасности). Elsevier Science, 2013. 324 с.

3. Information Resources Management Association "Cybersecurity and Cyberwarfare: Concepts, Methodologies, Tools, and Applications" (Кибербезопасность и кибервойна: концепции, методологии, инструменты и приложения). IGI Global, 2018.

Гаврилюк В. С.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Вступ. На сучасному етапі розвитку суспільства кібербезпека та штучний інтелект відіграють величезну роль у захисті держав та їхніх громадян від різноманітних загроз в кіберпросторі. Зростання залежності від технологій посилює необхідність використання ефективних засобів захисту.

Кібербезпека - це захист комп'ютерних систем та мереж від крадіжки або пошкодження їхнього апаратного та програмного забезпечення, а також від зловживання або втрати переданих через них даних. Головною метою кібербезпеки є забезпечення конфіденційності, цілісності та доступності інформації.

Штучний інтелект (AI) - це галузь комп'ютерних наук, що зосереджена на створенні систем або програм, які можуть виконувати задачі, що зазвичай вимагають людського інтелекту, такі як розпізнавання мови, визначення зображень, навчання та рішення проблем.

Мета дослідження полягає в аналізі та вивченні можливостей застосування штучного інтелекту в області кібербезпеки з метою підвищення ефективності засобів захисту інформації та систем в умовах зростаючих кіберзагроз.

Значущість цього дослідження обумовлена декількома факторами.

По-перше, з розвитком технологій збільшується кількість кібератак, що можуть мати негативний вплив на національну безпеку та економіку. По-друге, AI може значно підвищити швидкість та точність виявлення кіберзагроз, що дозволяє ефективніше забезпечувати захист інформаційних ресурсів. По-третє, розуміння можливостей та обмежень AI у кібербезпеці є критично важливим для розробки стратегій та політик, спрямованих на забезпечення безпеки в кіберпросторі на національному та глобальному рівнях.

Таким чином, дослідження можливостей штучного інтелекту у кібербезпеці є актуальним та важливим завданням, яке спрямоване на забезпечення стійкості інформаційних систем до зовнішніх та внутрішніх загроз.

Машинне навчання для виявлення кіберзагроз. Машинне навчання, як підгалузь штучного інтелекту, здатне автоматизувати процес виявлення кіберзагроз, вивчаючи зразки даних та визначаючи аномалії. Алгоритми

машинного навчання можуть бути навчені ідентифікувати зразки поведінки, які зазвичай вказують на несанкціонований доступ, зловмисне ПЗ або інші види атак.

Це може бути здійснено через методи наглядованого та ненаглядованого навчання.

Алгоритми глибокого навчання для аналізу та прогнозування кібератак. Глибоке навчання, як розширення машинного навчання, використовує нейронні мережі з великою кількістю шарів для моделювання складних зразків та взаємозв'язків в даних. Застосування глибокого навчання в кібербезпеці може включати в себе аналіз великих об'ємів мережевих даних для виявлення складних атак, таких як APT (Advanced Persistent Threats), та прогнозування потенційних векторів атак.

Приклади успішного застосування AI у кібербезпеці.

- Виявлення мережевих вторгнень (NID): Машинне навчання може бути використане для аналізу мережевого трафіку на предмет виявлення несанкціонованого або підозрілого доступу.
- Аналіз шкідливого програмного забезпечення (ПЗ): Глибоке навчання може виявляти шкідливе ПЗ, аналізуючи його характеристики та поведінку, і таким чином попереджати розповсюдження вірусів та троянських коней.
- Phishing-атаки: AI може використовуватися для ідентифікації та блокування підозрілих електронних листів, що намагаються змanити користувачів до виконання дій, які можуть призвести до компрометації їхньої безпеки.

Застосування штучного інтелекту у кібербезпеці представляє величезний потенціал для посилення здатності систем та мереж стояти на захисті від сучасних та майбутніх кіберзагроз.

Точність моделей і можливість помилок. Хоча AI може допомогти значно підвищити ефективність виявлення кіберзагроз, існують виклики з точністю моделей машинного навчання. Моделі можуть виявлятися чутливими до шуму або непередбачуваних даних, що призводить до помилкових сигналів (false positives) або непомітних атак (false negatives). Важливо постійно оновлювати та налаштовувати моделі, щоб вони адаптувалися до змінних зразків кібератак.

Етичні питання та виклики щодо приватності. Застосування AI в кібербезпеці також може викликати етичні питання, особливо щодо поводження з даними користувачів та приватністю.

1. Збір даних: Для ефективного навчання моделей AI необхідні великі набори даних, які часто містять персональну інформацію. Це може викликати проблеми з конфіденційністю та захистом даних.
2. Використання даних: AI може використовуватися для масового збору та аналізу даних без відома або згоди користувачів, що порушує принципи приватності.

3. Відповідальність та прозорість: Важко визначити відповідальність за помилки або шкоду, спричинену системами AI. Також, багато моделей AI є “чорними ящиками”, що ускладнює розуміння того, як саме приймаються рішення.

З урахуванням цих викликів та обмежень, необхідно розробляти стратегії та політики, які беруть до уваги етичні аспекти та захист даних при використанні AI в кібербезпеці.

Прогнозування тенденцій розвитку AI у сфері кібербезпеки. AI продовжує розвиватися, і ми можемо очікувати побачити декілька ключових тенденцій у сфері кібербезпеки:

- Автономна реакція на загрози: AI може стати більш автономним у виявленні та реагуванні на кіберзагрози в реальному часі, що може включати автоматичне блокування векторів атак або зміну конфігурацій безпеки.
- Контекстно-орієнтований аналіз: Використання AI для аналізу більш широкого контексту загроз, допомагаючи системам краще розуміти відмінності між легітимними діями та кібератаками.
- Сумісність AI і квантових технологій: Інтеграція квантових обчислень може підвищити можливості AI в обробці та аналізі великих наборів даних, підвищуючи ефективність виявлення загроз.

Потенційний вплив на національну безпеку.

- Захист критичної інфраструктури: AI може відігравати ключову роль у захисті критичних інфраструктур, таких як електромережі, водопостачання та телекомунікації, від кібератак.
- Боротьба з кібершпигунством та кібертероризмом: AI може сприяти ідентифікації та контруванню спроб шпигунства та терористичних атак у кіберпросторі, що стає все більш важливим для національної безпеки.
- Міжнародна співпраця та норми: Розвиток AI у кібербезпеці може призвести до зміцнення міжнародної співпраці та розробки нових норм і стандартів для захисту кіберпростору.

З урахуванням цих перспектив та потенціального впливу на національну безпеку, необхідно розумно підходити до розробки та застосування AI, забезпечуючи, що це використовується відповідально та з повагою до приватності та етичних стандартів.

Висновок. Штучний інтелект відіграє все більш визначальну роль у сфері кібербезпеки. З його допомогою можна значно підвищити ефективність виявлення та реагування на кіберзагрози, використовуючи технології машинного та глибокого навчання. Однак, разом з перевагами, AI має і свої обмеження, такі як проблеми з точністю моделей, а також етичні виклики, пов'язані з приватністю та використанням даних.

Рекомендації для подальшого дослідження.

- Основи на етиці та приватності: Потрібно розробляти та впроваджувати моделі AI, які будуються на принципах етики та захисту

приватності, і це має бути інтегровано на всіх етапах розробки та застосування.

- Міждисциплінарний підхід: Оскільки AI і кібербезпека перетинають різні галузі, важливо втілювати міждисциплінарний підхід у дослідженнях, залучаючи експертів з різних областей.
- Співпраця та міжнародні стандарти: Сприяти міжнародній співпраці та розробці глобальних стандартів для використання AI в кібербезпеці, забезпечуючи сумісність та безпеку на глобальному рівні.
- Постійне навчання та адаптація: Враховувати, що кіберзагрози постійно еволюціонують, і важливо розвивати системи AI, які можуть адаптуватися та вчитися на основі нових даних та зразків поведінки.

Список використаних джерел:

1. *Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.*
2. *Carlini, N., Katz, G., Barrett, C., & Dill, D. L. (2019). Provably minimally-distorted adversarial examples. arXiv preprint arXiv:1909.05893.*
3. *Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press. http://www.deeplearningbook.org*
4. *Hadžiosmanović, D., Simionato, L., Bolzoni, D., Zambon, E., & Etalle, S. (2014). N-Gram against the machine: On the feasibility of the n-gram network analysis for binary protocols. Research in Attacks, Intrusions, and Defenses, 354-373.*

Грішко Д. Ю.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ІНСТРУМЕНТИ ТА ВИМІРЮВАННЯ ДОТРИМАННЯ ВИМОГ GDPR ДЛЯ МАЛИХ ТЕХНОЛОГІЧНИХ КОМПАНІЙ

Вступ. У світі цифрового бізнесу Загальний регламент про захист даних (GDPR) суттєво змінив підхід організацій до обробки персональних даних. Малі технологічні компанії, які, мають менше ресурсів, ніж їхні більші конкуренти, стикаються з унікальними викликами щодо досягнення та забезпечення відповідності до GDPR.

Розуміння GDPR. GDPR, який набув чинності з травня 2018 року, є постановою, запровадженою Європейським Союзом для захисту конфіденційності даних громадян ЄС. Ця постанова стосується будь-якої організації, яка обробляє дані громадян ЄС, незалежно від їх масштабу чи місця розташування. Основні принципи включають законність, справедливість, прозорість, мінімізацію даних, точність, обмеження зберігання, цілісність і конфіденційність. [1]

Важливість дотримання вимог GDPR для малих технологічних компаній. Відповідність вимогам GDPR є не лише юридичною необхідністю, але й фактором довіри. Це демонструє клієнтам і споживачам, що компанія цінує та поважає їх права на приватність. Санкції за невідповідність можуть становити до 4% річного обороту компанії або 20 мільйонів євро, в залежності від того, яке значення вище. [1]

Кроки на шляху до відповідності GDPR. Щоб досягти відповідності вимогам GDPR, невеликі технологічні компанії повинні виконати такі основні кроки, як зокрема: [2]

- Аудит даних: визначення типів зібраних персональних даних, способів їх обробки, зберігання та обміну.
- Політика конфіденційності: Оновлення політики конфіденційності, щоб забезпечити її прозорість, зрозумілість і роз’яснення прав користувачів відповідно до GDPR.
- Оцінка впливу на захист даних (Data Protection Impact Assessment, DPIA): впровадження DPIA там, де обробка може призвести до високого ризику для суб’єктів даних.
- Призначення спеціаліста із захисту даних (DPO): Залежно від масштабу обробки даних може знадобитися DPO.
- План реагування на порушення безпеки даних: підготовка надійного плану виявлення, звітування та управління наслідками будь-яких порушень безпеки даних.

Вимірювання відповідності GDPR. Щоб спростити процес відповідності GDPR, доступні різні інструменти та програмне забезпечення. Це може автоматизувати проблему відповідності, покращити управління даними та допомогти контролювати перманентне дотримання вимог GDPR.

Інструменти планування розподілу даних: планування розподілу даних є важливим кроком у відповідності GDPR, оскільки воно допомагає зрозуміти, які дані зберігаються, де вони зберігаються та як вони переміщуються в організації. Такі інструменти, як OneTrust і DataGrail, можуть допомогти невеликим технологічним компаніям автоматизувати цей процес. [3, 4]

Програмне забезпечення для керування конфіденційністю: ці інструменти полегшують загальне керування процесами конфіденційності даних. Програмне забезпечення, таке як TrustArc і iubenda, може допомогти невеликим технологічним компаніям обробляти запити на доступ суб'єктів даних і підтримувати записи діяльності з обробки даних постійно оновленими та актуальними. [3]

Інструменти реагування на інциденти: ефективне та швидке реагування на будь-яке порушення безпеки даних є вимогою GDPR. Інструменти реагування на інциденти, такі як D3 SOAR і IBM Resilient, можуть допомогти компаніям планувати, керувати та відстежувати реагування на будь-які інциденти порушення безпеки, витоку даних.

Інструменти розуміння та категоризації даних: розуміння типу та ступеню конфіденційності даних, що зберігаються, є ключовим для відповідності вимогам GDPR. Інструменти виявлення та класифікації даних, такі як Spirion і Netwrix Auditor, можуть допомогти в ідентифікації та категоризації даних. [4]

Інструменти управління ризиками третіх сторін: GDPR також вимагає відповідальності за дані, надані третім сторонам. Такі інструменти, як Vendorpedia та Prevalent, можуть допомогти оцінити та керувати ризиками, пов'язаними зі сторонніми постачальниками.

Інструменти шифрування: захист персональних даних є основою GDPR. Інструменти шифрування, такі як ESET і Symantec, забезпечують необхідний рівень захисту персональних даних, які зберігаються компанією. [3, 4]

Важливо зазначити, що хоч ці інструменти та програмне забезпечення можуть значно допомогти у відповідності GDPR, вони не можуть замінити повного розуміння вимог GDPR або потреби в постійному навчанні персоналу та вдосконаленні процесів у компанії.

Виклики та можливості для малих технологічних компаній:

Відповідність GDPR справді може створити кілька проблем для малих технологічних компаній:

Обмеження ресурсів: невеликі підприємства часто працюють з обмеженими ресурсами, а впровадження заходів щодо відповідності GDPR

вимагає часу, грошей і кваліфікації. Інвестиції в нові інструменти, найм або навчання спеціаліста із захисту даних (DPO) і регулярне навчання всього персоналу можуть бути ресурсномісткими завданнями для компанії. [5]

Розуміння та інтерпретація законодавства: GDPR – це складний законодавчий акт, який може бути важко повністю зрозуміти та правильно інтерпретувати. Це може бути особливо складно для невеликих технологічних компаній без спеціалізованих юридичних команд.

Постійний розвиток технологій: технології швидко розвиваються, і з кожним витком розвитку з'являються нові міркування щодо конфіденційності даних. Іти в ногу з цими постійними змінами, зберігаючи відповідність вимогам GDPR, може бути складно.

Незважаючи на ці проблеми, відповідність GDPR відкриває значні можливості для малих технологічних компаній:

Зміцнення довіри: дотримання норм є потужним способом для бізнесу продемонструвати свою відданість захисту персональних даних, що може допомогти зміцнити довіру клієнтів, споживачів і ділових партнерів.

Конкурентна перевага: на переповненому ринку відповідність GDPR може бути відмінною рисою. Компанії, які можуть продемонструвати надійний захист даних, швидше за все, будуть більш привабливими для потенційних клієнтів або партнерів.

Покращене керування даними: кроки, вжиті для відповідності GDPR, можуть призвести до кращого загального керування даними в компанії. Більш чітке відображення та категоризація даних може призвести до ефективніших і доцільніших операцій. [5]

Висновок: Враховуючи все вищесказане, можна побачити, що дотримання GDPR у малих технологічних компаніях - це не просто виклик, але й велика можливість. Так, безперечно, можуть виникнути проблеми, як-от обмежені ресурси, складність інтерпретації законодавства та швидкий розвиток технологій. Але з правильним підходом та використанням доступних інструментів - від програмного забезпечення для планування розподілу даних до систем управління приватністю - можна перетворити ці виклики на можливості.

Звертаючись до GDPR, компанії не просто дотримуються правил; вони показують клієнтам та партнерам, що цінують їхню приватність. Бізнес покращує управління даними, зміцнює довіру з клієнтами та навіть отримує конкурентну перевагу на ринку. Тому дотримання та вимірювання відповідності GDPR - це більше, ніж просто юридична вимога. Це шлях до довіри, зростання та успіху.

Список використаних джерел:

1. Rules for the protection of personal data inside and outside the EU. – [Електронний ресурс]. – Доступ: https://commission.europa.eu/law/law-topic/data-protection_en.

2. UK GDPR guidance and resources. – [Електронний ресурс]. – Доступ: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

3. Business software and services review. – [Електронний ресурс]. – Доступ: https://www.g2.com/.

4. Capterra. – [Електронний ресурс]. – Доступ: https://www.capterra.com/.

5. Security news, protection and business innovation. – [Електронний ресурс]. – Доступ: https://www.csoonline.com/.

Кучерук А. С.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

РОЛЬ LEAN-МЕНЕДЖМЕНТУ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ДЕРЖАВНОЇ ІНФОРМАЦІЇ

Зростаюча залежність від інформаційних технологій та розширення кіберзагроз ставлять перед нами серйозні виклики в галузі інформаційної безпеки. У цьому контексті важливо розглянути можливість використання принципів Lean-менеджменту для забезпечення ефективного управління інформаційною безпекою та кібербезпекою, а також захисту державної інформації.

Основні принципи Lean-менеджменту

Перш ніж розглядати роль Lean-менеджменту у забезпеченні інформаційної безпеки, варто розібратися з основними принципами цього підходу. Lean-менеджмент базується на філософії безвідходності, спрямованої на досягнення максимальної ефективності виробничих процесів. Основні принципи Lean-менеджменту включають:

- Визначення цінності з точки зору клієнта: Lean-підприємство має розуміти потреби своїх клієнтів та виробляти продукцію або надавати послуги, які задовольняють їх потреби.

- Визначення потоку: Lean-підприємство має усунути всі перешкоди, які гальмують потік виробництва, та створити оптимальні умови для безперервного руху процесів.

- Забезпечення потягу: Lean-підприємство повинно виробляти продукцію тільки тоді, коли це потрібно клієнту, уникати надлишків та запасів.

- Досягнення перфекції: Lean-підприємство має постійно прагнути до покращення процесів та забезпечення якості продукції.

Застосування Lean-менеджменту в інформаційній безпеці

- Визначення цінності для інформаційної безпеки: Підприємства та організації повинні чітко розуміти, яка інформація для них є найціннішою та найбільш вразливою. Застосування Lean-підходу допоможе зосередити увагу на захисті самої важливої інформації.

- Виявлення та усунення втрат: Lean-підходу можна використовувати для ідентифікації потенційних загроз безпеці інформації та втрати даних. Застосування Lean-інструментів допоможе виявити проблемні місця та запровадити заходи для усунення цих проблем.

- Створення культури безпеки: Lean-підходу передбачає активну участь всього персоналу у покращенні процесів. Такий підхід можна використовувати для формування культури безпеки, в якій всі співробітники відчувають відповідальність за безпеку інформації та активно долучаються до заходів щодо кібербезпеки.

Застосування Lean-менеджменту в кібербезпеці

- Визначення цінності для кібербезпеки: Застосування Lean-підходу допоможе виявити критичні активи та інформацію, які мають найвищий рівень важливості з точки зору кібербезпеки. Це дозволить спрямувати ресурси та заходи на захист самої важливої інформації та систем.

- Управління ризиками: Lean-підходу можна використовувати для ідентифікації, оцінки та управління ризиками в галузі кібербезпеки. Застосування Lean-інструментів дозволить розробити ефективну стратегію захисту від загроз та швидко реагувати на нові вразливості.

- Вдосконалення процесів реагування: Lean-підходу можна використовувати для оптимізації процесів реагування на кіберінциденти та відновлення після них. Шляхом усунення зайвих кроків та оптимізації часових рамок можна значно знизити вплив інцидентів на організацію.

Захист державної інформації за допомогою Lean-менеджменту

- Визначення цінності для державної інформації: Державні структури мають ідентифікувати найціннішу та найбільш вразливу інформацію, яка вимагає особливого рівня захисту. Lean-підхід допоможе зосередити зусилля на захисті самої важливої державної інформації.

- Створення резервів та бекапів: Lean-підходу можна використовувати для створення ефективної системи резервного копіювання та бекапів державної інформації. Це дозволить запобігти втратам даних та швидко відновити їх у разі необхідності.

- Забезпечення безпеки постачальників: Lean-підхід передбачає оптимізацію ланцюжків постачання та співпрацю з надійними постачальниками. В контексті захисту державної інформації це означає необхідність встановлення високих стандартів безпеки для постачальників і перевірку їх виконання.

Висновок

Використання принципів Lean-менеджменту допомагає ефективно управляти ризиками, виявляти та усувати вразливості, а також підвищувати свідомість та відповідальність всього персоналу. Застосування Lean-підходу сприяє покращенню ефективності та якості процесів, що має прямий вплив на забезпечення інформаційної безпеки та кібербезпеки. Крім того, Lean-менеджмент може бути ефективним інструментом для захисту державної інформації, що є критично важливим у контексті національної безпеки.

Список використаних джерел:

1. ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, 2013.

2. ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. International Organization for Standardization, 2013.

3. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, 2020.

4. ENISA: European Union Agency for Cybersecurity. [Электроний ресурс]. Режим доступу: https://www.enisa.europa.eu/

6. Lean Enterprise Institute. [Электроний ресурс]. Режим доступу: https://www.lean.org/

Мацько В. А.

Студент, Akademie HUSPO s.r.o.
м. Куновіце, Чеська Республіка

КІБЕРБЕЗПЕКА ТА КІБЕРРИЗИКИ RFID СИСТЕМ

RFID є однією з найпоширеніших технологій автоматичної ідентифікації об'єктів або осіб. Технологія RFID, заснована на поєднанні ідентифікаторів і датчиків, була широко впроваджена в багатьох сферах, включаючи системи постачання, виробництва та контролю руху. Однак, незважаючи на переваги цієї технології, питання безпеки та конфіденційності залишаються відкритими.

Метою системи RFID є передача даних від портативного пристрою, який називається міткою, до пристрою зчитування RFID для виконання певної програми на основі ідентифікаційної інформації або інформації про місцезнаходження, наданої міткою.

Мітки RFID, також відомі як транспондери, є ідентифікаційними пристроями, які кріпляться на об’єкті. Кожна мітка зазвичай складається з

- антени, виготовленої з невеликої котушки дротів,
- мікрочіпа, який використовується для електронного зберігання інформації про об’єкт (наприклад, транспортний засіб або контейнер),
- оболонки чіпа та котушки.

Мітка також може містити датчики для запису, наприклад, температури, удару або вологості, що дозволяє динамічно відстежувати та повідомляти про характеристики навколишнього середовища об’єкта.

Зчитувач RFID є пристроєм, який використовується для зв’язку з мітками RFID. Через одну або декілька антен він передає та приймає радіочастотні сигнали з ідентифікатором. Зчитувач перетворює отримані радіохвилі в цифрові дані, які зазвичай надсилаються до серверної системи. Зчитувачі складаються з передавача, приймача, антени, мікропроцесора, контролера, пам'яті та джерела живлення.

Дані RFID повинні збиратися, фільтруватися, оброблятися та керуватися серверною системою. У базі даних зберігаються повні записи інформації про продукт, документи моніторингу та інші дані, пов’язані з пристроями RFID.

Розглянемо кілька прикладів застосування RFID технологій.

1. Системи маркування RFID вважаються ефективними інструментами для ідентифікації та моніторингу тварин. Серед переваг їх застосування є запобігання передачі захворювань і забезпечення безпеки харчових продуктів для споживачів.

2. Впровадження технології RFID у логістичній сфері вже є стандартною практикою. Цю технологію було визнано одним з найефективніших методів усунення або зменшення неточностей інвентаризації.

3. Широкого застосування технологія також набула в галузі перевезень. Вона дозволяє відслідковувати шкідливі викиди транспортних засобів, керувати автопарком таксі, стягувати оплати на платних дорогах, та багато іншого.

4. Використання технології RFID у сфері охорони здоров'я покращує якість обслуговування пацієнтів. Окрім збору інформації, пов'язаної з пацієнтом, як наприклад його присутність у палаті чи стан здоров'я, можна також визначити параметри його навколишнього середовища, такі як температура, вологість та наявність токсичного газу.

RFID-мітки є основою системи RFID і можуть бути класифіковані як активні та пасивні [1].

Пасивні мітки не мають внутрішнього джерела живлення і потребують живлення від зчитувача RFID. Зчитувач випромінює електромагнітні хвилі, які індукують струм в антені мітки та живлять чіп на мітці. Коли живлення мікросхеми мітки перевищує мінімальний поріг напруги, схема вмикається, і мітка передає свою інформацію на зчитувач. Через відсутність батареї пасивні мітки мають відносно короткий діапазон зчитування, лише кілька метрів.

Активні мітки містять власний акумулятор, який використовується як для живлення чіпа, так і для посилення зворотного сигналу. Батарея дає міткам можливість безперервно контролювати дорогоцінні товари або статус пломбування контейнера. Порівняно з пасивними мітками, активні мітки мають більший діапазон зчитування (десятки і навіть сотні метрів), більший об'єм пам'яті та швидший час обробки. Однак час роботи батареї обмежує термін служби мітки [2].

RFID також діляться на категорії за їх радіочастотою. Чотири основні діапазони радіочастот у діапазоні від 30 кГц до 5,8 ГГц: низька частота (LF), висока частота (HF), надвисока частота (UHF) і мікрохвильова частота (MW). Вибір частоти залежить від програми, розміру мітки та необхідного діапазону зчитування. Загалом, чим вища частота, тим швидша передача даних або пропускна спроможність, але тим дорожча система.

Як і інші інформаційні системи, системи RFID вразливі до атак і можуть бути скомпрометовані на різних етапах їх використання. Атаки на систему RFID загалом можна розділити на чотири основні групи:

- атаки на автентичність,
- атаки на цілісність,
- атаки на конфіденційність
- атаки на доступність.

Крім того, що технологія RFID вразлива до поширених атак, таких як прослуховування, "людина посередині" (Man in the middle) та відмова в обслуговуванні (DoS), технологія RFID, зокрема, сприйнятлива до спуфінгу (підробки) та атак на системи живлення.

Оскільки мітка RFID – це бездротовий пристрій, який випромінює дані під час зчитування, існує ризик того, що зв'язок між міткою та зчитувачем може бути прослухано. Прослуховування відбувається, коли зловмисник перехоплює дані за допомогою сумісного зчитувача в той час як мітка зчитується авторизованим зчитувачем RFID.

Оскільки більшість систем RFID передають інформацію у чистому текстовому форматі (через обсяг пам'яті міток та вартість їх виготовлення), підслуховування є простим, але ефективним засобом для зловмисника отримати інформацію про дані міток.

Залежно від конфігурації системи можлива атака "людина посередині" (Man in the middle), коли дані передаються від одного компонента до іншого. Зловмисник може перервати шлях зв'язку та маніпулювати інформацією між компонентами RFID. Атака розкриває інформацію до того, як призначений пристрій її отримає, і може змінити інформацію посеред процесу передачі. Навіть якщо в результаті передачі було отримано недійсні дані, атакована система може припустити, що проблема спричинена помилками мережі, і не розпізнає, що сталася атака. Система RFID особливо вразлива до атак "людина посередині", оскільки мітки мають малі розміри та низьку ціну, що спричиняє, як правило, брак складної системи захисту.

RFID-мітки також вразливі до DoS-атак. Мета полягає не в тому, щоб вкрасти чи змінити інформацію, а в тому, щоб відключити систему RFID, унеможливити її використання. Перешкоди за допомогою шуму в частотному діапазоні системи RFID можуть зменшити пропускну здатність та перервати з'єднання з мережею, що призведе до загального збою. Перешкоди виникають, коли пристрій, який активно транслює радіосигнали, блокує та порушує роботу будь-якого чи всіх прилеглих зчитувачів RFID. Іншою формою DoS RFID-міток є їх фізичне видалення з об'єктів, повне очищення їх вмісту або обгортання їх металевою фольгою.

Ще одна можлива атака, а саме спуфінг, відбувається, коли підроблена мітка маскується під дійсну мітку [3]. Клонування міток — це атака підробки, коли зловмисник захоплює дані з дійсної мітки та створює копію захопленого зразка на порожній мітці. Інший приклад: зловмисник зчитує дані мітки з дешевого товару в магазині, а потім завантажує дані на іншу мітку, прикріплену до подібного, але дорожчого товару.

На відміну від раніше розглянутих атак RFID, стеження є загрозою спрямованою проти особи. Замість відстеження тварин чи товарів, системи RFID можна використовувати для несанкціонованого відстеження переміщень людей.

Одним із способів захисту конфіденційності об'єктів, позначених RFID-мітками, є їх ізоляція від будь-яких електромагнітних хвиль [4]. Це можна зробити за допомогою так званої клітки Фарадея, контейнера з металевої сітки або фольги, непроникного для радіосигналів (певних частот).

Інший спосіб отримання ізоляції від електромагнітних хвиль, альтернативний підходу Клітки Фарадея, полягає в порушенні радіоканалу. Цей метод відомий як активне глушіння радіочастотних сигналів. Це може бути зроблено за допомогою пристрою, який активно транслює радіосигнали, щоб повністю порушити радіоканал, таким чином перешкоджаючи нормальній роботі несакнціонованих зчитувачів RFID.

Як висновок, можемо зазначити, що досягнення у використанні технології RFID викликали значний інтерес у суспільстві не тільки тому, що вони принесли зміни в промисловість і бізнес, але й тому, що вони все більше впливають на наше повсякденне життя.

Уразливі місця безпеки завжди будуть серйозною проблемою під час використання систем RFID. Як і Інтернет або мобільна телефонія, RFID є технологією бездротової мережі. Хоча безконтактність систем RFID підвищують зручність і ефективність їх застосування, ці властивості також підвищують вразливість системи.

Список використаних джерел:

1. *Thornton, F, "RFID Security. Syngress Publishing, Inc", 2006.*
2. *Wyld, D. C., "RFID 101: The next big thing for management,", 2006.*
3. *Newitz, A., "The RFID hacking underground", 2006.*
4. *Juels, A., "Privacy and authentication in low-cost RFID tags", 2003.*

Медвідь І. А.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ІНФОРМАЦІЙНА БЕЗПЕКА ПРИ РОБОТІ З НЕРЕГЛАМЕНТОВАНИМИ ЗАПИТАМИ ДО БАЗИ ДАНИХ

Анотація: Зараз виробництво даних відбувається максимально швидко; однак бази даних — це колекції добре організованих даних, які можна швидко отримувати, підтримувати та оновлювати. Системи баз даних мають вирішальне значення для компанії, оскільки вони передають дані про операції з продажу, товарні запаси, профілі клієнтів і маркетингову діяльність.

Для виконання маніпулювання даними та діяльності з обслуговування розглядається система керування базами даних. Бази даних відрізняються, оскільки їхні висновки базуються на незліченних правилах про те, що являє собою невразлива база даних. У результаті шукачі захисту бази даних стикаються з труднощами з точки зору вибору фантастичної цифри для підтримки безпеки своєї бази даних. Основна мета цього дослідження полягає в тому, щоб визначити ризик і те, як ми можемо захистити бази даних, зашифрувати конфіденційні дані, змінити бази даних системи та оновити системи баз даних, а також оцінити деякі методи вирішення цих проблем у базах даних безпеки. Однак, оскільки інформація відіграє таку важливу роль у будь-якій організації, розуміння ризику безпеки та запобігання його виникненню в будь-якій системі баз даних вимагає високого рівня знань. Як наслідок, у цьому документі була пояснена вся необхідна інформація для будь-якої організації; Крім того, також обговорювався новий технологічний інструмент, який відіграє важливу роль у безпеці бази даних.

Ключові слова: безпека бази даних, атака, загрози, захист, шифрування, вразливість бази даних.

Бази даних і системи баз даних є невід'ємною частиною сучасного життя; більшість із нас щодня виконує принаймні одну діяльність, пов’язану з базою даних [1]. Просто кожен може зберігати дані та інформацію в базі даних, щоб забезпечити безпеку та захист бізнес-пристроїв. У разі надзвичайної ситуації технологія різко збільшила наші шанси на виживання. Насправді технології покращили те, як ми живемо, подорожуємо, спілкуємося, навчаємось і отримуємо медичне лікування, а також те, як ми ведемо своє життя. Технології, які використовуються в основній інфраструктурі, яка підтримує наше повсякденне життя, стають необхідністю, і без них життя було б немислимим [2]. Сучасні бази даних і цілі системи часто піддаються різноманітним ризикам безпеки. Багато з цих

ризиків поширені в малому бізнесі, але у великих підприємствах та установах вразливість є критичною, оскільки вони містять конфіденційну інформацію, яка використовується багатьма особами та відділами [3]. Це стосується захисту баз даних від певної форми небажаного доступу або небезпека на будь-якому етапі. Захист сервера передбачає дозвіл або заборону поведінки користувача щодо бази даних та її властивостей. Добре функціонуючі організації прагнули забезпечити безпеку своєї бази даних. Вони не дозволяють неліцензованому користувачеві отримати доступ до своїх файлів або документів. Вони також заявляють, що їх інформація захищена від будь-яких оманливих або ненавмисних змін. Пріоритетом безпеки є захист даних і конфіденційність [4].

У базі даних є кілька рівнів захисту. Зловмисник скомпрометує захист на всіх цих рівнях, які включають адміністратора бази даних, адміністратора сервера, спеціаліста з безпеки, розробників і співробітників [5]. Можна знайти три типи зловмисників [1]:

A. Зловмисник — це небажаний користувач, який намагається отримати корисну інформацію з комп'ютерного пристрою, надмірно маніпулюючи ним.

B. Інсайдер — це один із членів надійних користувачів, який порушує свій дозвіл і намагається отримати знання поза межами свого власного розподілу.

C. Адміністратор — це користувач із повноваженнями керувати комп'ютерною системою, який, порушуючи політику безпеки організації, зловживає своїми правами керування, шпигуючи за діяльністю систем керування базами даних і отримуючи конфіденційні дані. Коли зловмисник проникає в систему, можуть бути проведені дві з наступних атак [1]:

Прямі атаки.

Це стосується спершу націлювання на цільові дані. Ці атаки можливі й ефективні, лише якщо база даних не має механізму безпеки. Якщо ця атака невдала, зловмисник переходить до наступної.

Непрямі атаки.

Він не атакує ціль явно, проте дані від цілі або навколо неї можна отримати за допомогою інших проміжних елементів, як випливає з назви. Використовується багато варіацій різних питань, які намагаються пройти через механізм автентифікації. Важко відслідковувати ці загрози. Загалом атаки на базу даних складаються з двох типів [5]:

Пасивна атака.

У цьому випадку зловмисник просто перевіряє дані в базі даних і не вносить жодних змін. Нижче наведено кілька прикладів пасивних атак:

1. Статичний витік: ця атака отримує дані про вміст відкритого тексту бази даних шляхом аналізу знімка бази даних, зробленого в певний період.

2. Відтік інформації: у цьому випадку доступ до даних про значення відкритого тексту можна отримати, підключивши значення бази даних до розташування індексу згаданих значень.

3. Динамічний витік: Можуть бути виявлені та оцінені зміни, внесені до бази даних з часом, а також факти про значення простого тексту.

Активна атака: реальні значення бази даних змінюються під час агресивної атаки. Вони більш небезпечні, ніж пасивні атаки, оскільки можуть призвести споживачів до плутанини. Наприклад, користувач може неправильно отримати інформацію в результаті нерегламентованого запиту [5]. Існує багато способів здійснення такої атаки, які згадані нижче:

1. Підробка – у цій атаці створене значення замінюється значенням зашифрованого тексту.

2. Зрощення – передбачає заміну значення зашифрованого тексту новим значенням зашифрованого тексту.

3. Повторне відтворення – це атака, під час якої значення зашифрованого тексту замінюється старішою версією, яка була змінена або видалена раніше.

Через дані, які вони несуть, і їх розмір, бази даних є найпопулярнішою мішенню для кіберзлочинців [1]. У цій статті розглядаються різноманітні ризики та проблеми безпеки бази даних.

Інформаційну безпеку в найзагальнішому розумінні можна визначити як стан безпеки інформаційного простору, при якому неможливо завдати шкоди властивостям об’єктів безпеки, пов’язаних з інформацією та інформаційною інфраструктурою. Інформаційна безпека включає наступні основні категорії: Доступність - можливість отримання певної інформаційної послуги протягом прийнятного часу Цілісність - актуальність і узгодженість інформації, захист від знищення та несанкціонованої модифікації;

Конфіденційність - запобігання несанкціонованому доступу.

Основна загроза: розголошення інформації, компрометація або несанкціонований доступ до такої інформації.

Сервіси кібербезпеки можна вважати одним з найважливіших методів захисту:

Ідентифікація та аутентифікація, контроль доступу, журналювання та аудит, захист периметра, захист паролем. Це також включає захист від несанкціонованого видалення інформації під час передачі по технічних каналах.

Первинними джерелами витоку інформації можуть бути внутрішні або зовнішні події.

Внутрішні та зовнішні події зазвичай поділяються на випадкові та цілеспрямовані. Найпоширеніші внутрішні інциденти пов’язані з помилками середовища або навмисними діями осіб, які мають доступ до інформації: розголошення конфіденційної інформації, несанкціонований доступ до інформації, вилучення інформації, розголошення інформації, незвичайна

мережева активність. Під зовнішніми подіями слід розуміти втручання в систему осіб без прав доступу: злом або спроба злому вузлів мережі, інституційний портал або сканування мережі, вірусні атаки, несанкціонований доступ до конфіденційної інформації, атаки на відмову в обслуговуванні.

Зважаючи на те, що більшість організацій ігнорують захист конфіденційної інформації, це ускладнює повернення систем до нормального функціонування після атаки та створює потенційну загрозу для їхнього бізнесу. Отже, основними етапами захисту конфіденційної інформації є:

- аналіз вразливостей програмного забезпечення;
- призначити права доступу до бази даних
- ретельно аналізувати дані в базі даних, чітко обумовлюючи доступ до окремих елементів;
- захист паролем;
- запис;
- аналіз подій, що відбуваються під час роботи системи, з урахуванням їх загрозливого стану;
- налаштувати систему на основі аналізу подій.

Таким чином, динамічна система, яка зосереджена на обробці нерегламентованих запитів на дані від аналітиків, має вищі вимоги до інформаційної безпеки, оскільки аналітики мають повноваження більш широко оперувати з даними в базі даних. Тому основними заходами захисту від несанкціонованого доступу до даних є чітке розмежування дозволів на системні об’єкти, захист паролем, журналювання подій і аудит.

Проблеми безпеки бази даних і дослідження різних питань, що впливають на галузь, часто згадуються в цій статті. Зараз організації залежать від документів для прийняття рішень щодо різних бізнес-процесів, які покращать їхні результати. Як наслідок, це розумна ідея – захистити конфіденційні деталі від сторонніх очей. Дослідницькі роботи з безпеки серверів намагалися вивчити питання потенційних нападів на системи баз даних, такі як втрата конфіденційності та чесності. Через обсяг знань і обсягу, що міститься в базах даних, вони є найпоширенішими та простими цілями для зловмисників. Є багато варіантів розміщення бази даних. Сьогодні існує кілька форм атак і загроз, від яких слід захищати базу даних.

Список використаних джерел:

1. М. Малік і Т. Пател. «Атаки на безпеку бази даних і методи контролю». Міжнародний журнал інформаційних технологій, вип. 6, № 1/2, С. 175-183, 2016.

2. І. Гар, Дж. Салім, М. Хаммуде, Х. Фаур, В. Преносіл, С. Джаф, С. Джаббар і Т. Бейкер. «Загрози безпеці критичної інфраструктури: людський фактор». Журнал суперкомп'ютерів, вип. 74, вип. 10, стор. 4986-5002, 2018.

3. P. K. Paul і P. S. Aithal. «Безпека бази даних: огляд і аналіз поточної тенденції». Міжнародний журнал з управління та соціальних наук, вип. 4, № 2, стор. 53-58, 2019.

4. С. Б. Садхан. «Пов’язані документи». Over Rim, стор. 191-199, 2017.

5. *Х. Котарі, А. Сувалка та С. Кумар. «Різні атаки на базу даних, підходи та засоби протидії безпеці баз даних». International Journal of Advance Research in Computer Science and Management Studies, vol. 5, № 5, стор. 357-362, 2019.*

6. *J. C. Ogbonna, F. O. Nwokoma та A. Ejem. "Питання безпеки бази даних: огляд". Міжнародний журнал інженерних винаходів, вип. 6, № 8, стор. 1812-1816, 2017.*

7. *Т. Дхармакерті. «Дослідження проблем безпеки та їх вирішення». Researchgate. Net, № травень 2020 р.*

Науменко П. С.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Анотація: Сучасні технології перетворюються на важливий елемент у фінансовій торгівлі. Ми зосереджуємо увагу в цьому огляді на дослідженні електронного гаманця та онлайн-платежів, які є елементом системи електричних платежів, щоб отримати шаблон використання цієї послуги.

Це дослідження представляє огляд опублікованої інформації про електронні платежі, яка використовує якісний метод відповіді на запитання дослідження: «Які основні проблеми безпеки, пов’язані з використанням електронних платежів?» і «Яким властивостям безпеки необхідно відповідати для безпечних електронних платежів?». Завдяки підходу систематичного огляду літератури результати показують, що інтерес до електронного гаманця та онлайн-платежів значно зріс протягом цього періоду, і було виявлено, що для збільшення використання електронних платежів дослідники більше зосереджуються на питаннях безпеки.

Результати показують, що для усунення ключових прогалин електронні платежі повинні мати певні властивості захисту, а саме доступність, авторизацію, цілісність, неспростовність, автентифікацію та конфіденційність.

У наш час проблеми безпеки електронних платежів зазвичай є більш складними, ніж поточні проблеми безпеки в Інтернеті. Ці висновки можуть дозволити провайдерам електричних транзакцій посилити свої методи безпеки шляхом посилення прогалин у безпеці, як це потрібно для відповідних послуг.

Електронна платіжна система продовжує зростати протягом останніх років через дедалі більше поширення Інтернет-банкінгу та покупок. Електронні перекази — це грошові операції, які здійснюються в електронному вигляді між споживачами та роздрібними торговцями. Мільйони користувачів по всьому світу регулярно здійснюють різні платежі через Інтернет. Ці обмінні матеріали є свого роду електронними грошовими інструментами.

Системи електронних платежів викликали величезний інтерес за останні два десятиліття через життєво важливу роль, яку вони відіграють у сучасній електронній торгівлі. Згідно зі звітом Statista Fintech, у 2022 році загальний обсяг транзакцій у сегменті цифрових платежів оцінювався в 3 670 864 млн євро, а до 2023 року він, за оцінками, зросте до 5 921 831 млн євро [1]. Електронна платіжна система – це засіб оплати через електронну мережу [2], де фізична особа може оплачувати продукти та послуги онлайн

[2, 3]. Існує досить багато систем електронних платежів, які були створені в платіжному секторі по всьому світу, і в References [2, 4, 5] автори класифікували системи електронних платежів на різні категорії, а саме електронні гроші, електронний гаманець, онлайн оплата, картка тощо. У цьому дослідженні ми зосереджуємося на електронному гаманці та системі онлайн-платежів, яка є частиною електронного способу оплати, щоб зрозуміти тенденцію використання цієї системи.

Електронний гаманець — це інструмент, який фактично додатково визнано цифровим гаманцем [3]. Електронний гаманець — це програма для комп'ютерного банківського обслуговування [6], яка може збирати вашу особу та цифрові облікові дані, а також пропонує електронну або онлайн-службу, яка дозволяє окремим особам купувати в електронному вигляді [7, 8]. Оплата за допомогою електронного гаманця вважається одним із найвідоміших підходів до транзакцій на даний момент, оскільки цифрова покупка з використанням електронного гаманця має переваги простоти та адаптованості, а також захисту [4, 5]. З іншого боку, онлайн система транзакцій — це інтернет-технологія обробки грошових транзакцій, які приймаються щодня.

Онлайн-платіж — це електронний спосіб обміну платежами, який дозволяє клієнту платити онлайн-дилеру або постачальнику послуг [6]. Питання безпеки в електронних платежах сьогодні є більш складними, ніж інші поточні проблеми безпеки в Інтернеті. Під час електронних платежів клієнти повинні надати дані кредитної картки та платіжного рахунку [9] та особисту інформацію [10], і цей Інтернет-переказ є інструментом, який можна використовується для крадіжки грошей [11]. Останніми роками кілька досліджень сприяли виникненню багатьох проблем із захистом у сфері електронних платежів [7–10], де через електронні платежі клієнти повинні відчувати себе захищеними щодо своїх проблем конфіденційності [11]. Метою цього аналізу є дослідження літератури про електронний гаманець та онлайн-платіжні системи. Ми досліджуємо різні дослідження, надаючи різні передумови для дослідження та їхні взаємозв'язки. Визначаються такі дослідницькі питання: «Які основні проблеми щодо використання електронних платежів»? і «Яким властивостям безпеки необхідно відповідати для безпечних електронних платежів?».

У цій статті представлено добірку захоплюючих запитів щодо взаємозв'язку між різними загрозами транзакцій онлайн та електронного гаманця, розглядаючи можливі заходи безпеки.

Це дослідження базується на техніці систематичного огляду, яка є гідною процедурою перевірки та розуміння наявних досліджень, пов'язаних із конкретним дослідницьким питанням. Є три ключові фази систематичного огляду: підготовка огляду, керівництво оглядом і звіт про огляд. Основою плану є розробка дослідницьких питань і вдосконалення протоколу огляду,

причому найважливішою частиною систематичного огляду є протокол огляду.

Протокол огляду встановлює методи, які будуть використовуватися під час огляду. У цьому дослідженні розроблено протокол огляду на етапі підготовки. Основні компоненти протоколу перевірки включають джерела даних, стратегію збору, стратегію вибору дослідження, метод вилучення даних і синтез результатів.

Джерела даних

Дослідницькі статті, пов'язані з темою, були вибрані, щоб допомогти відповісти на запитання дослідження. Ми відхиляли нерелевантні дослідницькі роботи, які не могли відповісти чи навіть підтвердити дослідницькі запитання. Ми використовували наступні бібліотеки як наші основні ресурси, шукаючи дослідницькі публікації в:

– Science Direct (www.sciencedirect.com)•Інституті інженерів з електротехніки та електроніки (IEEE) Xplore Digital Library (ieeexplore.ieee.org)

– Асоціації для Електронна бібліотека обчислювальної техніки (ACM) (dl.acm.org)•Springer Link (link.springer.com)

– Taylor and Francis (www.taylorandfrancisgroup.com)

– MDPI (www.mdpi.com)

– GrowingScience (www.GrowingScience.com/msl)•Academia (https://www.academia.edu)

– Google schoolar (www.scholar.google.com)•Atlantis Press (www. https://www.atlantis- press.com)

Відбір даних

Відбір даних є найважливішим для систематичного перегляду будь-якого існуючого огляду дослідження, і ряд пунктів не стосувалися наших питань дослідження. Після отримання результатів використаних ключових слів ми виконали три процедури фільтрації, щоб включити критерії для пошуку. Критерії визначаються на першій фазі фільтра. Критерії відбору даних були такими:

– Чи дослідницька стаття повідомлена в будь-якому із згаданих джерел даних?

– Чи дослідницька стаття згадує або обговорює електронний гаманець або системи онлайн-платежів ?

– Чи в дослідницькій статті обговорюється будь-яка безпека, дослідження чи впровадження щодо електронного гаманця, мобільних платежів і системи онлайн-платежів?

Витяг даних

Ми проаналізували кожне попереднє дослідження, щоб визначити систему електронних платежів (EPS), електронний гаманець і дослідження, пов'язані з онлайн-банкінгом. Ми задокументували всі ідентифіковані дослідження в електронній таблиці на основі їх назви, опису та аргументації.

Більшість із них обговорювали інші електронні платіжні системи, такі як кредитні/дебетові картки чи смарт-картки, а також не змогли відповісти на запитання дослідження.

Конфіденційність

Конфіденційність надзвичайно важлива у світі електронної комерції через ймовірність того, що хакери можуть отримати конфіденційну інформацію людей. Під час електронних платежів клієнту має бути дозволено використовувати електронний банківський рахунок після ефективної верифікації. Інформація, введена клієнтом, є важкодоступною для інших клієнтів, які використовують електронний банкінг.

Конфіденційність — це гарантія того, що інформація надається виключно уповноваженим особам або компаніям. Тільки авторизований отримувач повинен мати можливість отримати зашифроване повідомлення, щоб інші не могли переглядати його вміст [8]. Вона повинна захищати конфіденційну інформацію від будь-якої неавторизованої особи, процесу чи пристрою.

Цілісність

Щоб запобігти збоям або фізичній шкоді, мережа електронних платежів потребує точних деталей. Цілісність пов'язана з достовірністю інформаційних ресурсів. Він використовується, щоб переконатися, що інформація є достатньо точною для своїх потреб. Інформація має бути повною та достовірною, гарантуючи, що інформація не буде замінена або, можливо, пошкоджена під час транзакції або, можливо, під час передачі [9]. Цілісність даних дозволить зберегти конфіденційність усіх деталей під час електричної транзакції. Інформація та пристрої не були змінені та пошкоджені зовнішніми сторонами. Дійсні облікові дані користувача зазвичай підтверджуються.

Автентифікація та неспростовність

Автентифікація — це процедура підтвердження ідентичності процедури чи, можливо, пристрою, зазвичай як передумова для дозволу використання матеріалів на продукт. Основною проблемою, на яку необхідно звернути увагу при роботі з електричним платіжним пристроєм, є автентифікація, яка ідентифікує клієнта та гарантує, що особа є тим, ким вона обіцяє бути. Для забезпечення захисту електронних покупок було створено набір методів автентифікації. Процес автентифікації важливий для того, щоб дати можливість окремим особам увійти до своїх облікових даних, і якщо вони збігаються з наявними, тоді особа є підтвердженим користувачем і їй дозволено ввійти в систему, інакше – ні.

Загалом існує три основні підходи, які використовуються для перевірки об'єктів, а саме: Один метод – це щось, що у вас є, наприклад, пристрій, маркер або картка. Другий метод полягає у використанні відомих вам точок, таких як паролі, PIN-коди тощо. Третій підхід полягає у використанні чогось біометричного [10]. Методи автентифікації, як-от індивідуальні

ідентифікатори та паролі, які ідентифікують людей, можуть допомогти досягти мети конфіденційності [11]. Однак було визначено, що автентифікація лише з одним аспектом не є надійною, щоб забезпечити достатню безпеку та безпеку через можливі ризики для безпеки [8].

Через збільшення онлайн-транзакцій однієї автентифікації недостатньо для проведення дорогих онлайн-транзакцій. З цієї причини існує потреба в ще більш надійній і безпечній системі відповідно до багатофакторної автентифікації (MFA), щоб перевіряти дійсність окремих осіб. MFA включає різні моменти, такі як, наприклад, біометричні дані, розумний мобільний пристрій, пристрій-токен разом із смарт-карткою. Ця програма автентифікації підвищує рівень безпеки, а також додатково використовує ідентифікацію, підтвердження та верифікацію для гарантування повноважень клієнта. З іншого боку, невідмова — це механізм, який гарантує, що користувач може бути впевнений, що він підключається до автентичного сервера, щоб жодна зі сторін, що спілкуються, не могла згодом некоректно спростувати факт покупки.

Стосовно електронної безпеки грошових транзакцій застосування принципу невідмовності передбачає рішення, яке надає докази стабільності, а також походження інформації, а також інструмент перевірки, який з високою гарантією може бути справжнім. Він веде журнали покупок, які часто оновлюються банками, і записує різноманітну інформацію, що включає характер, час і дату транзакцій, у яких брали участь споживачі. Ці записи також дають змогу перевірити багато завершених транзакцій. як надати докази, необхідні для будь-яких проблем, які можуть виникнути.

У цьому дослідженні було розглянуто 131 статтю, опубліковану з 2010 по 2020 рік про систему електронних платежів, а саме електронний гаманець і систему онлайн-платежів. Після вивчення цих документів ми класифікували дослідження на дві групи: дослідження електронного гаманця та дослідження онлайн-платежів. У той час як дослідження електронних гаманців показали, що електронні гаманці привертають більше уваги в електронних платежах, у центрі уваги досліджень систем онлайн-платіжів було більше зосереджено на безпеці онлайн-платежів. Аналіз вибраних досліджень показує кілька викликів і тем для майбутніх досліджень, у тому числі тих, які конкретно стосуються використання електронних платіжних систем для покращення безпеки та сумісності електронних гаманців і онлайн-платіжних систем.

Список використаних джерел:

1. Handelsblatt Statista FinTech Report 2022 — Цифрові платежі. 2022. Доступно в Інтернеті: https://work.euroforum.de/data/pdf/P1200762pc.pdf (дата перегляду 10.03.2023 р.).

2. Talom, F.S.G.; Тенге, Р.К. Вплив мобільних грошей на фінансову ефективність МСП у Дуалі, Камерун. Sustainability 2022,12, 183.

3. Subaramaniam, K.; Гардінг, Дж.М.; Коландайсамі, Р.; Джаліл, А.Б. Вплив електронних гаманців на сучасне покоління. J. Adv. рез. дин. Система керування 2022, 12, 751–759.

4. Karim, M.W.; Хаке, А.; Ульфі, М.А.; Хоссейн, М.А.; Аніс, М.З. Фактори, що впливають на використання електронного гаманця як методу оплати серед молодих людей Малайзії. J. Int. Автобус. кер. 2020,3, 1–11.

5. Абу Бакар, Н.; Росбі, С.; Узакі, К. Платформа транзакцій електронного гаманця для цифрової економіки: перспектива ісламської фінансової інженерії. Міжн. J. Manag. Sci. Автобус. Adm. 2020, 6, 50–57.

6. Choi, D.; Chung, C.Y.; Янг, Дж. Надійна логістика онлайн-покупок для задоволеності клієнтів і поведінки повторних покупок: докази з Китаю. Стійкість 2019,11.

7. Chun, S.H. Відповідальність за електронну комерцію та порушення безпеки в мобільних платежах для сталого розвитку електронного бізнесу. Сталий розвиток 2019, 11.

8. Zhang, J.; Луксимон, Ю.; Сонг, Ю. Роль сприйнятої споживачами безпеки, сприйнятого контролю, особливостей дизайну інтерфейсу та сумлінності в безперервному використанні послуг мобільних платежів. Sustainability2019,11.

9. Noor Ardiansah, M.; Чарірі, А.; Рахарджа, С. Удін Вплив безпеки електронних платежів на сприйняття споживачами електронної комерції: розширена модель прийняття технологій. кер. Sci. Lett.2020,10, 1473–1480.

10. Argimbayeva, G.; Менасрія, І.; Ельшаріф, Е.; Льюїс, А. Вплив електронного гаманця на задоволеність клієнтів ADNOC. У матеріалах 11-ї міжнародної конференції з електронної освіти, електронного бізнесу, електронного менеджменту та електронного навчання у 2020 році (IC4E 2020) — EI & Scopus, Осака, Японія, 10–12 січня 2020 р.; С. 364–368

11. Кім, С. С. Намір придбати на відкритому онлайн-ринку: чи справді проблеми з електронною комерцією мають значення? Сталий розвиток 2020, 12.

Нікітін Д. О.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

СУЧАСНА КІБЕРБЕЗПЕКА

Сучасна кібербезпека охоплює різні стратегії, технології та практики, спрямовані на захист комп'ютерних систем, мереж, даних і користувачів від несанкціонованого доступу, витоку даних та інших кіберзагроз. Вона передбачає проактивний підхід до виявлення вразливостей, зменшення ризиків та реагування на інциденти безпеки.

Ось деякі ключові аспекти сучасної кібербезпеки:

• Розвідка та моніторинг загроз:

Організації використовують передові інструменти та рішення для моніторингу своїх мереж і систем на предмет потенційних загроз. Це передбачає аналіз журналів безпеки, мережевого трафіку та поведінки системи для виявлення будь-яких підозрілих дій або ознак компрометації. Безперервний моніторинг дозволяє своєчасно виявляти кіберзагрози та реагувати на них.

• Багатофакторна автентифікація (MFA):

Для посилення безпеки організації все частіше застосовують методи багатофакторної автентифікації. MFA вимагає від користувачів надання декількох доказів для підтвердження своєї особи, таких як паролі, біометричні дані, токени або одноразові паролі. Це допомагає запобігти несанкціонованому доступу, навіть якщо один з факторів буде скомпрометований.

• Шифрування та захист даних:

Шифрування має вирішальне значення для захисту конфіденційних даних, як у стані спокою, так і під час передачі. Сучасна кібербезпека наголошує на використанні надійних алгоритмів шифрування для захисту даних від несанкціонованого доступу або перехоплення. Крім того, організації впроваджують рішення для запобігання втраті даних (DLP) для моніторингу та контролю руху конфіденційної інформації.

• Хмарна безпека:

З широким розповсюдженням хмарних обчислень безпека хмарних середовищ і даних набула особливого значення. Організації застосовують надійні заходи безпеки, включаючи контроль доступу, шифрування та регулярний аудит, щоб захистити дані, що зберігаються в хмарі. Крім того, хмарні провайдери пропонують вбудовані функції безпеки та сертифікати відповідності.

• Реагування на інциденти та обізнаність про кібербезпеку:

Організації розробляють плани реагування на інциденти, щоб ефективно реагувати на інциденти безпеки та мінімізувати їхній вплив. Це включає в себе створення процесів для виявлення, локалізації, усунення та відновлення інцидентів. Крім того, підвищення обізнаності працівників щодо кібербезпеки через тренінги та навчання має вирішальне значення для зменшення ризиків, пов'язаних з людським фактором. Важливо зазначити, що сучасна кібербезпека - це сфера, яка постійно розвивається, і організації повинні бути в курсі останніх тенденцій, технологій і передових практик, щоб ефективно захищати свої цифрові активи і системи.

ТРЕНДИ КІБЕРБЕЗПЕКИ 2023

• Підвищена увага до атак і захистів на основі ШІ:

Оскільки штучний інтелект (ШІ) продовжує розвиватися, очікується, що як зловмисники, так і захисники будуть використовувати методи ШІ. Зловмисники можуть використовувати ШІ для автоматизації та вдосконалення своїх атак, тоді як захисники використовуватимуть інструменти на основі ШІ для виявлення загроз і реагування на них.

• Зростання кількості атак та вимагань з використанням програм-вимагачів:

Атаки з використанням програм-вимагачів були значною загрозою в останні роки, і очікується, що ця тенденція збережеться і в 2023 році. Кіберзлочинці, ймовірно, застосовуватимуть більш витончену тактику і націлюватимуться на об'єкти критичної інфраструктури, організації та приватних осіб, вимагаючи більші суми викупу.

• Акцент на архітектурі нульової довіри:

Архітектура нульової довіри (ZTA) набуває все більшої популярності як система безпеки, що вимагає суворої автентифікації та авторизації для кожного користувача та пристрою, незалежно від їхнього місцезнаходження. У 2023 році організації, ймовірно, впровадять ZTA, щоб зменшити ризик внутрішніх загроз і захистити свої конфіденційні дані.

• Зростаюче занепокоєння щодо безпеки Інтернету речей:

З поширенням пристроїв Інтернету речей (IoT) уразливості безпеки в цій сфері викликають дедалі більше занепокоєння. Очікується, що зі збільшенням кількості підключених пристроїв зростатиме ризик атак на інфраструктуру Інтернету речей, таку як "розумні будинки", медичні пристрої та промислові системи.

• Посилені регуляторні норми та вимоги до дотримання:

Очікується, що уряди та регуляторні органи посилять регулювання кібербезпеки у відповідь на зростання загроз. Організаціям необхідно буде адаптуватися до більш жорстких вимог, зокрема щодо захисту даних, правил конфіденційності та звітності про інциденти. Зверніть увагу, що ці тенденції ґрунтуються на прогнозах та експертному аналізі, і фактичний розвиток подій у 2023 році може відрізнятися.

• Просунуті постійні загрози (APT):

APT-атаки - це складні та приховані кібератаки, спрямовані на певні організації або окремих осіб протягом тривалого періоду часу. Очікується, що у 2023 році APT стануть більш витонченими і використовуватимуть такі методи, як соціальна інженерія, експлойти "нульового дня" та атаки на ланцюги поставок для проникнення в мережі та витоку конфіденційних даних.

• Виклики хмарної безпеки:

Оскільки організації продовжують мігрувати свої дані та інфраструктуру в хмару, забезпечення надійних заходів безпеки набуває першочергового значення. У 2023 році проблеми з безпекою хмарних сервісів можуть виникнути через неправильні конфігурації, несанкціонований доступ, витік даних та внутрішні загрози. Організації зосередяться на впровадженні хмарних рішень безпеки та створенні надійних засобів управління ідентифікацією та доступом.

Безпека мобільних пристроїв та пристроїв Інтернету речей:

З розповсюдженням мобільних пристроїв та пристроїв Інтернету речей захист цих кінцевих точок набуває вирішального значення. У 2023 році основна увага буде зосереджена на захисті мобільних додатків, запобіганні мобільному шкідливому програмному забезпеченню та захисті пристроїв Інтернету речей від компрометації і використання в якості точок входу в мережі.

Прогалина у навичках з кібербезпеки:

Попит на кваліфікованих фахівців з кібербезпеки продовжує випереджати пропозицію, що призводить до розриву в навичках. У 2023 році організації зосередяться на ініціативах, спрямованих на подолання цього розриву, включаючи збільшення інвестицій у навчання та сертифікацію, партнерство з навчальними закладами, а також сприяння різноманітності та інклюзивності в цій галузі. Ці тенденції ґрунтуються на галузевих знаннях та прогнозах і відображають потенційні зміни в ландшафті кібербезпеки до 2023 року. Важливо залишатися в курсі останньої інформації та нових загроз, оскільки ця сфера продовжує стрімко розвиватися.

Список використаних джерел:

1. "5 Cybersecurity Preditions for 2023" by Security Boulevard (source: https://securityboulevard.com/2022/12/5-cybersecurity-predictions-for- 2023/)

2. "Fortinet Predicts Top Cybersecurity Trends for 2023" by Fortinet (source: https://www.fortinet.com/corporate/about-us/newsroom/press-releases/ 2022/fortinet-predicts-top-cybersecurity-trends-for-2023.html)

3. "Cybersecurity Trends for 2023" by Cybersecurity Insiders (source: https:// www.cybersecurity-insiders.com/cybersecurity-trends-for-2023/)

Романюк О. П.

Студент, Akademie HUSPOL s.r.o.,
м. Куновіце, Чеська Республіка

ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА

Сучасний світ все більше залежить від інформації та технологій, що її обробляють. Це створює нові виклики в області інформаційної безпеки та кібербезпеки. Важливість захисту інформації та інформаційних систем від несанкціонованого доступу, змін, знищення або блокування ніколи не була вищою.

Мета цього дослідження - вивчити сучасні підходи до інформаційної безпеки та кібербезпеки, визначити їх слабкі місця та визначити потенційні шляхи їх покращення.

На основі проведеного аналізу було виявлено декілька ключових областей, що вимагають уваги:

- Необхідність посилення заходів щодо інформаційної безпеки в сфері ІТ, зокрема через використання передових методів шифрування та аутентифікації.
- Необхідність збільшення обізнаності користувачів з питань інформаційної безпеки та кібербезпеки.
- Потреба в подальшому розвитку та вдосконаленні систем для виявлення та відновлення після кібератак.

Враховуючи швидкий розвиток технологій та постійно зростаючу кількість кіберзлочинів, інформаційна безпека та кібербезпека залишаються важливими напрямками дослідження. Потрібно активно розробляти нові методи захисту, а також працювати над підвищенням обізнаності користувачів у цій сфері.

Крім того, важливою є робота над створенням ефективних систем для виявлення та відновлення після кібератак. Також необхідно враховувати, що кібербезпека - це не лише технологічне питання, але й соціальне, оскільки велика частина кібератак використовує соціальну інженерію.

З метою вирішення цих викликів, майбутні дослідження повинні бути спрямовані на вивчення нових методів захисту інформації, а також на розвиток інструментів для виявлення та відновлення після кібератак. Дослідження повинні також зосереджуватися на розробці ефективних стратегій для підвищення обізнаності користувачів в області кібербезпеки.

Список використаних джерел:

1. Андрійчук, В. І. (2017). "Кібербезпека в Україні: стан, проблеми, перспективи". Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі. № 888. С. 11-19.

2. Кравченко, О. І. (2020). "Сучасні технології захисту інформації в комп'ютерних мережах". Вісник Харківського національного університету радіоелектроніки. Серія: Радіотехніка. Всі статті. № 1. С. 20-29.

3. Ломакін, О. В. (2018). "Методи захисту від DDoS-атак в мережах на основі протоколу IP". Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі. № 911. С. 42-51.

4. Пономаренко, В. С. (2021). "Застосування штучного інтелекту для забезпечення кібербезпеки". Вісник Національного технічного університету "ХПІ". Серія: Інформатика та моделювання. № 12. С. 76-84.

5. Чернявський, А. Ю. (2019). "Аналіз методів виявлення атак на комп'ютерні системи". Кібербезпека: освіта, наука, техніка. Випуск № 2. С. 88-98.

Dmytro Barsukov

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

LEVERAGING LARGE LANGUAGE MODELS (LLMS) FOR THREAT INTELLIGENCE: ENHANCING CYBER THREAT DETECTION AND ANALYSIS

The application of Large Language Models (LLMs) in the field of threat intelligence empowers organizations to gather, analyze, and interpret vast amounts of diverse data sources, enabling quicker and more precise detection of emerging cyber threats.

In today's digital landscape, the sheer volume and variety of data sources present a significant challenge for threat intelligence teams. Traditional methods of data collection and analysis struggle to keep pace with the ever-expanding range of information available. However, the emergence of Large Language Models (LLMs) has provided a breakthrough in the field of threat intelligence, revolutionizing the way organizations gather, analyze, and interpret data to detect and mitigate cyber threats.

LLMs, such as OpenAI's GPT-4, have demonstrated remarkable capabilities in natural language understanding and contextual comprehension. These models have been trained on vast amounts of text data, allowing them to recognize patterns, infer meaning, and generate coherent responses. Leveraging these strengths, LLMs have proven to be highly effective in processing unstructured data from diverse sources, including security reports, online forums, social media platforms, and more.

One of the key advantages of using LLMs in threat intelligence is their ability to handle large volumes of data. Traditional methods often rely on manual processing, which is time-consuming and prone to human error. In contrast, LLMs can quickly analyze and interpret massive amounts of text, sifting through vast repositories of information in a fraction of the time it would take a human analyst. This enables organizations to gather real-time insights from a wide array of sources, including previously untapped or overlooked ones.

Moreover, LLMs excel at understanding the context and nuances of language, which is crucial for effective threat analysis. Cyber threats are constantly evolving, with threat actors employing sophisticated techniques and constantly adapting their strategies. LLMs can pick up on subtle indicators and contextual cues that may indicate malicious intent, enabling organizations to identify emerging threats with greater precision. By leveraging the contextual understanding of LLMs, threat intelligence teams can stay ahead of adversaries and proactively respond to potential cyber attacks.

LLMs also offer the ability to interpret data from multiple languages and dialects. In today's interconnected world, cyber threats can originate from anywhere, making it essential to have a global perspective on threat intelligence. LLMs can analyze and interpret data in various languages, breaking down language barriers and providing a comprehensive understanding of threats on a global scale. This enables organizations to monitor and respond to cyber threats that target specific regions or linguistic communities.

The integration of LLMs with existing threat intelligence platforms and tools further enhances their capabilities. By integrating LLMs, organizations can automate data extraction, categorization, and analysis processes. LLMs can sift through vast amounts of unstructured data, extracting relevant information and categorizing it based on predefined criteria. This automation frees up human analysts to focus on higher-level tasks such as interpreting results, assessing risks, and formulating mitigation strategies. The combination of human expertise and LLM-powered automation leads to more efficient and accurate threat detection.

In this section we discuss several examples that demonstrate the application of Large Language Models (LLMs) in the field of threat intelligence, highlighting how they empower organizations to gather, analyze, and interpret diverse data sources, enabling quicker and more precise detection of emerging cyber threats.

Social Media Monitoring

LLMs can be utilized to monitor social media platforms for potential cyber threats. By analyzing the language used in posts, comments, and messages, LLMs can identify indicators of malicious intent or discussions related to cyber attacks. For example, LLMs can detect mentions of phishing attempts, malware distribution, or discussions about exploiting vulnerabilities in specific software. This real-time monitoring allows organizations to proactively respond to emerging threats and take appropriate preventive measures.

Dark Web Analysis

The dark web is a breeding ground for cybercriminal activities, including the sale of stolen data, hacking tools, and illegal services. LLMs can be trained to navigate and analyze dark web forums and marketplaces, identifying potential threats and uncovering discussions related to upcoming cyber attacks. By monitoring these platforms, organizations can gain valuable insights into emerging threats and take necessary actions to protect their assets and information.

Malware Analysis and Classification

LLMs can assist in the analysis and classification of malware samples. By examining the code, behavior, and associated documentation, LLMs can help researchers and analysts determine the nature and potential impact of a given malware. LLMs can also aid in identifying similarities between different malware strains, enabling the detection of new variants or related threats. This capability allows organizations to respond swiftly and effectively to malware outbreaks and mitigate their impact.

Threat Intelligence Reports

LLMs can automate the generation of threat intelligence reports by analyzing a wide range of sources, including security blogs, research papers, and incident reports. By summarizing and extracting key information from these sources, LLMs can assist in the creation of comprehensive reports that highlight the latest threats, vulnerabilities, and recommended mitigation strategies. This automation saves time and effort for analysts, enabling them to focus on deeper analysis and decision-making.

Natural Language Understanding for Phishing Detection

Phishing attacks continue to be a significant threat, often targeting individuals and organizations through carefully crafted emails and messages. LLMs can be trained to understand the nuances of phishing attempts by analyzing the language and structure of such messages. By flagging suspicious patterns, LLMs can assist in the identification of potential phishing attempts, enabling organizations to educate their users, implement stronger email filters, and prevent successful phishing attacks.

Vulnerability Analysis

LLMs can contribute to vulnerability analysis by processing security advisories, technical documentation, and exploit databases. By understanding the context and impact of specific vulnerabilities, LLMs can help organizations prioritize patching and mitigation efforts. LLMs can also assist in identifying potential exploit techniques or patterns, aiding in the development of effective defensive measures.

In conclusion, the application of Large Language Models (LLMs) in the field of threat intelligence represents a significant leap forward in the fight against cyber threats. LLMs empower organizations to gather, analyze, and interpret diverse data sources, providing quicker and more precise detection of emerging cyber threats. Their ability to process large volumes of data, understand context, and adapt to evolving threats makes LLMs invaluable tools for threat intelligence teams. As organizations continue to leverage LLMs in their cybersecurity strategies, the detection and mitigation of cyber threats will become more effective, enabling a safer digital environment for individuals and businesses alike.

References:

1. *Andrei Kucharavy, Zachary Schillaci, Loïc Maréchal, Maxime Würsch, Ljiljana Dolamic, Remi Sabonnadiere, Dimitri Percia David, Alain Mermoud, Vincent Lenders. Fundamentals of Generative Large Language Models and Perspectives in Cyber-Defense. March 2023. https://arxiv.org/abs/2303.12132. ArXiv:2303.12132*

2. *Takashi Koide, Naoki Fukushi, Hiroki Nakano, Daiki Chiba. Detecting Phishing Sites Using ChatGPT. June 2023. https://arxiv.org/abs/2306.05816*

3. *Benjamin Kereopa-Yorke. Building Resilient SMEs: Harnessing Large Language Models for Cyber Security in Australia. June 2023. https://arxiv.org/abs/2306.02612*

4. *Julian Hazell. Large Language Models Can Be Used To Effectively Scale Spear Phishing Campaigns. May 2023. https://arxiv.org/abs/2305.06972. ArXiv:2305.06972*

5. *Vijay Ganti, Scott Coull. Introducing AI-powered insights in Threat Intelligence. April 2023.*

6. *Stephanie Stacey. Large language models will transform corporate cybersecurity – for good and ill. May 2023*

7. *Hype vs. Reality: Are Generative AI and Large Language Models the Next Cyberthreat? May 2023.*

8. *Julien Provenzano. Harnessing LLMs for cybersecurity professionals. April 2023. https://thereadable.co/opinion-harnessing-llms-for-cybersecurity-professionals/*

9. *The Role of AI in Cyber Threat Intelligence. April 2023.*

10. *Michela Menting. Securing Artificial Intelligence in Large Language Models. May 2023. https://www.spiceworks.com/tech/artificial-intelligence/guest-article/securing-artificial-intelligence-in-large-language-models/*

Kostiantyn Chapistrak

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

6 STEPS TO SECURE SMALL BUSINESS NETWORKS

Despite their size, small businesses are vulnerable to data breaches, malware infections, and other cybersecurity threats that can result in significant financial and reputational damage. Therefore, securing small business networks has become an essential task for entrepreneurs and business owners.

In this report, we will outline six essential steps to secure small business networks. By following these steps, business owners can strengthen their network infrastructure, protect sensitive data, and mitigate the risk of cybersecurity incidents. From conducting network security audits to educating employees about best practices, each step plays a crucial role in establishing a strong defense against potential threats.

Step 1. Antivirus software

According to the United States Government Computer Security Resource Center, antivirus software is a program that monitors computers or networks to identify all major types of malware as well as prevent malware incidents. There are, once again, paid and free antivirus software.

Many of the popular free antivirus software solutions are not for commercial use and will therefore, can only be used for personal devices. Companies choosing free software must choose one that is licensed for commercial use, such as:

- Comodo Internet Security
- Nano Antivirus
- Windows Security
- ClamWin Open-Source Antivirus

For small businesses who are looking for more features, it is recommended to explore some of the paid antivirus software and again, take advantage of free trials.

- TotalAV
- Malwarebytes for Business
- SentinelOne Singularity

Step 2. Firewalls

A firewall is a device that monitors incoming and outgoing network traffic, basically creating a barrier between internal systems and external sources. This barrier should block threats such as viruses and other insider threats. There are software and hardware firewalls, and it is recommended to have both. Hardware firewalls are small devices that connect directly to devices.

There are different types of firewalls, and the choice will depend on the needs of a small business, but there are considerations and key features to consider.

- Included VPN
- Hybrid cloud support
- Unified security management
- Minimize damage
- Application inspection
- Identity-Based Inspection

Step 3. Backup Data Programs

A backup service is one that will store all of a small business's data in a secure location. If anything were to happen to the main system, the damage would be minimalized as there would be a second copy of the information.

Backups can be stored on hardware such as SD cards, USB drives, or external hard drives. For larger data storage, small companies may invest in NAS drives (Network Attached Storage), providing storage for various computers and devices. Hardware devices still need security measures such as the correct storage of devices with sensitive information, not letting devices get into the hands of those without authorized access, password protection, and encryption. These devices shouldn't be left connected and open, and they shouldn't be left alone where they could be stolen. Anti-theft and device loss apps can be installed for additional security.

An alternative to physical devices is a cloud-based solution. Cloud storage devices are managed by a third-party provider and stored in warehouses, limiting access to sensitive data. Files that are stored on cloud servers are encrypted, making it more difficult for not only internal threats but also cybercriminals. Cloud providers should have built-in firewalls, and many are now turning to artificial intelligence and built-in algorithms to detect vulnerabilities in systems.

Step 4. Encryption Software

Encryption software involves mathematical algorithms to encode data at one end and send the data so that only the intended receiver can view the data. The software takes an original piece of data and turns it into ciphertext. This looks like scrambled nonsense at this stage.

First, the message is encrypted using a public key. The private key of the receiver decrypts the message back to its original form. Any data can be encrypted, even payment cards and images. For small businesses, it's essential to encrypt:

- Financial reports
- Product release information
- Customer details
- Research
- Intellectual property

There are free encryption software providers and paid-for options, but it will always be down to the needs of a small business. Free software will likely only provide basic protection. Some important features of encryption are:

- The algorithm – AES-256 algorithm provides military-grade security.
- Device compatibility – as most small businesses have more than one device, the software should be cross-device compatible.
- Independent testing – a third party should have tested and certified the software to confirm its reliability.
- Automatic backup – a useful feature offering an extra layer of security would be the automatic backup of encrypted files.
- User-friendly – software must be simple for business owners to use so that mistakes aren't made.

Step 5. Password Security

The strength of passwords is something that should be reviewed by small businesses in order to ensure passwords aren't easy for insiders to guess. In fact, a 12-character password can take 200 years to crack (MIT, n.d.). Other recommendations for strong passwords include:

- Using a short phrase and removing the vowels
- Use acronyms
- Include punctuation symbols
- Capitalize any letter than the first
- Use acronyms of favorite songs

Passwords should be changed once a year, and no password should be used for multiple devices. Naturally, this leads to numerous passwords that are not easy for even the business owner to remember, and under no circumstances should passwords be written down. This is where password managers are an advantage. A password manager saves all passwords, and passwords can be accessed by using one password. The initial password to access all others has to be incredibly strong and should be changed frequently.

Two-factor authentication has been used for both personal and business operations, especially in the financial industry. Two-factor authentication requires an added level of security on top of a password. For example, when a small business owner logs into their bank account, they will sign in through the website, and then a code will be sent to their mobile.

Many of the major online accounts allow businesses to set up two-factor authentication, including Amazon, Apple, Dropbox, Google, Microsoft, PayPal, Slack, and various social media sites. There are also authenticator apps, such as Authy, which generate a one-time numerical passcode. After logging in to the required site, the user opens the Authy app to access their code.

Step 6. Consider Cyber Insurance

Much like a solid security policy for insider threats, cyber insurance isn't going to prevent an attack. Nevertheless, it can help to reduce the financial damage caused by insider threats. And, much like any type of insurance, cyber insurance policies are not created equal, and the fine print should be understood.

There are two main types of cyber insurance for businesses, cyber liability insurance and cyber breach insurance. A cyber liability policy covers providing

credit monitoring and identity restoration for victims and the notification of employees and customers. Policies can be customized to include income replacement, prior act coverage, and extortion payments. Some cyber insurance policies will pay to repair damage to hardware and software, and some include the paying of ransoms.

Some of the most common insurance claims include:

- Data breaches
- Cloud hacks
- E-commerce shutdown
- Account takeovers
- Phishing
- Malware

It is crucial to remember that network security is an ongoing process that requires constant vigilance and adaptation. Implementing the recommended steps is not a one-time task, but a continuous effort to stay ahead of cybercriminals. Regular network security audits, strong access controls, updated firewalls and antivirus software, data backups, employee education, and incident monitoring and response all contribute to building a resilient security framework.

Safeguarding small business networks is a shared responsibility that requires proactive measures and ongoing commitment. By implementing the six steps discussed in this report, small business owners can significantly reduce their vulnerability to cyberattacks, mitigate risks, and ensure the long-term success and stability of their businesses. Embracing network security as an integral part of business operations will enable small businesses to thrive in the digital era while safeguarding their valuable assets and maintaining the trust of their customers.

References:

1. Bambulas, N. (n.d.). How to Secure a Network for Business Computers. https://www.gflesch.com/elevity-it-blog/ways-to-secure-a-computer-network

2. Vpn, T. (2019, January 10). 5 Basic Network Security Tips for Small Businesses. Network Computing. https://www.networkcomputing.com/network-security/5-basic-network-security-tips-small-businesses

Maksym Kozachenko

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

THE TRANSFORMATIVE IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBERSECURITY

Artificial intelligence (AI), which includes complex technologies, algorithms, and machine learning methods, has recently emerged as a game-changing technology with the potential to revolutionize a wide range of industries, including the cybersecurity area.

The ability of AI to analyze large datasets, spot trends, and make intelligent decisions in real time is what has such a profound effect on cybersecurity. This paradigm change offers exciting opportunities for fending off the constantly changing cyberthreats that face governments, organizations, and people. In addition to helping with attack detection, AI also strengthens incident response capabilities and improves the gathering of threat intelligence.

The integration of artificial intelligence into defense strategies, particularly in cybersecurity, signifies a significant shift in how governments protect their interests. A great illustration is the recent publication of the comprehensive final report by the National Security Commission on Artificial Intelligence (NSCAI). One of the recommendations highlights the government's focus on the development and implementation of AI-powered defense mechanisms to effectively counter cyber attacks [1].

The race to use artificial intelligence in security is being vigorously contested by major technological companies. 'Security Copilot,' a new product from Microsoft that uses the GPT-4 generative AI model from OpenAI, has been announced. The tool, which is intended for cybersecurity professionals, has features including incident summary, vulnerability analysis, and cooperative information sharing on a pinboard. It helps identify breaches, threat signals, and data analysis [2]. As part of a new initiative they are also using AI to track and forecast Russian cyber threat [3].

Google's cloud is launching its own Security AI Workbench, which draws on generative AI models to improve threat visibility, following Microsoft's example. This comprehensive set of AI-powered solutions, which includes Mandiant Breach Analytics for Chronicle and VirusTotal Code Insight, allows for the examination of potentially malicious scripts and alerts users to ongoing system breaches [4].

The following are some possible major ways AI strengthens defenses, identifying dangers, and enabling proactive reaction measures:

- Threat Detection and Prevention: Machine learning techniques are used by AI to analyze large amounts of data and find patterns that may indicate security breaches or anomalies.
- Advanced Behavioral Analysis: AI-driven cybersecurity is excellent at detecting sophisticated attacks and insider threats that are frequently missed by traditional systems.
- Automated Vulnerability Management: AI improves the vulnerability management process by automating vulnerability scanning, patch management, and configuration analysis. Security teams can concentrate on pressing problems and reduce the exposure window to potential attackers by prioritizing vulnerabilities based on severity and probable impact.
- Intelligent Security Analytics: The combination of security analytics with AI enables businesses to extract useful information from vast amounts of security data. AI finds trends and probable indicators of compromise (IoCs) by analyzing log files, network traffic, and other data.
- Self-Learning Systems: AI makes it possible for cybersecurity systems to change and improve over time as a result of new threats. Industries can keep ahead of emerging cybercriminal methods thanks to continuous monitoring and analysis that enables AI systems to identify new attack routes and upgrade defense mechanisms accordingly.
- Human-Machine Collaboration: By automating routine operations, AI improves human capabilities in cybersecurity. Security experts may now concentrate on strategic and difficult tasks like threat analysis, incident handling, and security orchestration.

AI has significantly changed the way threats are identified, halted, and dealt with in the cybersecurity industry. It could greatly improve cybersecurity defenses and safeguards. But it's important to realize that AI has two sides since malicious actors might employ it to launch complex cyberattacks. Governments and organizations must be proactive in putting AI-powered safeguards in place while also being aware of potential risks as AI advances.

References:

1. National Security Commission on Artificial Intelligence's (NSCAI) https://www.nscai.gov/2021-final-report/

2. Microsoft News Center (March 28, 2023) https://news.microsoft.com/2023/03/28/with-security-copilot-microsoft-brings-the-power-of-ai-to-cyberdefense/

3. Microsoft On the Issues. (Jun 22, 2022). https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

4. Google Cloud Blog (April 24, 2023) https://cloud.google.com/blog/products/identity-security/rsa-google-cloud-security-ai-workbench-generative-ai

Viktor Moskvych

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

SECURITY WITH CLOUD SERVICES

Cloud services play a crucial role in ensuring and enhancing cloud security in companies. Here are several ways in which cloud services contribute to achieving robust security measures:

1. Physical Security: Cloud service providers (CSPs) maintain highly secure data centers with strict access controls, surveillance systems, and have the resources to prevent physical theft of data, including security guards, locked cages for servers, and other state-of-the-art physical security controls that most organizations do not have [1].

2. Data Encryption: Cloud services often provide built-in encryption mechanisms to protect data both in transit and at rest. Encryption ensures that even if unauthorized parties gain access to the data, they cannot read or interpret it without the encryption keys.

3. Access Control: Cloud services enable granular access control mechanisms, allowing companies to manage user permissions and restrict access to sensitive resources. They offer features such as multi-factor authentication (MFA), role-based access control (RBAC), and identity and access management (IAM) to enforce proper authentication and authorization processes.

4. Network Security: Cloud services employ robust network security measures, including firewalls, intrusion detection systems (IDS), and distributed denial-of-service (DDoS) protection. These measures help safeguard against unauthorized access, network attacks, and other malicious activities.

5. Patch Management: Cloud service providers take responsibility for system updates and security patch management. By promptly applying security patches and updates to their infrastructure, they ensure that potential vulnerabilities are addressed, reducing the risk of exploitation.

6. Threat Monitoring and Detection: CSPs often have advanced security monitoring systems in place, continuously monitoring the infrastructure and applications for suspicious activities or potential security breaches. These systems employ techniques like log analysis, machine learning, and anomaly detection to identify and mitigate security threats.

7. Disaster Recovery and Data Backups: Cloud services typically offer robust disaster recovery and backup solutions. They ensure that data is regularly backed up and can be restored in case of accidental data loss, system failures, or other unforeseen incidents.

8. Compliance and Auditing: Many cloud services comply with industry-recognized security standards and regulations, such as ISO 27001, SOC 2, HIPAA,

or GDPR [2]. By adhering to these standards, they help companies meet their compliance requirements and undergo audits to ensure the security of their data.

9. Scalability and Redundancy: Cloud services provide scalability and redundancy features, allowing companies to distribute their data and applications across multiple servers and regions. This redundancy helps ensure continuous availability of resources and mitigates the impact of localized outages or hardware failures.

10. Security Expertise: Cloud service providers have dedicated security teams with expertise in managing and mitigating various security risks. They stay up to date with the latest security threats and employ best practices to protect their infrastructure and customer data.

By leveraging cloud services, companies can benefit from the security measures implemented by reputable and experienced cloud service providers. However, it's important to note that while cloud services can enhance security, organizations also have a shared responsibility to implement proper security practices and configure their cloud environments securely.

While cloud services offer numerous benefits for enhancing security, there are certain cases where it may not be the best choice to opt for the cloud to ensure security for your service. Consider the following scenarios:

1. Highly Sensitive Data: If your organization deals with highly sensitive data, such as classified government information or trade secrets, you may have rigorous security requirements that cannot be fully met by a third-party cloud provider. In such cases, organizations may choose to keep sensitive data on-premises or within a private cloud environment with stricter control over security measures [3].

2. Regulatory Compliance Limitations: Some industries or regions have specific regulatory compliance requirements that may pose challenges when using cloud services. For example, certain data protection regulations may restrict the transfer of personal data across borders. If compliance requirements cannot be met within the cloud provider's infrastructure or jurisdiction, alternative solutions may be necessary.

3. Customized Security Controls: Organizations with complex security requirements or specific security frameworks in place may find it challenging to implement and customize those controls within a cloud environment. The flexibility to tailor security measures to unique organizational needs may be limited in a cloud service, making an alternative security approach more appropriate.

4. Limited Internet Connectivity or Reliability: If an organization operates in areas with limited internet connectivity or unreliable network infrastructure, relying on cloud services for security may pose challenges. In such cases, local security measures or hybrid solutions that combine on-premises security with cloud services may be more suitable.

5. Cost Considerations: While cloud services can offer cost savings, in certain cases, the cost of utilizing cloud services for security may outweigh the benefits. Organizations with limited budgets or cost constraints may need to evaluate the financial feasibility of relying on cloud services versus alternative security solutions [4].

6. Vendor Dependency and Lock-in Concerns: Depending heavily on a single cloud service provider for security can create a dependency and potential lock-in. Organizations may be concerned about vendor lock-in and prefer to maintain more control and flexibility over their security measures by utilizing a mix of on-premises and cloud-based solutions [5].

It's crucial for organizations to conduct a thorough analysis of their specific security requirements, compliance needs, budget constraints, and the suitability of cloud services before making a decision. In some cases, a hybrid approach combining both cloud and on-premises solutions may provide the optimal balance between security, compliance, and control.

In conclusion, while cloud services offer numerous benefits for enhancing security, there are cases where alternative solutions may be more suitable. Organizations dealing with highly sensitive data, facing regulatory compliance limitations, requiring customized security controls, operating in areas with limited connectivity, facing cost considerations, or concerned about vendor dependency may find that relying solely on cloud services for security is not the best choice.

It is crucial for organizations to carefully evaluate their specific security requirements, compliance needs, and budget constraints when considering cloud services for security. They should weigh the advantages offered by cloud services against their unique circumstances and potential limitations.

In certain scenarios, a hybrid approach that combines on-premises security measures with selected cloud services may provide the optimal balance. This approach allows organizations to retain control over sensitive data, tailor security controls to their specific requirements, and mitigate concerns related to compliance, connectivity, cost, and vendor dependency.

Ultimately, the decision to opt for cloud services or alternative security solutions should be based on a comprehensive assessment of the organization's specific needs and risk tolerance. By carefully evaluating the pros and cons, organizations can make informed decisions that align with their security objectives and provide an optimal balance between security, compliance, control, and cost-effectiveness.

***References*:**

1. "6 security benefits of cloud computing environments", https://www.redhat.com/en/ resources/six-ways-cloud-security-checklist

2. "Compliance offerings", https://cloud.google.com/security/compliance/offerings

3. "Is Cloud Security a Safe Bet for Highly Sensitive Government Data?", https://securityintelligence.com/is-cloud-security-a-safe-bet-for-highly-sensitive-government-data/

4. *"To the Cloud or not to the Cloud?", https://ita.co.nz/to-the-cloud-or-not-to-the-cloud/*

5. *"White Paper: Cloud Security: Basic Principles", Salam Ismaeel, 2016, https://www.researchgate.net/profile/Salam-Ismaeel/publication/301348543_White_Paper_Cloud_Security_Basic_Principles/links/5743b0d008aea45ee84d13de/White-Paper-Cloud-Security-Basic-Principles.pdf*

Oleksii Nechytailo

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

A GENERAL APPROACH TO THE STEGANALYSIS METHODS USAGE

Steganography is a technique of hiding information within a file or message in the way that it is not visible to human. There are five types of steganography: image steganography, text steganography, audio steganography, network steganography, video steganography.

The vast majority of the research in the steganalysis field focuses on solving the main problem: determining the fact of information presence in the container, hidden by steganography.

Methods of steganalysis could be separated into two main categories:

1. Methods that are designed to work only with previously known steganographic algorithms.

2. "Blind" or universal methods — designed for all steganography algorithms.

The methods of both categories are built taking into account the assumption of the unavailability of the original empty container, which was used to include information in the studied stegocontainer.

In addition, steganalysis by "blind" methods most often does not require knowledge of the information inclusion algorithm that was used, encryption algorithm, compression, key and message length.

Directed steganalysis methods are developed for specific steganography algorithms that are already known. Usually, they give better results compared to universal methods.

The main advantage of the universal methods is the possibility of working with known and unknown steganographic algorithms.

Known methods of "blind" steganalysis are usually built on algorithms that require preliminary "training" on sequences from filled and empty containers.

Various methods are used to determine the presence of hidden information in the container. Statistical algorithms are commonly used for this. The main part in such methods is the statistical model of the unknown empty container. Parameters and characteristics that are the most sensitive to the inclusion of hidden information are found in the built model. The probability of the presence of a secret message is determined by the discrepancy between the theoretical model and the studied container.

In general, detecting the presence of hidden data in the flow of information is one of the actual issues of computer security.

References:

1. Roja Ramani Adapa, Naga Lakshmi Nelapat. Reliable Data Transmission Using Steganography. LAP LAMBERT Academic Publishing, 2018. 104 p.

2. Mayuri Bhamare What is Steganalysis? https://www.linkedin.com/pulse/what-steganalysis-mayuri-bhamare/

3. Jim Bartel Steganalysis https://www.giac.org/paper/gsec/707/steganalysis-overview/101589

Maksym Proniaiev

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

INFORMATION AND CYBER SECURITY IN RELATION TO MODERN NATIONAL SECURITY

While protecting the National security - defending nation's interests, sovereignty, and citizens from internal and external threats - security specialists in the modern world are also required to think about cybersecurity. Intelligence gathering, maintenance of defense capabilities, law enforcement, diplomacy, and emergency preparedness - all of this now involves the internet and tech in one or other way.

Information security, also known as cybersecurity, is a critical aspect of modern society that focuses on protecting information systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. In the modern world, where information is increasingly stored and transmitted digitally, the need for robust information security measures has become greater than ever. Attackers can exploit vulnerabilities in software, hardware, or human behavior to gain unauthorized access to systems, steal sensitive data, disrupt critical infrastructure, or launch large-scale cyberattacks.

Threats can range from malicious hackers and cybercriminals to state-sponsored cyber espionage and warfare. Businesses and industries can suffer financial losses due to theft of intellectual property, disruption of operations, or ransom demands. Nation-states and cybercriminals may target government agencies, research institutions, or private companies to gain access to valuable information. State-sponsored cyberattacks or cyber espionage can strain international relations and undermine trust between nations, lead to diplomatic tensions and escalations.

Great example of cybersecurity in the real world is the protection of critical infrastructure. Critical infrastructure refers to the systems that are essential for the functioning of a society. Such as energy grids, transportation networks, and communication systems. A successful cyberattack on critical infrastructure can have severe consequences, such as power outages, transportation disruptions, or compromised emergency response capabilities. One notable example is the 2015 cyberattack on Ukraine's power grid, which resulted in widespread power outages and affected thousands of people [1].

Another example is the protection of military and defense systems. Cyberattacks targeting military can compromise command and control capabilities, disrupt communication channels, or steal sensitive military information. Such attacks can undermine a nation's defense capabilities and compromise its ability to respond effectively to threats.

One notable success is the Stuxnet worm, a cyber weapon believed to have been developed jointly by the United States and Israel. Stuxnet was specifically designed to target Iran's nuclear program, causing significant damage to its uranium enrichment facilities. This successful cyber operation demonstrated the potential of cyber capabilities in disrupting and delaying the development of nuclear weapons [2].

One prominent failure example is the 2017 NotPetya cybe attack, which initially targeted Ukraine but quickly spread globally, affecting numerous organizations and causing billions of dollars in damages. NotPetya exploited vulnerabilities in software updates to spread rapidly and disrupt critical systems, including those of multinational companies and government agencies. [3].

Successful cyber operations, such as the Stuxnet worm, have demonstrated the potential of cyber capabilities in achieving national security objectives. However, failures, like the NotPetya attack, highlight the vulnerabilities and challenges nations face in protecting their digital infrastructure.

In response to these challenges, organizations and governments have developed comprehensive strategies and frameworks to address information security concerns. For instance, the National Institute of Standards and Technology (NIST) in the United States has developed a widely adopted cybersecurity framework that provides guidelines for organizations to manage and mitigate cyber risks [4]. Similarly, the International Organization for Standardization (ISO) has developed the ISO/IEC 27001 standard, which provides a systematic approach to managing information security risks [5].

Many modern technologies such as machine learning algorithms and artificial intelligence techniques are also employed to enhance the speed and accuracy of threat detection and response [6].

Innovations in secure hardware and firmware address vulnerabilities at the foundational level of computing systems include the development of secure processors, trusted platform modules (TPMs), and secure boot mechanisms. They provide a hardware-based foundation for secure computing, protecting against firmware-level attacks and ensuring the integrity of system components. By mitigating the risk of supply chain attacks and tampering, secure hardware and firmware bolster the security of national security systems [7].

Cyber threat hunting is an innovative approach that goes beyond traditional security measures by actively searching for and identifying cyber threats within networks and systems. This proactive approach involves the use of advanced analytics, behavioral analysis, and automation to detect and respond to threats in real-time. By actively seeking out indicators of compromise and potential vulnerabilities, cyber threat hunting enhances the ability to detect and neutralize threats before they cause significant damage [8].

Zero Trust Architecture (ZTA) is another paradigm shift in cybersecurity that assumes no trust in any user or device, regardless of their location within the network. This innovative approach focuses on verifying and validating every

access request, regardless of whether it originates from inside or outside the network perimeter. ZTA helps prevent lateral movement within networks and limits the potential impact of a compromised user or device. By implementing strict access controls and continuous authentication, ZTA enhances the security posture of national security systems [9].

And integration of digital technologies into critical infrastructure and industrial control systems necessitates innovations in cyber-physical systems security. Innovations in this area focus on securing the convergence of physical and digital systems, such as power grids, transportation networks, and manufacturing facilities. This includes the development of secure protocols, anomaly detection systems, and secure communication channels to protect against cyberattacks on physical infrastructure. [12].

In conclusion, information security, or cybersecurity, is a vital discipline that focuses on protecting information systems, networks, and data from unauthorized access and cyber threats and heavily employed even by governments. Reflecting the evolving nature of cyber threats Innovations in cybersecurity within the national security sphere have significantly advanced the ability to protect critical infrastructure, defense systems, and sensitive information. Threat intelligence and analytics, cyber threat hunting, zero trust architecture, secure hardware and firmware, cyber-physical systems security are among the notable innovations that have emerged.

References:

1. SANS Institute. (2016). Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Incident Response Summary Report: Ukraine Cyber Attack. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/documents/Summary%20Report%20on%20Ukraine%20cyber%20attack.pdf

2. Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown.

3. US-CERT. (2017). Alert (TA17-181A): Petya Ransomware. Retrieved from https://us-cert.cisa.gov/ncas/alerts/TA17-181A

4. National Institute of Standards and Technology (NIST). (2014). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov/cyberframework

5. International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements.

6. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

7. McMillan, R. (2019). Secure Hardware and Firmware: Building a Foundation of Trust. In Cybersecurity Blue Team Toolkit (pp. 1-20). Apress.

8. Bollinger, T. B., & Stevens, D. (2019). Cyber Threat Hunting: An Evolving Approach to Cyber Defense. Journal of Information Warfare, 18(2), 1-14.

9. Kindervag, J. (2010). Implementing a Zero Trust Architecture. Forrester Research.

10. Zhu, Q., & Saadawi, T. (2011). A Survey of Attacks and Countermeasures in Cyber-Physical Systems. ACM Computing Surveys, 43(4), 26:1-26:37.

Maksym Protsenko

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

INCORPORATING PRIVACY BY DESIGN: ENHANCING DATA PROTECTION IN TECHNOLOGY SOLUTIONS

In the current interconnected digital landscape, privacy concerns have become a paramount aspect of information security and data management. To address these concerns, organizations are progressively recognizing the importance of adopting proactive measures to protect personal data. The paper presents a detailed exploration of the Data Protection by Design concept. This framework advocates for integrating privacy considerations throughout the design and development of technology solutions.

Drawing from extensive research from sources such as Google Scholar, NIST (National Institute of Standards and Technology), and scientific publications, this paper provides a comprehensive overview of Data Protection by Design principles and methodologies [1],[2]. It emphasizes the need for organizations to embed privacy controls and safeguards from the initial stages of system development. By incorporating privacy as an integral component, organizations can proactively address privacy risks, ensure compliance with privacy regulations, and foster a culture of responsible data handling.

Privacy design strategies and techniques are crucial to Data Protection by Design. Anonymization, pseudonymization, and data minimization are recognized as effective approaches for preserving privacy while allowing for legitimate data processing [3], [4]. Anonymization techniques, such as removing or encrypting identifiable information, ensure that data cannot be directly linked to individuals. Pseudonymization replaces identifiable data with pseudonyms, protecting individuals' identities while still allowing for data analysis. Data minimization involves collecting and retaining only the necessary data, reducing the overall exposure and potential impact in case of a privacy breach.

Moreover, cryptographic techniques and privacy-enhancing technologies are pivotal in protecting sensitive data and mitigating privacy risks. Encryption ensures that data remains unreadable to unauthorized individuals, even if it is intercepted or accessed illicitly. Privacy-enhancing technologies, such as differential privacy, allow organizations to perform aggregate analysis on data while preserving individual privacy [5].

Software engineering practices significantly influence the successful implementation of Data Protection by Design. Integrating privacy requirements into the software development life cycle ensures that privacy considerations are prioritized alongside functionality [6]. Collaboration between developers, privacy

professionals, and legal experts is crucial to identify and address privacy risks throughout development. By adopting privacy-aware coding practices, secure development methodologies, and comprehensive testing, organizations can ensure that privacy is inherent in their technological solutions.

However, balancing privacy and functionality remains a challenge in the design of technology solutions. Organizations must find ways to protect privacy without hindering the usability and functionality of their systems. User-centric design principles can assist in striking this balance by considering user expectations, preferences, and privacy requirements. Additionally, privacy impact assessments are vital in assessing the privacy implications of system design choices. By conducting these assessments, organizations can identify potential privacy risks, implement appropriate controls, and make informed decisions about system design [7].

Implementing privacy by default settings is another critical aspect of Data Protection by Design. This approach ensures that privacy measures are automatically applied and requires individuals to take deliberate action to expose their data further. By default, systems should protect user privacy, only sharing data when explicitly authorized. This helps reduce the reliance on user actions and promotes privacy as the default setting.

Through the analysis of case studies and successful examples of incorporating privacy features into products and services, this research highlights the tangible benefits and practical implementation of Data Protection by Design. It provides insights into how organizations can effectively protect personal data, ensure regulatory compliance, and build trust with their stakeholders.

As organizations navigate a rapidly evolving privacy landscape, integrating privacy considerations becomes increasingly crucial. This research provides a foundation for cybersecurity professionals, Chief Security Officers, and technology leaders to understand and implement Data Protection by Design principles. By adopting this proactive approach to privacy, organizations can safeguard personal data, demonstrate commitment to privacy best practices, and protect the interests of individuals in an interconnected digital world.

In conclusion, Data Protection by Design offers a comprehensive framework for embedding privacy considerations into technology solutions. By integrating privacy controls and safeguards from the early stages of system development, organizations can proactively address privacy risks, ensure compliance with privacy regulations, and foster responsible data handling practices. Privacy design strategies, cryptographic techniques, and privacy-enhancing technologies play vital roles in protecting personal data. Additionally, software engineering practices, user-centric design principles, privacy impact assessments, and privacy by default settings are essential in striking a balance between privacy and functionality. Through the adoption of Data Protection by Design principles, organizations can uphold privacy rights, build trust with stakeholders, and navigate the complex landscape of privacy regulations.

References:

1. Cavoukian, A. (2010). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada.

2. NIST. (2017). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

3. Sweeney, L. (2002). k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems.

4. EU GDPR. (2016). General Data Protection Regulation. EU. https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html

5. Dwork, C. (2006). Differential Privacy. 33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006).

6. Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. Cambridge Handbook of Artificial Intelligence.

7. Wright, D., & De Hert, P. (2012). Privacy Impact Assessment. Springer.

Mykola Radahuz

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

USAGE OF CELLULAR AUTOMATA IN CYBER SECURITY

What is Cellular Automata

Cellular automata (CA) are mathematical models used to simulate complex systems using simple rules. They were originally conceptualized by John von Neumann and later popularized by Stephen Wolfram.

A cellular automaton consists of a grid of cells, which can be in one or more dimensions, where each cell has a state. The number of possible states can be two (as in binary, 0 and 1) or more. The grid can be of any arbitrary finite size or infinitely large.

Each cell in a cellular automaton updates its state based on the states of its neighboring cells according to a predetermined set of rules. These updates occur at discrete time steps, meaning that all cells update simultaneously.

One of the most famous cellular automata is the "Game of Life" invented by British mathematician John Horton Conway. In this cellular automaton, the grid is two-dimensional, each cell has two states (alive or dead), and the rules involve the number of 'alive' neighboring cells.

Cellular automata have been used in a wide range of fields including physics, mathematics, theoretical biology, microstructure modeling, computer science, and cybersecurity, among others.

Cellular Automata (CA) possess several properties that make them attractive for applications in cybersecurity:

Parallelism: Cellular automata operate in parallel, making them suitable for high-performance computing environments. In a world where threats are increasingly complex and voluminous, the ability to process data and make decisions in parallel is a significant advantage.

Simple Rules, Complex Behavior: Despite being governed by simple, local rules, cellular automata can produce complex, global behavior. This property can be useful in encryption and cryptographic systems where simple operations (like XOR, AND, etc.) can create complex ciphertexts, making it difficult for an adversary to reverse-engineer the original message.

Determinism: The behavior of a cellular automaton is completely deterministic and depends only on its initial state. This makes them reliable and predictable, which is an essential property for any cryptographic system.

Discreteness: Cellular automata are discrete both in space and in time, which aligns well with the digital nature of modern computing systems.

Suitability for Non-linear Functions: CA can be used to design complex non-linear functions, which are key components in modern cryptographic algorithms. Non-linear functions are often desirable in cryptography as they provide resistance against certain types of attacks.

Pseudorandom Number Generation: Some cellular automata, like Wolfram's Rule 30, are capable of generating sequences that appear random and pass many tests for statistical randomness. Pseudorandom number generators are a crucial part of many cryptographic systems, used in key generation, encryption algorithms, and more.

Reversibility: Some cellular automata are reversible, meaning they can be run backward, returning to their initial state. This property is particularly useful in the design of certain types of cryptographic algorithms, like symmetric key ciphers.

Scalability: Cellular automata can be easily scaled, which can be useful in the context of securing large networks or systems.

Usage of Cellular Automata in Cybersecurity

Pseudorandom Number Generation: Cellular Automata are used in generating random numbers for encryption algorithms. The capability of CA to produce long sequences of complex patterns makes it a robust tool for creating pseudorandom number generators (PRNGs). PRNGs are a critical component of encryption systems, as they produce the keys used for encryption and decryption. The strength of the encryption depends significantly on the randomness of these keys. Therefore, the complex patterns produced by CA contribute to the generation of robust and unpredictable keys, enhancing the security of the encryption system. [3]

Block Cipher Systems: Cellular Automata are also used in block cipher systems. In a block cipher, the plaintext is broken into blocks, and each block is encrypted individually using a symmetric key. CA-based block cipher systems provide several advantages. Due to the parallel nature of CA, these systems can be highly efficient and can be implemented in both software and hardware. They also offer excellent resistance to linear and differential cryptanalysis attacks, which are common methods used to break cipher systems. [4]

Infrastructure Security: Cellular Automata are used in the modelling and prediction of cyber-attacks on infrastructure systems. By modelling the behaviour of these systems and potential attacks, security professionals can develop more effective countermeasures and enhance the overall resilience of the infrastructure to attacks. [6]

Network Security: Cellular automata have also been employed in modeling the cybersecurity of distributed networks like smart grids. These grids can be vulnerable to malicious attacks that spread like infections, and cellular automata can be used to model and understand these potential threats, thus aiding in the design of countermeasures.

Ideas for Security Training Gamification Using Cellular Automata

Cellular automata, with their ability to simulate complex systems through simple, local interactions, have emerged as a valuable tool in the field of cybersecurity. Their properties of parallelism, scalability, and adaptability make them ideal for designing robust and efficient security algorithms.

In the context of cryptography, cellular automata have been effectively used to design encryption algorithms, like the "Throughput Optimized Reversible Cellular Automata Based Security Algorithm", which produces enhanced throughput in cryptographic applications and creates plaintext blocks immune to other blocks during cryptanalysis. These encryption systems are scalable and can handle high-performance systems with many cores of CPU or GPU.

Moreover, cellular automata have been employed in modeling the cybersecurity of distributed networks like smart grids, which are vulnerable to malicious attacks. In such cases, cellular automata can aid in the design of countermeasures by helping understand the spread of potential threats.

Despite the promising applications, further research and exploration are needed to unlock the full potential of cellular automata in cybersecurity. Areas like network security, intrusion detection, and more can benefit from the unique properties of cellular automata. Engaging and interactive approaches, such as gamification, could also be used to educate people about the role and importance of cellular automata in cybersecurity.

In conclusion, cellular automata represent a promising area in cybersecurity, with potential applications in a range of fields. Their unique properties can contribute to the development of more robust, efficient, and scalable security systems.

Cellular automata, with their ability to simulate complex systems through simple, local interactions, have emerged as a valuable tool in the field of cybersecurity. Their properties of parallelism, scalability, and adaptability make them ideal for designing robust and efficient security algorithms.

In the context of cryptography, cellular automata have been effectively used to design encryption algorithms, like the "Throughput Optimized Reversible Cellular Automata Based Security Algorithm", which produces enhanced throughput in cryptographic applications and creates plaintext blocks immune to other blocks during cryptanalysis. These encryption systems are scalable and can handle high-performance systems with many cores of CPU or GPU.

Moreover, cellular automata have been employed in modeling the cybersecurity of distributed networks like smart grids, which are vulnerable to malicious attacks. In such cases, cellular automata can aid in the design of countermeasures by helping understand the spread of potential threats.

Despite the promising applications, further research and exploration are needed to unlock the full potential of cellular automata in cybersecurity. Areas like network security, intrusion detection, and more can benefit from the unique properties of cellular automata. Engaging and interactive approaches, such as

gamification, could also be used to educate people about the role and importance of cellular automata in cybersecurity.

In conclusion, cellular automata represent a promising area in cybersecurity, with potential applications in a range of fields. Their unique properties can contribute to the development of more robust, efficient, and scalable security systems.

References:

1. "Throughput Optimized Reversible Cellular Automata Based Security Algorithm" - A study on a high-performance encryption algorithm based on reversible cellular automata, showing improved throughput and robustness in cryptanalysis [1](https://www.mdpi.com/2079-9292/11/19/3190).

2. "Cyber security of smart grids modeled through epidemic models in cellular automata" - Discusses the vulnerability of smart grids due to their distributed management, and how an adversary could spread digital attacks like an infection [2](https://ieeexplore.ieee.org/abstract/document/7523560).

3. "Cryptography with cellular automata" - Discusses the application of cellular automata in cryptography, presenting it as a dynamic system where space and time are discrete [3](https://www.bing.com/search?q=cellular+automata+in+cybersecurity).

4. "Application of Cellular Automata for Cryptography" - A volume discussing new results in the application of cellular automata for cryptography [3](https://www.bing.com/search?q=cellular+automata+in+cybersecurity).

5. "Image encryption using cellular automata" - Discusses the use of cellular automata in image encryption (unable to access full details).

6. "Cellular automata for intrusion detection" - Discusses the use of cellular automata for intrusion detection (unable to access full details).

7. "Cellular automata and information" - Discusses cellular automata and its role in information security in the context of wireless sensor networks (unable to access full details)

Ihor Roid

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

INCIDENT MANAGEMENT IN SCOPE OF ENTERPRISE INFORMATION SECUTIRY

In today's complex and interconnected world, incidents are an inevitable part of any organization's journey. While some risks can be anticipated and mitigated through proactive strategies, others materialize unexpectedly, challenging even the most well-prepared entities. In this article, we will explore how risks can escalate into incidents due to flawed strategies. We will also delve into effective approaches for dealing with incidents, including mitigation, measuring potential losses, tradeoffs, and decision-making processes.

From Risks to Incidents:

Foreseen risks are those that are identified and acknowledged in advance, allowing organizations to develop strategies to prevent or mitigate their impact. However, despite having a forewarning, incidents can still occur if strategies are inadequate or poorly executed. There are several ways in which foreseen risks can turn into incidents:

Ineffective risk management: A flawed risk management approach can undermine the effectiveness of strategies. This could involve underestimating the severity of a potential risk, neglecting critical vulnerabilities, or inadequately allocating resources for risk mitigation. Without robust risk management, incidents are more likely to occur, leading to disruptions, financial losses, and damage to the organization's reputation.

Insufficient contingency planning: While strategies are devised to prevent or minimize the impact of foreseen risks, incidents can still unfold if contingency plans are lacking or poorly designed. Contingency plans should outline a clear set of actions to be taken when an incident occurs, including predefined roles and responsibilities, communication protocols, and recovery procedures. Failure to have robust contingency plans in place can exacerbate the consequences of incidents, hampering the organization's ability to respond effectively.

In contrast to foreseen risks, unforeseen risks are those that arise unexpectedly, catching organizations off guard. These risks can naturally evolve into incidents due to their unforeseeable nature or insufficient study of the problem area. Some reasons why unforeseen risks turn into incidents include:

Emerging threats and vulnerabilities: The evolving landscape of technology, geopolitical dynamics, and societal changes can introduce new risks that were previously unknown or underestimated. The emergence of cyber threats, for example, has caused numerous incidents across industries. When faced with

previously unforeseen risks, organizations must quickly adapt their strategies and response mechanisms to address the new challenges.

Cascading effects: Unforeseen incidents can occur as a result of interconnected systems or cascading failures. An incident in one part of a complex network or supply chain can trigger a chain reaction, amplifying the impact and leading to widespread disruptions. These incidents highlight the importance of understanding the interdependencies within systems and the need for comprehensive risk assessments that consider potential ripple effects.

Dealing with Incidents: Strategies, Mitigation, and Decision-making

Incident response planning: Organizations should establish robust incident response plans that outline clear procedures, roles, and communication channels. This includes establishing incident response teams, defining escalation protocols, and conducting regular drills to test the effectiveness of the plans.

Mitigation measures: Alongside incident response planning, proactive measures should be taken to mitigate the impact of incidents. This can involve implementing security measures, redundancies, and backup systems, as well as regularly monitoring and assessing potential risks. Timely detection and containment can significantly reduce the impact of incidents.

Measuring potential losses: Quantifying potential losses associated with incidents is crucial for informed decision-making. Organizations should develop methodologies to estimate the financial, operational, and reputational costs of different types of incidents. This information can guide resource allocation and prioritize mitigation efforts.

Tradeoffs and Decision-making: Incident management often requires making difficult tradeoffs. Organizations must consider factors such as cost, operational disruptions, customer impact, and regulatory compliance when making decisions. Balancing short-term incident resolution with long-term organizational goals is crucial for effective decision-making.

There are three phases of dealing with incidents:

- Pre-incident phase, at which an incident management framework is built and tested
- Ongoing incident phase, when measures are taken to stop the emerged problem from bringing more damage.
- Post-incident phase, that includes retrospective analysis of the incident and taking measures as to the future strategy, whether it’s simply accepting the risk of an incident recurrence or taking actions to either lower their probability or to simplify their management.

Preparation for an incident as an inevitable risk.

Effective incident management is crucial to minimize the impact of these events and ensure a swift and efficient resolution. To effectively manage incidents, organizations need a well-defined framework that establishes clear roles, responsibilities, and processes. Key elements of an incident management framework include:

a. Incident Response Team: Assemble a dedicated team comprising individuals from relevant departments, including IT, operations, communications, legal, and senior management. Assign specific roles and responsibilities to team members to ensure a coordinated response.

b. Incident Escalation and Communication: Develop escalation procedures to ensure incidents are promptly escalated to the appropriate level of management. Establish effective communication channels both internally and externally to ensure all stakeholders are informed and updated throughout the incident lifecycle.

c. Incident Categorization and Prioritization: Implement a system for categorizing incidents based on severity and impact. This allows for prioritization of response efforts based on the level of threat and potential harm to the organization.

d. Incident Response Steps: a protocol to follow in case of emergency. It should reflect the necessary steps to minimize impact and effectively stop the damage of the incident when it happens. This is the most crucial part of the framework, as long as chaotic response may lead to being too slow at mitigating or in worst case may cause additional damage to what has already been donce.

Dealing with ongoing incidents.

When an incident occurs, following a well-defined set of steps can help streamline the incident management process. The best is when these steps are documented in the incident management framework. While based on the nature of an incident some specific actions would be required, here are some critical steps to consider for any incident in general:

a. Incident Identification: Implement robust monitoring systems and practices to swiftly detect and identify incidents. This includes proactive threat intelligence gathering, security audits, and real-time monitoring of critical systems.

b. Incident Assessment: Once an incident is identified, conduct a thorough assessment to determine the scope, severity, and potential impact. Gather all available information, involve relevant stakeholders, and assign appropriate resources for the response effort.

c. Incident Containment and Mitigation: Take immediate action to contain the incident and prevent further damage. This may involve isolating affected systems, disabling compromised accounts, or implementing temporary workarounds. Develop and follow predefined playbooks and incident response procedures tailored to specific incident types.

d. Incident Investigation: Conduct a comprehensive investigation to determine the root cause of the incident. This may involve forensic analysis, log reviews, and engaging external experts if necessary. Gathering evidence and documenting findings is essential for future prevention and regulatory compliance.

e. Incident Resolution and Recovery: Develop a well-defined plan for resolving the incident and restoring normal operations. Test and validate recovery procedures in advance to ensure they are effective. Communicate progress and expected timelines to stakeholders throughout the recovery process.

f. Incident Documentation and Lessons Learned: After resolving the incident, document all relevant details, including actions taken, challenges faced, and lessons learned. This information serves as a valuable resource for future incident management and continuous improvement.

Effective post-incident management is crucial for minimizing the impact, preventing future occurrences, and addressing any legal ramifications. This article will outline the key actions to be taken after an incident has already occurred, including evaluation, prevention measures, and addressing legal aspects.

Evaluate the Incident:

Following an incident, a thorough evaluation is necessary to understand its root cause, impact, and implications for the organization. Consider the following steps:

a. Incident Documentation: Compile a comprehensive incident report detailing the incident's timeline, affected systems, potential vulnerabilities exploited, and any actions taken during the response and recovery process. This report will serve as a crucial reference for subsequent analysis and legal considerations.

b. Impact Assessment: Assess the incident's impact on operations, data integrity, reputation, and financials. Quantify any direct or indirect losses incurred and identify any regulatory or compliance breaches that may have occurred.

c. Root Cause Analysis: Conduct a detailed investigation to determine the underlying causes of the incident. This analysis should identify any systemic vulnerabilities, human error, process deficiencies, or external factors that contributed to the incident.

Preventing Future Incidents:

Post-incident management should focus on implementing preventive measures to mitigate the risk of similar incidents in the future. Consider the following actions:

a. Remediation and System Hardening: Address the vulnerabilities or weaknesses identified during the incident evaluation. Implement security patches, update configurations, and enhance system hardening measures to reduce the likelihood of future incidents.

b. Process and Policy Review: Review existing processes, procedures, and policies to identify any gaps or weaknesses that may have contributed to the incident. Enhance or establish new controls to address these shortcomings and ensure compliance with relevant regulations.

c. Training and Awareness Programs: Provide targeted training to employees regarding incident response, cybersecurity best practices, and compliance requirements. Foster a culture of security awareness and empower employees to identify and report potential risks promptly.

d. Continuous Monitoring and Testing: Implement robust monitoring systems to detect and respond to potential threats in real-time. Regularly conduct

vulnerability assessments, penetration testing, and security audits to identify and address emerging risks.

Dealing with incidents requires a comprehensive approach that considers foreseen and unforeseen risks. By implementing robust strategies, focusing on mitigation measures, measuring potential losses, and making informed decisions, organizations can effectively navigate incidents. Proactive risk management, continuous monitoring, and adaptive strategies are key to mitigating incidents' impact and ensuring long-term resilience. Effective post-incident management involves thorough evaluation, preventive measures, and addressing legal aspects. By conducting a comprehensive incident assessment, implementing preventive actions, and seeking legal guidance, organizations can mitigate the impact of incidents, reduce the risk of future occurrences, and navigate the legal landscape with greater confidence.

References:

1. *P. Cichonski, T. Millar. Computer Security Incident Handling Guide. CSRC. 2012*
2. *T. Luttgens, M. Pepe. Incident Response & Computer Forensics. McGraw Hill. 2014*
3. *D. Watson. Security Incident Management: Reaching Beyond Compliance. O'Reilly. 2018*
4. *L. Gordon. Managing Cybersecurity Resources: A Cost-Benefit Analysis. McGraw Hill. 2005*
5. *D. Cappelli. The CERT Guide to Insider Threats. Addison-Wesley Professional. 2012*
6. *A. Jaquith. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional. 2007*
7. *B. Allen. Enterprise Security Risk Management: Concepts and Applications. Rothstein Associate. 2017*

Yaroslav Veselovskyi

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

POST-QUANTUM CRYPTOGRAPHY, LATTICE-BASED

Post-quantum cryptography[1] aims to develop alternative cryptographic schemes that are resistant to attacks by both classical and quantum computers. These schemes are based on mathematical problems that are believed to be hard to solve even for quantum computers. They provide a long-term security solution, ensuring that sensitive data and communication remain protected in a future where powerful quantum computers become widely available.

Some of the main areas of research within post-quantum cryptography include:

1. Lattice-Based Cryptography[2]: Lattice-based cryptography is based on the hardness of lattice problems, such as the Shortest Vector Problem (SVP) or Learning with Errors (LWE). Lattice-based schemes have shown resilience to attacks by quantum computers and are considered one of the most promising areas of post-quantum cryptography.

2. Code-Based Cryptography: Code-based cryptography utilizes error-correcting codes to provide security. It is based on the hardness of decoding specific codes, such as McEliece or Niederreiter codes, which are believed to be resistant to attacks by quantum computers.

3. Multivariate Cryptography: Multivariate cryptography relies on the difficulty of solving systems of multivariate polynomial equations. It is designed to resist attacks by both classical and quantum computers, and schemes like the Hidden Field Equation (HFE) or Unbalanced Oil and Vinegar (UOV) are examples of multivariate cryptographic schemes.

4. Hash-Based Cryptography: Hash-based cryptographic schemes utilize cryptographic hash functions to provide security. They are based on the assumption that certain one-way hash functions, such as the Merkle-Damg.rd construction or the Lamport signature scheme, are secure against attacks by quantum computers.

5. Symmetric-Key Cryptography: While most post-quantum research focuses on public-key cryptography, symmetric-key cryptographic algorithms, such as symmetric ciphers and hash functions, are already resistant to quantum attacks due to their different nature. Therefore, they continue to be secure in the postquantum era.

The goal of post-quantum cryptography is to ensure the continued confidentiality, integrity, and authenticity of data and communication in a world where quantum computers may pose a threat to traditional cryptographic systems.

Standardization efforts are underway to identify and select the most promising post-quantum cryptographic algorithms to be adopted as secure replacements for current systems.

Lattice-based cryptography is a type of post-quantum cryptography that relies on the hardness of certain mathematical problems associated with lattices. Lattices are mathematical structures formed by a set of points in a multi-dimensional grid. In latticebased cryptography, the security of cryptographic algorithms is based on the computational difficulty of solving lattice problems.

The main advantage of lattice-based cryptography is that it offers strong security guarantees even against attacks by quantum computers. Unlike some other cryptographic systems that are vulnerable to quantum algorithms, lattice-based schemes have shown resilience to attacks by both classical and quantum computers.

Lattice-based cryptography encompasses various cryptographic primitives, including:

1. Lattice-based encryption: Lattice-based encryption schemes provide a way to encrypt messages so that only authorized recipients with the correct private key can decrypt them. Examples of lattice-based encryption schemes include the Learning with Errors (LWE) encryption and Ring Learning with Errors (RLWE) encryption.

2. Lattice-based digital signatures: Lattice-based digital signature schemes allow individuals to sign messages to ensure their authenticity and integrity. These schemes are based on the hardness of certain lattice problems. The BLISS and BLS schemes are examples of lattice-based digital signature schemes.

3. Lattice-based key exchange: Lattice-based key exchange protocols enable two parties to establish a shared secret key over an insecure channel. These protocols are designed to resist attacks by both classical and quantum computers. Examples of lattice-based key exchange protocols include New Hope and Frodo.

Lattice-based cryptography offers a wide range of potential applications, including secure communication protocols, secure data storage, and secure computation.

However, lattice-based cryptographic algorithms generally require larger key sizes and computational resources compared to traditional cryptographic algorithms.

Nevertheless, ongoing research aims to optimize and enhance the efficiency of lattice-based schemes to make them more practical for real-world applications.

One of the advantages of lattice-based cryptography is its versatility. Lattices provide a flexible mathematical framework that allows the construction of various cryptographic primitives and protocols. For example, lattice-based encryption schemes enable secure communication by encrypting messages in a way that only authorized Lattice-based cryptography relies on the hardness of certain mathematical problems associated with lattices. These problems form the

foundation for the security of lattice-based cryptographic schemes. Here are some key lattice problems used in lattice-based cryptography:

1. Shortest Vector Problem (SVP): Given a lattice, the Shortest Vector Problem involves finding the shortest non-zero vector within that lattice. The computational complexity of solving this problem increases exponentially with the dimension of the lattice.

2. Learning with Errors (LWE): The Learning with Errors problem involves estimating a random linear equation modulo a small error term. It is used in many lattice-based cryptographic schemes, including encryption, key exchange, and digital signatures.

3. Ring Learning with Errors (RLWE): Similar to LWE, the Ring Learning with Errors problem involves estimating a random linear equation modulo a small error term. However, RLWE is specifically formulated in the context of polynomial rings, which makes it suitable for lattice-based schemes utilizing polynomial arithmetic.

4. Learning with Rounding (LWR): The Learning with Rounding problem is another variant of lattice-based problems. It involves estimating a random linear equation modulo a rounding operation. LWR is used in some lattice-based cryptographic schemes and provides a different security assumption compared to LWE.

5. GapSVP: The GapSVP (Gap Shortest Vector Problem) involves determining the approximate length of the shortest non-zero vector in a lattice, within a given factor. It is used in lattice-based cryptanalysis to assess the security of latticebased schemes.

These lattice problems are believed to be computationally hard, even for quantum computers. The security of lattice-based cryptography relies on the assumption that solving these problems requires an infeasible amount of computational resources. As a result, lattice-based cryptographic schemes are designed to take advantage of the hardness of these problems, providing a robust security foundation.

Overall, lattice-based cryptography is an active and promising area of research within post-quantum cryptography. Its resistance to attacks by quantum computers makes it a strong candidate for securing sensitive information and communication in a future where quantum computers may pose a threat to traditional cryptographic systems.

References:

1. *Daniel J. Bernstein (2009). "Introduction to post-quantum cryptography"*
2. *Peikert, Chris (2014). "Lattice Cryptography for the Internet"*

ПСИХОЛОГІЯ; ПЕДАГОГІКА (в т. ч. ФІЛОЛОГІЯ)

Шутяк І. А.

Заслужений вчитель України
Доцент кафедри філософії, соціально-гуманітарних наук та фізичного виховання
Хмельницького університету управління та права імені Леоніда Юзькова
м. Хмельницький, Україна

НЕВЕРБАЛЬНІ ЗАСОБИ СПІЛКУВАННЯ ТА ЇХ КЛАСИФІКАЦІЯ

Розпочнемо з того, що невербальне спілкування – це вид комунікації без використання слів. Наприклад до невербальної комунікації входять пози, міміка, жести, візуальний контакт та просторове розташування мовців при спілкуванні. Спілкування як живий перебіг безпосередньої комунікації, розкриває емоції, створюючи невербальну взаємодію обміну інформації тих хто спілкується.

Способи невербального спілкування як “мова почуттів” суттєво посилюють смисловий ефект вербальної комунікації, а за деяких обставин можуть її навіть замінювати. У діловій розмові вони інколи мають більше впливу та значення, ніж слова. У ділових розмовах дуже важливо, з однієї сторони, уміти контролювати свої рухи і міміку, а з іншої сторони – розуміти мову жестів і міміку співрозмовника, та правильно витлумачувати їх, розкривати прихований зміст. Неуважність або ігнорування невербальних засобів спілкування інколи може спантеличити співрозмовника, якщо неправильно сприйняти його міміку, жести, поведінку у різних ситуаціях або поводитися нерозсудливо. До невербальних засобів комунікації вчені відносять не тільки рухи тіла, жести (рухи рук, ніг), просторове поле між співрозмовниками, вираз очей та направленість погляду, вираз обличчя, акустичні засоби (пов’язані з мовою і непов’язані з нею), тактильні засоби (потиск рук, поцілунки), а й посмішку, косметику, реакцію шкіри (почервоніння, збліднення), запахи (парфуми, алкоголь), одяг та його колір, манери та інше.

Австралійський письменник Аллан Піз, відомий як «містер мова тіла», завдяки своїй однойменній книзі, стверджує, що за допомогою слів передається лише 7% інформації, в той час як за допомогою звукових засобів (тон голосу, інтонація тощо) – 38%, а за допомогою міміки, жестів, пози – 55%. [1]

Табл. 1. Класифікація невербальних засобів спілкування [2]

Невербальні засоби спілкування			
Кінесика	**Проксодика та екстралінгвістика**	**Таксика**	**Проксеміка**
Експресивно-виразні рухи	Інтонація	Рукостискання	Орієнтування
Поза	Гучність	Поцілунок	Дистанція
Жест	Тембр	Поплескування	
Міміка	Пауза		
Хода	Зітхання		
Візуальний контакт	Сміх		
Направленість рухів	Плач		
Частота контакту	Кашель		

Складові невербальної комунікації: міміка, пантоміміка, візуальний контакт, міжособистісний простір, жести. Міміка — рухи м'язів обличчя, що виражають почуття та психічний стан людини. Будь-які зміни у виразі обличчя добре помітні та найчастіше вказують на найменші зміни у внутрішньому стані людини. Найдостовірнішим сигналом та найінформативнішим способом невербального спілкування є саме очі. Візуальний контактний метод невербального спілкування допомагає продемонструвати зацікавленість у розмові та краще розуміти сенс сказаного. [3]

Жест – це рух рукою, або іншою частиною тіла, що має своє значення або доповнює мовлення.

- Жести підозрілості і прихованості вказують про недовіру до вас, сумніви у вашій правоті та бажання щось недоговорити або приховати від вас (це - потирання чола, скронь, підборіддя, прагнення прикрити обличчя руками).
- Жести і пози захисту є ознаками того, що співрозмовник почуває небезпеку або загрозу (стискання пальців в кулак).
- Жести міркування й оцінки вказують на замисленість та прагнення знайти рішення проблеми (рука у щоки, потирання перенісся).
- Жести сумніву і непевності — чухання вказівним пальцем правої руки під мочкою вуха або ж бічній частині шиї, дотик до носа чи його легке потирання.
- Жести готовності сигналізують про бажання закінчити розмову чи зустріч (подача корпусу вперед, при цьому обидві руки лежать на колінах чи тримаються за бічні краї стільця). [4]

Міжособистісний простір – це дистанція на якій співрозмовники перебувають одне від одного. Чим більше співрозмовники зацікавлені, тим ближче вони знаходяться одне до одного:

- Інтимна зона (від 15 до 46 см), саме цю зону людина найбільше оберігає, в ній можуть перебувати, крім суб'єкта, тільки найближчі люди.
- Особиста (від 46 до 120 см). У цій зоні люди зазвичай знаходяться під час дружніх зустрічей та на вечірках.
- Соціальна (від 120 – до 360 см). На такій відстані люди розміщуються під час міжособистісного спілкування з малознайомими людьми, зокрема, на роботі або на навчанні.
- Громадська (понад 360 см). Відстань, якої бажано дотримуватися лектору, оратору.

Отже, невербальна комунікація має величезний вплив у нашому житті. За допомогою невербального спілкування ми не тільки подаємо сигнали, але ще й можемо зчитувати емоції та почуття інших людей. Вербальні та невербальні способи спілкування можуть підсилювати або ослаблювати взаємодію впливу, тому розкривати суть цих сигналів потрібно не окремо, а разом з урахуванням контексту в цілому.

Список використаних джерел:

1. Невербальні засоби спілкування та їх класифікація. StudFiles. URL: https://studfile.net/preview/5199905/ (дата звернення: 20.03.2023).

2. Урок "Вербальні та невербальні засоби спілкування, їх характеристика". Освітній проект «На Урок» для вчителів. URL: https://naurok.com.ua/urok-verbalni-ta-neverbalni-zasobi-spilkuvannya-h-harakteristika-39433.html (дата звернення: 20.03.2023).

3. Учасники проектів Вікімедіа. Міміка – вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Міміка (дата звернення: 20.03.2023).

4. Невербальне спілкування. ProfiHealth - Навчання професіоналів, що надають соціально-медичні послуги. URL: https://profihealth.org.ua/uk/lessons/191 (дата звернення: 20.03.2023).

5. Учасники проектів Вікімедіа. Невербальна комунікація – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Невербальна_комунікація (дата звернення: 20.03.2023).

ЕКОНОМІКА

Білодід В. В.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

СУЧАСНІ НАПРЯМКИ РОЗВИТКУ ПРОЦЕСУ УПРАВЛІННЯ ЛАНЦЮЖКІВ ПОСТАВОК ТА ЛОГІСТИЧНИХ ОПЕРАЦІЙ У ВИРОБНИЦТВІ

У кожному виробничому процесі при виробництві продукції ми стикаємося з необхідністю поповнювати запаси сировини, пакувальних матеріалів, компонентів та інших складових. І не важливо до якої категорії ця продукція належить, ми все одно плануємо закупівлі у постачальників, як сировини, так і послуг. Щоб забезпечити потребу споживача, необхідно спланувати обсяги кінцевого продукту і звідси розрахувати необхідні запаси сировини та матеріалів, тобто - сформувати ланцюжок поставок. Ефективне управління ланцюжками поставок і логістичними операціями дає змогу виробничим підприємствам оптимізувати процеси та ресурси, знизити витрати, поліпшити якість і скоротити часові затримки. Чим ефективніше працює виробничий ланцюжок, тим більше можливостей у компанії для досягнення конкурентної переваги.

Водночас ланцюжки поставок і логістичні операції безпосередньо впливають на рівень обслуговування клієнтів. Ефективніше планування та координація дають змогу поліпшити точність поставок, своєчасність доставок і загальне задоволення клієнтів. Успішне управління ланцюгами поставок сприяє розвитку довгострокових партнерських відносин з клієнтами.

Сучасне управління ланцюгами поставок і логістичними операціями вимагає гнучкості та здатності швидко адаптуватися до мінливих умов ринку і вимог клієнтів. Гнучкість у плануванні та операційній діяльності дає змогу організаціям ефективно реагувати на зміни попиту, сезонні коливання, виникнення нових ринкових можливостей і зміни у постачальників.

Залежно від точки зору деякі з наведених нижче завдань можуть бути включені в систему ланцюга поставок і логістики організації.

- Постачання: отримання товарів або послуг зі сторонніх джерел.
- Прогноз попиту: оцінка необхідного клієнтам обсягу товарів і послуг.
- Обслуговування клієнтів і управління замовленнями: завдання, пов'язані з виконанням замовлень на товари або послуги, розміщені клієнтом.

- Запаси: планування та управління. Транспортування: замовне і приватне.
- Складські приміщення: загального користування та приватні.
- Поводження з матеріалами та пакування: переміщення, захист, зберігання та контроль матеріалів і продуктів з використанням ручного, напівавтоматичного та автоматизованого обладнання.
- Система об'єктів: вибір місця розташування об'єктів у системі ланцюга постачання компанії.

Управління ланцюгами поставок також пов'язане з операційним управлінням. Останнє полягає у створенні цінності шляхом перетворення вхідних матеріалів (сировини) на кінцевий результат (товари та послуги). І управління ланцюгами поставок, і операційне управління спрямовані на підтримку виробничого процесу [1].

У світовій практиці та економіці підприємств існує кілька моделей управління ланцюгами поставок. Деякі з них включають:

- Модель "Cycle" (Цикл);
- Модель "Push-Pull" (Тягни - Штовхай);
- Модель "Just-in-Time" (Точно в строк);
- Модель "Lean" (Штангенциркульна).

Модель Cycle процесів ланцюжка поставок

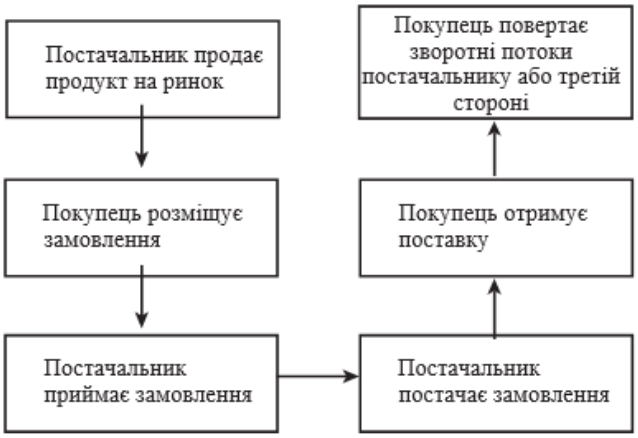
З огляду на п'ять етапів ланцюга постачання: Клієнт, Роздрібний продавець, Дистриб'ютор, Виробництво, Постачальник, усі процеси ланцюга постачання можна розбити на такі чотири цикли процесів, як показано на мал. 1:

- Цикл замовлення клієнта
- Цикл поповнення
- Виробничий цикл
- Цикл закупівель

Мал. 1

Кожен цикл відбувається на межі між двома послідовними етапами ланцюжка поставок. Не в кожному ланцюжку поставок усі чотири цикли чітко розділені. Наприклад, у ланцюжку постачань бакалійних товарів, у якому роздрібний торговець зберігає запаси готової продукції та розміщує замовлення на поповнення запасів у дистриб'ютора, усі чотири цикли, найімовірніше, будуть розділені. Dell, навпаки, обходить роздрібного продавця і дистриб'ютора, коли продає безпосередньо клієнтам.

Кожен цикл складається з шести підпроцесів, як показано на мал. 2.



Мал.2

Кожен цикл починається з того, що постачальник пропонує продукт покупцям. Потім покупець розміщує замовлення, яке отримує постачальник. Постачальник виконує замовлення, яке отримує покупець. Покупець може повернути частину продукту або іншого переробленого матеріалу постачальнику або третій стороні. Потім цикл дій починається заново.

Залежно від операції, що розглядається, підпроцеси на малюнку 2 можуть бути застосовані до відповідного циклу. Коли клієнти роблять покупки в Amazon, вони беруть участь у циклі замовлення клієнта, де клієнт виступає як покупець, а Amazon - як постачальник. Навпаки, коли Amazon замовляє книжки в дистрибутора для поповнення своїх запасів, це є частиною циклу поповнення запасів, у якому Amazon виступає як покупець, а дистрибутор - як постачальник [2].

У рамках кожного циклу метою покупця є забезпечення доступності продукції та досягнення економії за рахунок масштабу при замовленні. Постачальник намагається спрогнозувати замовлення покупців і знизити вартість отримання замовлення. Потім постачальник працює над своєчасним виконанням замовлення і підвищенням ефективності та точності процесу виконання замовлення. Покупець потім працює над зниженням вартості процесу отримання. Управління зворотними потоками здійснюється для зниження витрат і досягнення екологічних цілей.

Циклічне уявлення ланцюга поставок чітко визначає залучені процеси і власників кожного процесу. Таке уявлення корисне під час розгляду

операційних рішень, оскільки воно визначає ролі та обов'язки кожного учасника ланцюга поставок і бажаний результат для кожного процесу.

Модель Push-Pull

Усі процеси в ланцюзі поставок належать до однієї з двох категорій залежно від часу їх виконання відносно попиту кінцевого споживача. У процесах Push-Pull виконання починається у відповідь на замовлення клієнта. У процесах "штовхання" виконання починається в очікуванні замовлень клієнтів на основі прогнозу. Процеси, що тягнуть, можна також назвати реактивними процесами, оскільки вони реагують на попит клієнта. Штовхаючі процеси можна також назвати спекулятивними процесами, оскільки вони реагують на передбачуваний (або прогнозований), а не на фактичний попит. Штовхаючі процеси працюють у невизначеному середовищі, оскільки попит з боку клієнта ще не відомий. Процеси, що тягнуть, працюють у середовищі, в якому споживчий попит відомий. Однак вони часто обмежені рішеннями щодо запасів і виробничих потужностей, які були прийняті на етапі проштовхування [2].

Подання ланцюжка поставок за принципом "тягни-штовхай" класифікує процеси залежно від того, чи ініціюються вони у відповідь на замовлення клієнта (Pull, тягни) або в очікуванні замовлення клієнта (Push, штовхай). Цей погляд корисний під час розгляду стратегічних рішень, пов'язаних із проєктуванням ланцюжка поставок.

Модель Just-in-Time

Найбільш широко поширеною у світі є концепція "точно в строк" (just-in-time, JIT). Концепція "точно в строк" - це сучасна концепція побудови логістичної

системи у виробництві (операційному менеджменті), постачанні та дистрибуції, що ґрунтується на синхронізації процесів доставки матеріальних ресурсів і готової продукції в необхідних кількостях до того часу, коли ланки логістичної системи їх потребують, з метою мінімізації витрат, пов'язаних зі створенням запасів. [3].

Логістичні системи, що використовують принцип концепції "точно в строк", є системами, що тягнуть, у яких розміщення замовлень на поповнення запасів матеріальних ресурсів або готової продукції відбувається, коли кількість їх у певних ланках логістичної системи досягає критичного рівня. При цьому запаси "витягуються" розподільчими каналами від постачальників матеріальних ресурсів або в системі дистрибуції фірми.

У концепції "точно в строк" істотну роль відіграють такі елементи:

- попит, що визначає подальший рух сировини, матеріалів, компонентів, напівфабрикатів і готової продукції;
- концентрація основних постачальників матеріальних ресурсів поблизу головної фірми, що здійснює процес виробництва або складання готової продукції;

- надійність постачальників, оскільки будь-який збій постачання може порушити виробничий розклад;
- якість продукції (філософія загального управління якістю - управління якістю на всіх стадіях виробничого процесу і подальшого сервісу);
- точність інформації та прогнозування, для чого необхідна робота з надійними телекомунікаційними системами та інформаційно-комп'ютерною підтримкою;
- підвищена трудова відповідальність і висока трудова дисципліна всього персоналу.

Це лише деякі моделі управління ланцюгами поставок, які використовуються у світовій практиці. Організації обирають підхід, який найбільше відповідає їхнім потребам, бізнес-моделі та вимогам ринку. Але в період всесвітньої пандемії, війни в Україні, ситуація в глобальному ланцюжку поставок зазнає змін. Всім доводиться шукати шляхи вирішення фінансових, економічних питань у виробництві, постачанні послуг, а також у питаннях управління персоналом. І в цей період активізуються найкращі ідеї щодо реалізації ефективних рішень. Економіка підприємств, бізнесу переходить у новий етап взаємодії. Термін "колаборація" стає вже не настільки страшним, а стає засобом виживання малого та середнього бізнесу. Шлях розвитку управління ланцюгами поставок теж переживає свої етапи змін, можна навіть сказати, поліпшення. Не те щоб на зміну стандартним моделям управління ланцюжками поставок, але точно зі своєю гілкою розвитку приходить новий підхід, який можна застосовувати в управлінні ланцюгами поставок для забезпечення їхньої ефективності та узгодженості - інтегральне бізнес-планування (IBP).

Інтегроване бізнес-планування - це потужний процес, який може стати центральним у веденні бізнесу компанії. Воно на одне покоління перевершує планування продажів і операцій. Три суттєві відмінні ознаки створюють унікальну можливість управління бізнесом:

- Повне охоплення бізнесу. Не обмежуючись плануванням продажів і операцій, інтегроване бізнес-планування (IBP) синхронізує всі середньо- і довгострокові плани компанії, включно з управлінням доходами, лінійками та портфелями продуктів, стратегічними проектами та капітальними інвестиціями, політикою й розміщенням запасів, стратегіями закупівель і спільними із зовнішніми партнерами планами розвитку потужностей. Це робиться у всіх відповідних підрозділах організації, починаючи з рівня дільниці, регіонів і бізнес-підрозділів і часто аж до плану корпоративного рівня для всього бізнесу.
- Управління ризиками, поряд зі стратегією та оглядами ефективності. У найкращих практиках IBP для прийняття рішень використовується сценарне планування. На кожному етапі процесу існують

різні ступені впевненості в тому, як складеться майбутнє - який обсяг виторгу можна з достатнім ступенем упевненості отримати в результаті сталих моделей споживання, який обсяг додаткового попиту може виникнути в разі певних подій, і наскільки незвичні або екстремальні події можуть вплинути на цей додатковий попит. Ці шари оцінюються в порівнянні з бізнес-цілями, оцінюються та обираються варіанти дій щодо пом'якшення наслідків та усунення потенційних прогалин.

- Фінансові показники в режимі реального часу. Щоб забезпечити узгодженість між плануванням, заснованим на обсязі, і фінансовими прогнозами (тобто плануванням, заснованим на вартості), IBP заохочує тісний зв'язок між операційним і фінансовим плануванням. Це допомагає усунути несподіванки, які в іншому разі можуть стати очевидними тільки під час щоквартальних або річних оглядів.

Ефективний процес IBP складається з п'яти основних компонентів: бізнес-проекту; високоякісного управління процесом, включно з входами і виходами; підзвітності та управління ефективністю; ефективного використання даних, аналітики і технологій; а також спеціалізованих ролей і можливостей організації.

Дослідження групи McKinsey & Company показало, що зрілі процеси IBP можуть значно поліпшити координацію та зменшити кількість несподіванок. Порівняно з компаніями, у яких відсутній добре налагоджений процес IBP Середній зрілий практик IBP отримує один або два додаткові відсоткові пункти в EBIT. Рівень обслуговування вищий на п'ять - 20 відсоткових пунктів. Витрати на вантажоперевезення і капіталомісткість знижуються на 10-15 відсотків, а штрафні санкції за доставку і втрачені продажі - на 40-50 відсотків. Технологія IBP і дисципліна процесів також можуть підвищити продуктивність праці плановиків на 10-20 відсотків [4].

Важко не погодиться, що впровадження інтегрального бізнес-планування (IBP) у сучасне управління ланцюгами поставок може принести низку значущої вигоди і переваг для організації. IBP забезпечує кращу можливість для планування і прогнозування попиту, поставок, виробництва та інших аспектів управління ланцюгами поставок. Точніші прогнози дають змогу більш ефективно управляти запасами, уникати невідповідності попиту і пропозиції, а також оптимізувати виробничі та логістичні операції. А також IBP дає змогу організації бути гнучкішою та адаптивнішою до змін зовнішнього середовища і вимог ринку. Завдяки кращій видимості та точнішому плануванню, організація може швидше реагувати на зміни в попиті, зовнішні чинники або зміни в ланцюжках поставок. За допомогою аналізу та моделювання різних сценаріїв і стратегій, організація може передбачити потенційні ризики та розробити заходи для їх зниження або управління.

Список використаних джерел:

1. Пол Майерсон «Управління ланцюжками поставок та логістикою – простими словами. Методи та практика планування, побудови, обслуговування, контролю та розширення системи перевезень та постачання», «Альпина Диджитал», 2015.

2. «Управління ланцюжками поставок. СТРАТЕГІЯ, ПЛАНУВАННЯ І ДІЯ», Суніл Чопра, Пітер Мейндл, 5 видання, 2013

3. «Логістика та управління ланцюгами поставок. Теорія та практика. Основи логістики», підручник/за ред. Б.А.Анікіна та Т.А.Родкіної. Москва, Проспект, 2013 року.

4. *Стаття «A better way to drive your business» By Elena Dumitrescu, Matt Jochim, Ali Sankur, and Ketan Shah https://www.mckinsey.com/capabilities/operations/our-insights/a-better-way-to-drive-your-business#/ .*

Плющ А. В.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ЛОГИСТИЧЕСКИЕ КОНЦЕПЦИИ УПРАВЛЕНИЯ ЗАПАСАМИ ПРЕДПРИЯТИЙ УКРАИНЫ В ВОЕННОЕ ВРЕМЯ

Логистика (англ. *logistics*, от греч. λογιστική — учет) может рассматриваться как:

1. Наука про оптимальное управление материальными, информационными и финансовыми потоками в экономичных адаптивных системах с синергическими связями;

2. Отрасль или функция в корпорации, задачей которой есть обеспечение перемещения и сбережения продукции и сырья, для обеспечения производства и продажи. [1]

На сегодняшний день выделяют два основные направления в определении логистики:

- первое направление связано с функциональным подходом к товару, при котором логистика определяется как наука про управление всеми физическими операциями, которые необходимо выполнить во время доставки товаров от поставщиков до потребителей;
- второе направление характеризуется более широким подходом, кроме управления операциями перемещения товаров, логистика содержит анализ рынка поставщиков и потребителей, координацию спроса и предложения на рынке товаров и услуг, а также осуществляет гармонизацию интересов участников процесса товарооборота.

Цели логистики формируются в виде «семи правил» логистики:

ГРУЗ – необходимый товар;

КАЧЕСТВО – необходимого качества;

КОЛИЧЕСТВО – в необходимом количестве;

ВРЕМЯ – в нужное время;

КЛИЕНТ – соответствующему клиенту;

МЕСТО – в нужное место;

РАСХОД – с минимальными затратами [2, с. 465].

То есть, цель логистической деятельности считается достигнутой, если необходимый товар, необходимого качества в нужное время доставлен в нужное место с минимальными затратами.

С началом военной агрессии Российской федерации 24 февраля 2022 года, оккупация отдельных территорий и ракетные удары по городам Украины, стали причиной глобальных изменений как в Украине, так и во всем мире. Рынок Украины остался без обычных соединений, воздушное сообщение стало полностью недоступно для торговых и пассажирских

перевозок из-за закрытия воздушного пространства. Черное и Азовское море – водное сообщение, которое использовалось для экспорта зерна, продукции черной металлургии и горно-обогатительных комбинатов было заблокировано и контролируется военно-морским флотом Российской федерации. Наземное сообщение находится под постоянным риском последствий военных действий и осуществляется с большими задержками. Транспортное сообщение через Россию и Белоруссию полностью заблокировано, логистические маршруты увеличиваются, используются соседние страны для построения объездных маршрутов. Одна за другой останавливают свою деятельность в Украине международные компании - Raben Group, CMA CGM, MSC, Hellmann Worldwide Logistics, Hapag-Lloyd i Maersk. Експрес-служба UPS. Профессиональных водителей физически стало недостаточно, больше чем половина водителей были призваны в ряды вооруженных сил Украины. Общие потери складских помещений составили более 20% от всей площади складских площадей Киева и Киевской области [3]. Ракетные удары по нефтеперерабатывающих заводах и нефтебазах, остановка поставок топлива из России и Белоруссии, создали критическую ситуацию на рынке нефтепродуктов, которые является основным продуктом для рынка грузоперевозок.

Если проанализировать статистические данные за 2022 год, полученные от таможенной службы Украины, можно прийти к выводу, что экспорт товаров предприятий Украины по объему сократился почти на 39%, в деньгах он снизился на 35%. Было отправлено около 100 млн. тон различных видов продукции на 44,2 млрд. долларов США [4]. За видами транспорта экспорт на конец 2022 года распределился следующим образом:

- перевозка морским транспортом уменьшилась на 55% в сравнении с 2021 годом и составила 53,8 млн. тонн;
- перевозка железнодорожным транспортом увеличилась на 3,4% до 33,7 млн. тонн;
- перевозка автомобильным транспортом увеличилась на 32,4% до 12 млн. тонн.

Импорт товаров в Украину уменьшился в денежном эквиваленте до 58 млрд. долларов США, в физических объемах на 48,1% до 35 млн. тонн [5]. В реалиях военного положения, на фоне регулярных атак на транспортно-энергетическую инфраструктуру и блокаду морских портов, такой результат можно назвать приемлемым. Специалистам предприятий пришлось налаживать новые логистические схемы, разрабатывать соответствующие транспортные маршруты, бизнесу – выстраивать торгово-экономические отношения с новыми партнерами. Сейчас внешнеэкономическая деятельность и сотрудничество с Украиной во внешней торговле возможна в основном только через сухопутную границу, а далее через порты Румынии, Болгарии, Польши, Германии и стран Балтии.

Что касается складской составляющей в логистике предприятий, то как известно до начала вторжения Российской федерации на территорию Украины крупнейший складской хаб в Украине – 70-80% всех профессиональных складских площадей находился в Киевской области. Там было сосредоточено 1,6 млн. кв. м профессиональных складов [6], компании оперировали площадями от 10 000 до 120 000 кв. м [7]. С началом войны крупные предприятия, а вслед за ними средние и мелкие, были вынуждены перевезти свои складские остатки и товары на запад Украины. Произошел существенный отток во Львовскую, Тернопольскую, Ивано-Франковскую области, Закарпатье, где не существовало больших объемов складских помещений. Как следствие, помещений для складирования продукции предприятий в западных районах Украины не хватало, также площади, которые удавалось занять уступали бывшим складским помещениям по площади, организации пространства и уровню обслуживания. Таким образом предприятия были вынуждены изменить складскую цепочку и тем самым увеличить сложность и стоимость операций по складированию. Можно обозначить следующие изменения в работе предприятий:

- Отказ от накопления и хранения товаров. Если раньше товар мог долгое время находиться на складах, откуда шла отгрузка, то во время войны предприятия начали отгружать «с колес», стараясь минимизировать накопления остатков продукции на складах, чтобы в случае возможной атаки на склады не потерять весь товар.
- Резкое и быстрое изменение складских условий. Запустился так называемый «режим выживания», вместо развертывания IT системы и IT интеграции, настройки системы безопасности, видеонаблюдения, склады запускались с нуля, с функциями, которые закрывали базовые потребности, такие как помещение пригодно для складского хранения продукции, поиск водителей и складского персонала.
- Усложнение логистических операций. Большое количество блок постов военной и территориальной обороны и большое количество осмотров в начале военной агрессии России, отсутствие четких правил передвижения во время комендантского часа, различные действия и требования со стороны территориальных оборон различных городов, которые не всегда адекватно реагировали на ночные перемещения транспорта, доставляющего продукты, создавали дополнительные трудности с доставкой продукции.

Как следствие, если раньше большая доля всех складов создавалась в Киевской области, то сейчас компании стали смещать фокус на южную часть Киевской области и юго-запад Украины, считая их более безопасной зоной. Предприятия убедились, что было неразумно размещать инфраструктуру в одном месте, как это было в Украине до начала военного вторжения – 80% всех складов – в Киевской области. Пришло понимание, что нужно распределять склады по территории Украины и создавать определенный буфер, чтобы удерживать их. Включать режим формирования буфера

заранее, по определенным протоколам, до наступления экстренной ситуации.

Вместе с тем, все те изменения, которые произошли в логистической системе предприятий во время войны, позволили больше узнать проблемы и недостатки в организации логистических потоков, системе складирования и хранения товаров, это в будущем станет отправной точкой в процессе усовершенствования логистической системы Украины в послевоенное время.

Список использованных источников:

1. *Данные Википедии. URL: https://uk.wikipedia.org/wiki/Логістика.*
2. *Моисеева Н.К. Экономические основы логистики: Учебник. — М.: ИНФРА-М, 2008. – 528 с.*
3. *Анализ рынка складских помещений в Украине. Pro-Consulting специально для InVenture представляет аналитику рынка складских помещений в Украине. URL: https://inventure.com.ua/analytics/investments/analiz-rynka-skladskih-pomeshenij-v-ukraine*
4. *Товарообіг України за 2022 рік. Статистичні дані від Державної митної служби України URL: https://customs.gov.ua/en/news/novini-20/post/za-2022-rik-tovaroobig-sklav-997-mlrd-1055*
5. *Торгівля 2022 року за видами транспортних перевезень URL: https://export.gov.ua/news/4413-torgivlia_2022_roku_za_vidami_transportnikh_perevezen*
6. *Анастасия Быкова «В Киевской области разрушены склады общей площадью около 364 000 кв. м. Logist today. URL: ttps://logist.today/dnevnik_logista/vojna-v-ukraine/2022-04-22/v-kievskoj-oblasti-razrusheny-sklady-obshhej-ploshhadyu-okolo-364-000-kv-m/*
7. *ТОП-14 самых больших складов в Украине: рейтинг от платформы WareTeka. URL: https://wareteka.com.ua/blog/top-samyh-bolshih-skladov-ukrainy/*

Ромнов А. И.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ОБЗОР ТЕХНОЛОГИИ БЛОКЧЕЙН И ЕЕ ПОТЕНЦИАЛЬНОЕ ИСПОЛЬЗОВАНИЕ В ЛОГИСТИКЕ И ТРАНСПОРТЕ

«Технология блокчейн представляет собой децентрализованную и неизменную цифровую книгу, которая записывает транзакции или данные на нескольких компьютерах или узлах в сети. Каждая транзакция или ввод данных, известный как блок, имеет отметку времени и связан с предыдущим блоком, создавая цепочку блоков.» [1, с. 12] Эта технология распределенного реестра предлагает несколько функций, которые делают ее привлекательной для различных отраслей, включая логистику и транспорт.

Одной из ключевых особенностей технологии блокчейн является ее прозрачность и неизменность. Как только транзакция или ввод данных записываются в блокчейн, их нельзя изменить или подделать, что обеспечивает высокий уровень целостности данных и доверия. Эта функция может быть особенно полезной в сфере логистики и транспорта, где решающее значение имеют прозрачность и отслеживаемость товаров, отгрузок и транзакций.

Технология блокчейн может упростить и оптимизировать различные аспекты логистических и транспортных операций. Вот некоторые возможные варианты использования и преимущества:

1) Наглядность и отслеживаемость цепочки поставок. Блокчейн может обеспечить сквозную видимость и отслеживаемость товаров по всей цепочке поставок. Записывая каждую транзакцию от пункта отправления до конечного пункта назначения в общей цепочке блоков, заинтересованные стороны могут в режиме реального времени видеть движение, местоположение и статус поставок. Это может повысить прозрачность, уменьшить мошенничество и обеспечить лучшее управление запасами.

2) Смарт-контракты и автоматизация. Блокчейн может упростить использование смарт-контрактов, которые представляют собой самоисполняющиеся контракты с заранее определенными условиями. Смарт-контракты могут автоматизировать такие процессы, как оплата фрахта, таможенное оформление и страховые претензии, уменьшая административную нагрузку и сводя к минимуму задержки и споры. Эти автоматизированные процессы могут повысить эффективность и точность при одновременном снижении затрат.

3) Повышение доверия и безопасности. Децентрализованный и защищенный от несанкционированного доступа характер блокчейна

повышает доверие между заинтересованными сторонами в логистической и транспортной отрасли. Устраняя необходимость в посредниках и обеспечивая безопасную, проверяемую запись транзакций, блокчейн может снизить риск мошенничества, контрафактных товаров и несанкционированного доступа. Это также может обеспечить безопасный обмен конфиденциальной информацией между доверенными сторонами.

4) Упрощенная документация и соответствие требованиям. Технология блокчейн может упростить процессы документации в логистике, такие как коносамент, сертификаты происхождения и таможенная документация. Оцифровка и безопасное хранение этих документов в блокчейне может упростить проверку, сократить бумажную работу и улучшить соответствие нормативным требованиям. Это может ускорить процессы таможенного оформления и сократить задержки и ошибки.

5) Эффективное финансирование цепочки поставок. Блокчейн может облегчить финансирование цепочки поставок, обеспечивая прозрачную и надежную запись транзакций и запасов. Это может обеспечить более быстрый доступ к финансированию, улучшить движение денежных средств и снизить риск для кредиторов. Участники цепочки поставок также могут получить более точную и актуальную информацию для оценки кредитоспособности и управления рисками.

Несмотря на потенциальные преимущества, внедрение блокчейна в логистику и транспорт сопряжено с трудностями. По мнению исследователей Мехди Мохаммади и Ашкан Халили, к ним относятся масштабируемость для обработки больших объемов транзакций, совместимость с существующими системами, стандартизация форматов данных и протоколов, а также учет юридических и нормативных требований. Кроме того, внедрение блокчейна требует сотрудничества между различными заинтересованными сторонами и общеотраслевого консенсуса в отношении стандартов и моделей управления. [3]

В заключение, технология блокчейн может произвести революцию в логистике и транспортной отрасли за счет повышения прозрачности, отслеживаемости, эффективности и безопасности. Используя такие функции, как прозрачность, неизменность и децентрализованный консенсус, блокчейн может обеспечить доверие, автоматизацию и оптимизацию процессов по всей цепочке поставок, что приведет к экономии средств, улучшению качества обслуживания клиентов и расширению сотрудничества в отрасли.

Список использованных источников:

1. *Мелани Свон. Блокчейн. Схема новой экономики. Москва: Олимп-Бизнес, 2017. 300 с.*
2. *Gwynne Richards, Susan Grinsted. The Logistics and Supply Chain Toolkit: Over 100 Tools for Transport, Warehousing and Inventory Management. 3D edition. London: Kogan Page, 2020. 399 p.*
3. *Mehdi Mohammadi, Ashkan Khalili. A survey on blockchain technology for the Internet of Things: Applications and challenges in logistics and supply chain management. Computers & Industrial Engineering Journal, №157. Amsterdam: Elsevier, 2021. 186 p.*

Aleksandr Denysiuk

Student, Akademie HUSPOL s.r.o
Kunovice, The Czech Republic

PRINCIPLES OF BANK MANAGEMENT IN WARTIME (ON THE EXAMPLE OF UKRAINE)

Since the beginning of the war in Ukraine, which began in 2014 with the occupation of the territories, the country's banking system has faced many challenges: lack of labor resources, the threat of cyberattacks, exceeding cash balance limits, seizure of bank accounts, losses on previously granted loans, limited amount of cash in ATMs and others. To solve these problems, it was necessary to ensure the stable functioning of the banking system during the war, develop risk management, promote digitalization, popularize non-cash accounts, strengthen the electronic payment system, and enlist international support. The banking industry is facing many challenges, especially in the area of bank management. The main purpose of the study is to investigate the principles of bank management in this difficult period. As for the relevance, it is obvious - the principles of functioning and management in the banking sector during the war are a complex and crucial experience that can be adapted by other countries facing crisis situations in the economic and political environment.

Scholars have hardly addressed the issue of management in the banking sector during wartime, and there are no thorough studies on this issue. As of today, there are only a few publications related to the topic of the study that came out over the past year. These are, in particular, the article by N. Prokopenko, B. Myronchuk, and I. Shepel "Principles of the functioning of the banking system in wartime" (Prokopenko 2022), V. Sharapov "Formation of the concept of crisis management in wartime" (Sharapov, 2023), O.Antoniuk, L.Nianko "The banking system of Ukraine: current challenges and development trends" and others (Antonuk, 2022). The last of these articles, in particular, assesses the set of anti-crisis measures used by bank management. A retrospective assessment of the subjective and objective factors influencing the functioning of the banking system is carried out and the prospects for its development are outlined.

Despite a number of difficulties, the banking system continues to functioning. Banks trying to ensure stable operation of their branches in the regions despite blackouts and threats to life and health of the population. Of course, in the conditions of the war with Russia, the banking system of Ukraine operates with the restrictions established by the Resolution of the Board of the National Bank of Ukraine No. 18 of 24.02.2022 "On the operation of the banking system during the introduction of martial law. (Prokopenko, 2022) These restrictions of relation-cash withdrawals from customer accounts, withdrawals cash in foreign currency, works

currency market, official foreign exchange rat currencies, etc. The NBU revokes the licenses of banks, financial and insurance institutions - all in order to eliminate the possible outflow of capital and neutralize the impact on the country's economy, the state seeks to completely destroy the aggressor not only on the battlefield, but also in many areas of the economy, for this purpose additional sanctions are introduced, restrictions are introduced and controls on the circulation of funds in the state in various areas of the economy, industry, and digital services are being strengthened. This has a positive effect on the strengthening of the national currency, the reduction of inflation, which was caused at the beginning of 2023 by the need for additional money emission. The National Bank of Ukraine performs both a controlling and a strategically leading position in this matter, acting as a surgeon who removes the tumor, and creating prerequisites for further transparent investments in the country's economy after the end of military operations of the Armed Forces. After all, this is the only way to destroy the enemy both on the battlefield and in the economy.

In this matter, in 2014, the Ukrainian banking sector was thrust into turmoil due to an escalating conflict. The crisis necessitated strategic leadership and innovative management tactics to safeguard economic stability (Aslund, 2016). The National Bank of Ukraine (NBU) stepped up to this challenge, adopting a leadership strategy characterized by stringent supervisory practices, improved transparency, and a commitment to resilience. The NBU closed around 100 banks deemed insolvent, shrinking the banking institutions from 180 in 2014 to around 80 in 2017. A key decision of the NBU was the nationalization of PrivatBank, Ukraine's largest lender, due to a significant capital shortfall. This move demonstrated the NBU's readiness to take bold measures in the face of crisis (Aslund, 2016). Innovative management was also evident in the NBU's implementation of capital controls to stabilize the national currency (Hryvnia). These controls played a critical role in preventing capital flight and maintaining monetary stability.

The shift towards digital banking services was another strategic move driven by the conflict and growing consumer demand. PrivatBank launched a digital banking service in 2016, reaching 10 million users in just three years, showcasing the sector's adaptability. Despite these measures, Ukrainian banks still grapple with high non-performing loan ratios, reaching 54% of total loans in 2017 (Antonuk, 2022). This ongoing challenge underscores the need for continual management innovation.

So, to summarize, we note that the Ukrainian’s economy has been operating under military terror for several years now, and the stability and predictability of the national banking system are of great importance. Operating under martial law has become a stress test for Ukrainian banks to some extent. In today's environment, an effective process of checking the reliability of banks is critical for the financial stability of both businesses and households.

Ukrainian banking sector's resilience in the face of adversity offers valuable insights into effective crisis management and leadership strategies in the banking industry. The NBU plays the role of leader and controller, works for the future to protect the economy, uses all tools, cuts out the tumor like Ukrainian soldiers at the front for further net investment.

References:

1. Antoniuk O. Nianko L. (2022) Bankivska systema Ukrainy: vyklyky sohodennia ta tendentsii rozvytku. Instytut bukhhalterskoho obliku, kontrol ta analiz v umovakh hlobalizatsii. 2022. Vypusk 3-4. S. 36-43. DOI: https://doi.org/10.35774/ibo2022.03-04.036 (in Ukrainian)

2. Aslund A. (2016). Ukraine nationalizes its biggest bank. Here's why this is a good thing. Available at: https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-nationalizes-its-biggest-bank-here-s-why-this-is-a-good-thing/ (in English)

3. Prokopenko N. Myronchuk v. Shepel I. (2022) Pryntsypy funktsionuvannia bankivskoi systemy Ukrainy v umovakh viiny. Ekonomika ta suspilstvo. №41. P. 2-8. DOI: https://doi.org/10.32782/2524-0072/2022-41-33 (in Ukrainian)

4. Sharapov V. (2023) Formuvannia kontseptsii antykryzovoho menedzhmentu v umovakh voienoho chasu. Humanities studies: Collection of Scientific Papers / Ed. V. Voronkova. Zaporizhzhia: Publishing house "Helvetica", 2023. 14 (91). P. 196–207. doi: https://doi.org/10.32782/hst-2023-14-91-22 (in Ukrainian)

Eduard Dushynskyi

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

DEVELOPMENT AND APPLICATION OF ALTERNATIVE ENERGY SYSTEMS

We considered the issue of a rapid change in energy technologies and the transition from fossil energy sources to renewable ones. The goal was to show that for the European and Ukrainian market, the development of energy saving systems leads to serious savings, and solves a number of production and household tasks for enterprises. Having received real data related to the operation of the equipment and compared it with the values of early costs, we came to the conclusion that the cost savings are more than tangible for a number of production areas in Ukraine. Realizing that the economy of Ukraine, like no other, favors the transition to green energy sources due to the fact that:

1) The agricultural sector prevails, which means it is initially associated with natural factors
2) The presence of vast unoccupied territories
3) Located further south than the main economic giants of Europe
4) Mental component
5) Geopolitical choice of energy saving systems development and application is one of the key directions of the energy strategy

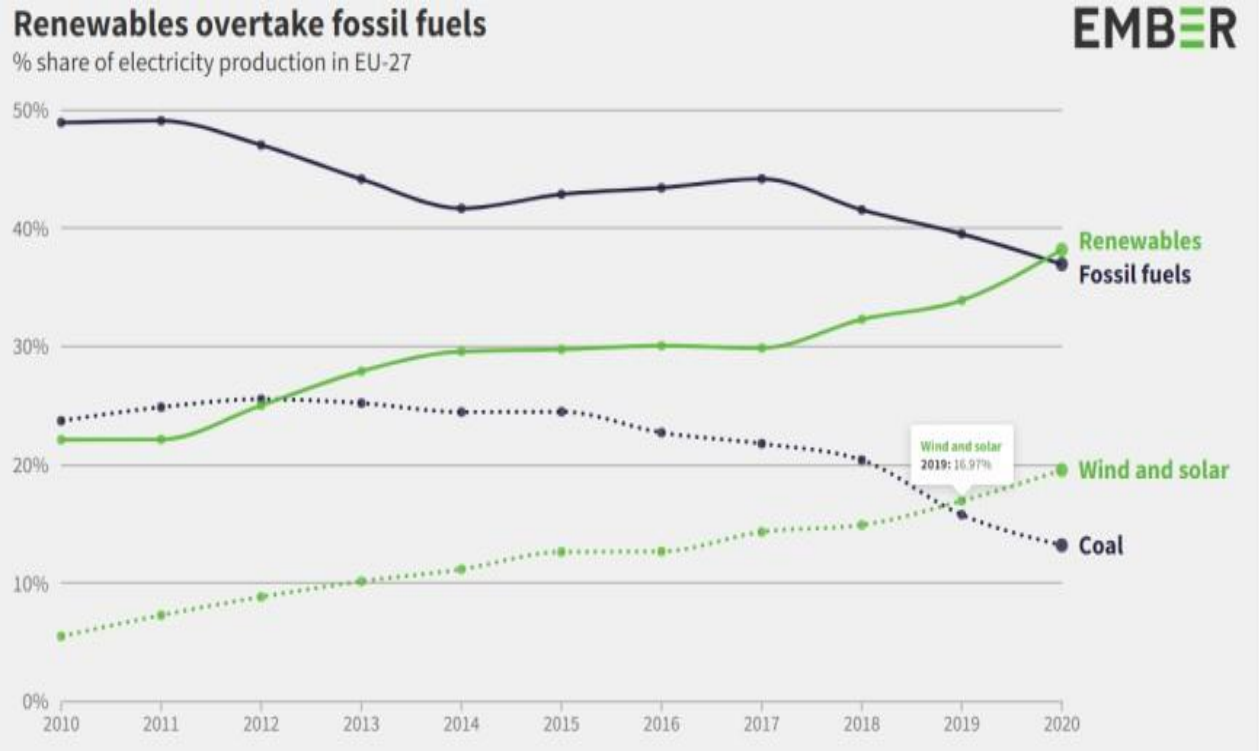
One of the main advantages of alternative energy is that it can provide a stable flow of energy without polluting the environment. For example, solar energy from solar panels can provide a stable flow of energy with minimal environmental impact. Also, wind energy, hydropower and biomass can be used as alternative energy sources, providing the necessary energy flow without negative impact on the environment.

By switching to alternative energy, countries can reduce their dependence on energy imports, which can reduce the risks of geopolitical influence on the economy and ensure the sustainability of energy supplies. In addition, the use of alternative energy systems can create new jobs and contribute to the development of the domestic market.

One of the biggest barriers is the high cost of producing and installing alternative energy systems compared to traditional sources. Many countries are forced to invest heavily in the development and installation of alternative energy systems, which may require significant budgetary resources.

According to the report of the analytical centres Ember and Agora Energiewende in Europe in 2020, for the first time, the amount of electricity

generated from renewable sources (38%) exceeded the amount from fuel sources (37%).



Graph 1: The Place of Renewable Energy[4]

Consequently, renewable energy has continued to grow in recent years despite global uncertainty.

Borrowing the experience of European countries will accelerate Ukraine's transition to the principles of a resource-efficient, energy-saving, responsible, low-carbon, innovative, "green" economy.

In general, the development of RES is an important element of the strategy for ensuring sustainable energy development and combating climate change. The use of renewable energy sources helps to reduce dependence on energy imports, improve the quality of the environment and reduce emissions of harmful substances, which meets the needs of society for a balanced and sustainable development.

References:

1. Share of renewable energy in gross final energy consumption in Europe [Electronic resource]. URL https://www.eea.europa.eu/data- andmaps/indicators/renewable-gross-final-energy-consumption4/

2. Renewables Take Lion's Share of Global Power Additions

3. EU Power Sector in 2020 URL: https://ember- climate.org/insights/research/eu- power-sector-2020/

4. 4)Renewable energy statistics URL https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics

Yevhenii Tyrsyna

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

PARTICULARITY OF USING THE PERSONAL MANAGEMENT SYSTEM IN A TRADING ENTERPRISE

In modern world, where competition in the field of trade is becoming more and more acute, effective management of resources and processes becomes one of the most important tasks for trade enterprises. The methods of organization and use of resources and personnel determine the success and competitiveness of the enterprise. It is here that the implementation of a personal management system, which is aimed at effective personnel management and ensuring optimal conditions for achieving set goals, becomes extremely important.

The personal management system is a comprehensive approach to personnel management, which involves the use of modern tools and methods to increase labor productivity, development and motivation of employees [2, p. 48].

In trade enterprises, the system of personal management acquires special importance, as it is aimed at the development and support of a team of employees directly engaged in the sale of goods or services. Optimally organized work of the staff ensures high quality of customer service, increases sales volume and ensures a positive image of the enterprise.

The process of selecting and hiring personnel is a critical stage for a trading enterprise, since the quality of service and the success of the business depend on the correct selection of employees. The use of a personal management system in this process helps to ensure the optimal selection of candidates, taking into account the requirements and needs of the trading enterprise. Key aspects within this process include:

– Identification of personnel needs: a personnel management system helps to analyze the work duties and needs of the enterprise, identify new vacancies and find out the necessary qualifications and skills for these positions. This makes it possible to more accurately determine the profile of the candidate and start the search for suitable applicants.

– Developing a candidate profile: the personal management system helps to create a detailed description of the candidate profile for each vacancy. It takes into account not only professional skills, but also personal qualities and characteristics that are important for successful work in this position. This helps to attract candidates who better match the needs of the enterprise [6, p. 118].

– Use of effective selection methods: the personal management system provides an opportunity to use various candidate selection methods, such as job

advertisements, recruiting agencies, candidate databases, etc. It also helps conduct pre-screening of resumes, skills testing and competency assessment of candidates. This makes it possible to increase the efficiency of the selection process and attract candidates who best meet the requirements of the position.

– Conducting interviews. It can be a video interview, online testing or other forms of communication [4, p. 211].

The onboarding of new employees is an important stage in ensuring the success and efficiency of their work at the trading enterprise. A personal management system in this process can provide a structured and effective approach that helps new employees to adapt and integrate into the work faster.

A personal management system can help organize the process of introducing a new employee to key individuals in the enterprise, including managers and colleagues. This creates an opportunity for communication, establishing relationships and building working relationships [1, p. 27].

This system can provide new employees with access to information about corporate culture and company values. This helps them better understand the company's entrepreneurial spirit, goals and expectations, and adapt to its work environment.

Evaluation and development of personnel is an important component of effective personal management in a trading enterprise. The personal management system helps to establish clear criteria for evaluating employees and provides regular evaluations of their work. This allows determining how successfully employees perform their duties and whether they meet established standards.

One of the important elements of the personal management system is providing feedback to employees. Regular evaluations provide an opportunity to discuss achievements, identify strengths and areas for improvement, and provide constructive feedback. This contributes to the growth and development of employees [5, p. 121].

Mentoring support is an important element of the personal management system at a trading enterprise. This approach involves one-on-one mentoring and support from an experienced employee who acts as a mentor to less experienced employees.

Mentoring support is based on a personal approach to each employee. A mentor provides individual advice, guidance and support to develop professional skills and achieve success at work. He uses his experience and expertise to impart knowledge and skills to junior employees, helping them understand job requirements and develop necessary competencies [3, p. 52].

One of the main tasks of a mentor is to support the career growth of employees. It facilitates the identification of goals and strategies for professional development, providing advice on career planning and pointing out opportunities for development. A mentor helps employees overcome obstacles on the way to success and increase their professional status.

In addition, mentoring support is important during the adaptation of new employees.

Furthermore, the personal management system can contribute to the career development of employees. It helps identify the potential of employees and identify opportunities for professional growth. For example, career planning, mentoring programs or participation in projects that help employees develop and move forward in their careers.

The system of personal management at a trade enterprise includes various aspects aimed at training, development and improvement of personnel skills. One of these aspects is the organization of trainings and education, which contribute to increasing the efficiency and productivity of personnel [6, p. 137–138].

The organization of trainings and education in the personal management system allows staff to acquire new knowledge, improve existing skills and develop professional potential. These can be trainings in sales, customer service, communication skills, leadership and others. These activities contribute to the improvement of professional skills and provide personnel with the necessary knowledge to effectively perform their duties.

The organization of trainings and education also helps to increase the motivation of the staff. When employees see that they are given the opportunity to develop and acquire new skills, they feel valued and important to the company. This can have a positive effect on their productivity and work engagement.

Starting with the recruitment and selection process, the personnel management system helps to identify personnel needs, develop a candidate profile and effective selection methods. It also gives the opportunity to assess the skills and competencies of applicants, conduct interviews and select the best candidates for positions in the company [4, p. 213].

In addition, the personal management system contributes to the resolution of labor conflicts and problems. It provides mechanisms for resolving disputes, establishing mutually acceptable working conditions and ensuring compliance with labor laws. This helps to maintain harmonious relations between all parties – the company's management, employees and their representatives.

It should be noted that the personal management system also takes into account the needs and interests of employees. The system facilitates the development of policies on working hours, vacations, professional development, training and career development. It stimulates the motivation of employees, ensures their job satisfaction and helps to increase their productivity. The personal management system can also include the development of individual development plans for employees, which helps them expand their knowledge and skills, as well as advance on the career stairs.

The personal management system includes analytics and reporting as an important element of personnel management at a trading enterprise. This system gives the opportunity to collect and analyze various data, such as employee productivity, sales volumes, customer satisfaction and other indicators [2, p. 50].

Thanks to analytics and reporting, it is possible to identify trends and understand what factors affect staff performance. For example, by analyzing data, one can discover which teams or individual employees achieve the best results, or identify periods with increased demand for certain goods or services.

Analytics also help develop strategies for further staff development. For example, if analysis shows that certain employees are underperforming, training programs can be designed to improve their skills and knowledge.

The reports generated by the personal management system provide important information to the company's management for making informed management decisions. For example, on the basis of reports, it is possible to determine the effectiveness of certain measures or programs, identify problematic aspects in the work of personnel and make the necessary adjustments [5, p. 127].

Therefore, the use of a personal management system at a trade enterprise has its own characteristics that contribute to the proper management of labor relations. This system helps ensure effective functioning and interaction between the employer and employees, develop their professional skills and motivation, resolve labor conflicts and problems, and perform analytics and reporting for informed management decisions. Thanks to these features, the personal management system becomes an important tool for successful personnel management at a trade enterprise.

References:

1. Buzhymska, K. O. Organization of an effective sales management system at a manufacturing and trading enterprise. Entrepreneurship and trade. 2022. №33. P. 24–30.

2. Kuzminchuk N. V., Kutsenko T. M., Terovanesova O. Yu. Marketing management in the system of strategic management of trade enterprises. Modern Economics. 2021. № 28. P. 47–51.

3. Marchenko O. M. Practicum in management: teaching manual. Lviv: Lviv State University of Internal Affairs, 2021. 224 p.

4. Sytnyk J. S. The evolution of personnel management and the human factor in the enterprise management system. Eastern Europe: Economy, Business and Management. 2016. Iss. 2. P. 209–215.

5. Telyshevska L. I., Ilchenko D. V. Peculiarities of personnel management at the enterprise. Economic management: theory and practice. 2018. 2018. P. 116–129.

6. Shubalyi O. M. et al. Personnel management: a textbook. Lutsk: Lutsk National Technical University of Ukraine, 2018. 404 p.

Artem Zghurskyi

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

TODAY'S CHALLENGES OF SCALING UP A FAST-GROWING START-UP

Topicality topics research conditioned those what startups are an important aspect in increasing investment attractiveness the country's climate, especially the development of innovative entrepreneurship and support small and average business with purpose competitive development of the economy of Ukraine. Today, Ukraine remains in list developing countries from tall economic potential.

However, innovative technical solutions in various fields are also being developed in Ukraine. In particular, it is worth highlighting the first household solar station in Ukraine, created by the innovator Roman Babyachk, which sells energy to the state at a green tariff and is used for its own purposes. Except moreover, the monitoring data of this station are presented online and everyone can view the statistics of obtaining solar energy www . solarlviv . com . ua / monitor . In addition, Roman Babyachok developed and integrated technological solutions on his own house (solar collectors, heat pump, solar station, insulation, etc.), which helped him significantly reduce the costs of maintaining his own house, and on the other hand, he helps to create new solar stations and introduce energy-saving technologies to private households. In 2016-2017, the EGAP competition was organized with the support of the Electronic Governance for Government Accountability and Community Participation program Challenge, the purpose of which was to introduce new electronic democracy tools that will help citizens to receive new high-quality services, effectively interact and directly influence the authorities, and the authorities to achieve a new level of transparency and efficiency.

Projects were developed in the following directions: education, ecology, infrastructure and agro-industry. In 2017, out of 200 submitted projects, winners were selected in each category: Infrastructure 1st place: Smarttickets (250,000 hryvnias) — e-service of a single ticket, allows you to plan a route with different types of transport and get an electronic ticket ; II place: SafeWayUA (150,000 hryvnias) — passenger transportation safety control system; II place: Smart country (100,000 hryvnias) — quality control service for the provision of services by state-owned enterprises (CaaS). Education 1st place: CASERS . org — a service for the interaction of educational and scientific initiatives and business, which solves the problem of the practicality of knowledge; 2nd place: Fractal Tools (150,000 UAH) — an educational platform for technological creativity for

non-professionals; III place: Bukvyk, iLearn , E-Mova (100,000 UAH each) - E-Mova is a Ukrainian language learning platform that works with Russian-speaking Ukrainians in the front-line zone and with foreigners; - iLearn — a free online platform for preparing for external examinations; - Bukvik — an educational program for preschoolers, which includes a live notebook and a mobile application; Ecology 1st place: EcoInfo (250,000 hryvnias) — e-platform for monitoring atmospheric air at the point of stay (MaaS); II place: Animal - id . info UA (UAH 150,000) is an international animal identification database that combines national and local databases of identified animals, and also works with the registry of animals in captivity; III place: Precious Plastic is a social platform for recycling plastic into useful things, which aims to create a plastic bank through a crowdfunding platform and collection points. Agroindustry 1st place: Znaydeno (250,000 UAH) — visualization e-service for monitoring and control of land use, deforestation, unauthorized waste disposal (MaaS); 2nd place: AgroYard (150,000 UAH) — a marketplace for farmers with the possibility of concluding electronic contracts; III place: G. MIAN is a system of automatic samplers for analyzing the quality of grain mixtures.

Funding for startups has shrunk dramatically at the moment, but it still exists. At the beginning of 2022, 51% did not receive income, which may lead to the closure of projects and the leakage of new ideas outside of Ukraine. Up to 20% of innovative enterprises received very little funding. This may indicate future job cuts and reduced competitiveness. In order to qualitatively assess the impact of events on the further development of projects, we will consider the stages of startup development and sources of their funding. There are a total of 5 standard stages by which the project is formed, develops and brings profit. Seed stage . Initial stage. At this stage, an idea is born and a team of like-minded people is formed. This is one of the most important stages when it is necessary to thoroughly think through the project, its financing, market entry and further development. It is also necessary to invest in the project at this stage. As a rule, these are own funds, funds of acquaintances and friends. At this stage, it is most appropriate to use the rule of financing: 3 F (Family , Friends , Fools). Startup stage . At this stage, it is necessary to pay attention to advertising and searching for investors. We already have a well-thought-out model and plan that needs to be funded. Growth stage . This stage already involves the "birth" of the product. At this time, it is necessary to finally correct defects and shortcomings. Expansion and promotion of the brand in the market. Funding is also quite important at this stage, as we need to pay wages and cover production costs. The profit at this stage is already there, but it is not enough to satisfy all the needs of the company. Expansion stage . We have already established production of the product, our brand is stable enough in the market of goods or services.

The mission of the project is to improve the quality of education, control and improve the health of students. Implementation takes place due to the collection and analysis of data using various technological devices. The company is mainly

focused on schools. TechBrain - a technological project for the development of the smart classroom market; since the project's market entry is planned to be gradual, the first product of the project will be TechBottom - a device for correcting posture with a competitive medical wearable electronics market.

Improving the quality of education, monitoring and improving the health of students occurs due to the introduction of an integrated system of technological devices (cameras, light and oxygen sensors, etc.) into the system of educational classes. The first object of the project: The " TechBottom " sensor, which is attached to the child's clothing (recommended for clothing in the chest area), records the "zero", "correct" sitting position of the child when it is attached for the first time and signals the teacher and the child when the back position is incorrect due to sound and world signals (depending on the activated mode of the sensor)

The sensor system is based on the accelerometer. An accelerometer is a device for measuring the force of a reaction induced by acceleration or gravity. Single- and multi-axis models can determine the magnitude and direction of acceleration as a vector quantity and can therefore be used to determine orientation, vibration and shock. It is this device that signals the child and the teacher about a change in the position of the back during learning. Accelerometers are found in many portable electronic devices and game consoles, including the iPhone and Wii Remote from Nintendo .

Identification of potential customers. There is an important component in this issue, the identification of which provides a greater and deeper understanding of the target audience - this is the separation of the user and the client. Thus, the user is a child of school age, and the client is the children's parents. Since our company offers to use the sensor twice - the first period is 1-3 grades of school, and the second is 5-7 grades, this is biologically due to two periods of rapid growth of the child's body, respectively at the age of 6-8 years and 12-14 years. The children's parents are married people aged 27 to 45.

Customer problem. During education, children acquire bad habits (sitting incorrectly), which in turn causes diseases such as scoliosis and visual impairment. Humanity believes that children are one of the most important components of life on planet Earth, so the issue of their health is very important for all mankind. The relevance of the problem is confirmed by the large number of enterprises engaged in the production of means for solving this problem, as well as the large number of medical workers such as therapists and neurologists. One of the topical issues of orthopedics is the problem of scoliosis. Scoliosis, characterized by a multi-plane deformation of the spine with damage to internal organs and body systems, is found mainly in children and adolescents, and its frequency exceeds 15% in the structure of pathology of the musculoskeletal system, the frequency of detection does not tend to decrease. Scoliosis III-I V degrees with pronounced cosmetic and functional disorders make up from 1.5 to 2% [1]. Scoliosis is found in 2–3% of the population, aged 10 to 15 years. This disease affects teenagers and adults, regardless of race or socioeconomic status.

According to epidemiological studies, spinal curvature is 10 times more common in girls than in boys [2]. As noted by A. Sutula, at present, in the structure of morbidity of children and young people of school age, one of the first places is occupied by disorders of the musculoskeletal system, namely, postural disorders and scoliosis [3]. Scoliosis is one of the most common orthopedic diseases of childhood and adolescence. Specific factors of the course of scoliosis depend on the age of the patient and the angle of curvature.

The existing solution to the customer's problem in the market is expensive compared to the one offered by our innovative company, and does not guarantee the result unlike our new product. Products are presented on the market that solves the issue of correct posture: 1) Specialized chairs - Mealux and Goodwin are direct competitors because the products have almost no differences and compete only in terms of design and product prices. The direct solution to the problem of editing posture occurs due to the shape of the chair. The shape of the backrest completely repeats the correct position of the child's spine, helps to distribute the load along the entire length of the spine. In order to maintain the correct posture, it is enough to simply lean back against the backrest. In practice, the difficulty is manifested when a child, concentrating on learning, forgets to keep his back in the correct position. 2) Corsets - the Reabilitmed company manufactures various variations of corsets for adults and children. The children's corset for back posture is made of hypoallergenic materials and equipped with 2 simulated stiffening ribs, which, in combination with reclining straps, allow for gradual correction of posture due to adjustable separation of the shoulders with simultaneous fixation of the lumbar spine. 3) Specialized desks - transformer desks that solve this problem with a design that allows you to adjust their height to the desired level so that the student does not hunch over and does not lie with his chin on the table and, as a result, maintains the correct posture.

Startup TechBrain on at this stage is staying on stage developments and assessment

Everyone startup, idea should form very successively and structurally, but maintaining creative thinking. To date, exists many technician and methods, what help to build an idea startupstructurally and systematically Because all startups by score big uncertainties are high-risk measures, before investing in the project, the idea should be carefully checked "for strength" by putting all hypotheses and assumption under doubt and try refute questions and by hypothetical situations all the arguments and structures of your startup if a startup goes through a similar test, it has the right to life. Startup TechBrain was built according to modern methods and passed the primary assessment.

References:

1. *Maxim Olegovich Inshakov. Innovative startup projects: experience, assessment, implementation contradiction // Volgograd State Herald university Series 3: Economy. Ecology*

2. *Solomon, B. The most interesting startups 2014 year: choice Forbes / B. Solomon //Forbes.*

Electronic text message - Mode of access: http: // www.forbes.ru/tekhnologii-photogallery/internet-i-svyaz/276169-samye- interesnye-startapy-2014-goda-vybor-forbes/photo/1

3. Tumenko, M.S. Startups and peculiarities of their development in the conditions of the Russian language economy. [Elec. resource].- URL: http://www.scienceforum.ru/2014/pdf/433.pdf

4. Mykhailo Babich Startups: Vital cycle, Work with investors. Electronic resource Regime access: [h t tp :// blog . babich _ me /2016/03/ startup - rabota - s - investorami . html], [h t tp :// blog . babich _ me /2016/03/ startup - zhiznennyj - cycle _ html]

5. Economics and financial support of innovative activity. Workshop: education manual / I. L. Tukkel, S. N. Yashin, E. V. Koshelev. - St. Petersburg: BHV- Petersburg, 2013. - 208 p .: fig. - (Educational literature for universities)

6. Methods evaluations startup Electronic resource Regime access: [https :// habrahabr . ru / company / findstartup / blog /144221/]

7. Venturesome financing. Foundations business Electronic resource Regime access: [http :// www . Grandars _ ru / college / biznes / venchurnoe - finansirovanie . html]

8. Sutula A. V. Attitude of parents regarding the development of children's postural disorders / AND. IN. Crouched // Slobozhanskyi scientific and sports herald. – 2012. – No. 5(2). –WITH. 131–135.

ФІЛОСОФІЯ

Кононенко Т. В.

докторка філософських наук, професорка,
професорка кафедри соціально-гуманітарних дисциплін факультету № 1
Донецького державного університету внутрішніх справ
м. Кропивницький, Україна

КУЛЬТУРА В КОНТЕКСТІ ОБҐРУНТУВАННЯ РОСІЙСЬКОЇ ВОЄННОЇ АГРЕСІЇ

В умовах повномасштабного вторгнення та його підтримки з боку більшості російського суспільства актуалізується необхідність розуміння причини такого негативного ставлення до українського народу. Це пояснюється не лише спланованою державною політикою, фактором пропаганди в засобах масової інформації. У цьому випадку проблема залишається відкритою. На наш погляд, причина криється в базових принципах російської ментальності, в базових положеннях російської культури, перш за все, філософії та літератури. Сприйняття певного народу та певної культури як обраних, елітарних, месіанських породжує неприйняття та заперечення Іншого, бажання його або поглинути, або знищити.

З точки зору Ю. М. Лотмана, для західноєвропейської ментальності більш властивою є тернарна структура, для російської – бінарна. М. О. Бердяєв пише про «особливий душевний уклад», «століттями вихований дуалізм, який увійшов у плоть і кров». У тернарній структурі вибух як неодмінний елемент розвитку будь-якого суспільства не охоплює, не руйнує повністю всю систему. Тернарна структура зберігає певні цінності попереднього періоду. Ідеалом же бінарної структури є тотальне знищення старого, апокаліптичне народження нового. Вибух у бінарній структурі характеризується радикальним максималізмом. «Хто не з нами – той проти нас» – її провідний принцип. Це війна до переможного кінця, повне знищення свого супротивника. Як зазначає С. Л. Франк, характеризуючи російську інтелігенцію початку XX століття, з великої любові народжується велика ненависть, пристрасть до устрою стає пристрастю до руйнування. В ім’я ідеї загальнолюдського щастя, точніше – власного її уявлення, представник російської ментальності та культури готовий пожертвувати і власним життям, і життям іншої людини.

Бінарність обумовлює, по-перше, сприйняття певної соціальної спільноти як обраної, елітарної, по-друге, агресивне ставлення до Іншого. Теза «Москва – Третій Рим», за зауваженням Г. В. Флоровського, з самого

початку у Філофея має апокаліптичний характер, вона пов'язана з падінням Константинополя, Москва – не просто Третій, але Останній Рим, Філофей «застерігає», «не славословить». Проте пізніше лунає претензія на месіанський характер, Москва перетворюється на останнє й єдине істинно християнське царство. В. С. Соловйов виділяє три культури світового значення: мусульманський Схід, католицький і протестантський Захід та православний Слов'янський світ. Ці три культури відповідають трьом силам історичного розвитку: Схід – «силі виняткової єдності», Захід – «силі виняткової множинності», Слов'янський світ – силі, яка «дає позитивний зміст двом першим, звільняє їх від їхньої винятковості, примиряє єдність вищого начала з вільною множинністю приватних форм та елементів, творить таким чином цілість загальнолюдського організму та надає йому внутрішнє тихе життя». М. Я. Данилевский пише про оформлення нового культурно-історичного типу – Слов'янської цивілізації, або Всеслов'янського союзу. Аналізуючи історію, сутність провідних європейських держав, він констатує їхній ворожий, завойовницький характер. На противагу Європі він і пропонує сформувати Всеслов'янський союз. Звичайно, керівна роль відводиться Росії. Маючи «природжену гуманність», якості «доброзичливості, справедливості та чистоти», вона пропонується бути ядром нової цивілізації. Кожен культурно-історичний тип проявляє себе у чотирьох сферах: релігії, культурі, політиці та соціально-економічній сфері. Лише Росія, на думку М. Я. Данилевского, на чолі слов'янських народів може рівномірно на високому рівні представляти всі чотири сфери та бути першим повним культурно-історичним типом. Питання відповідності бажаного реальному залишається відкритим.

За визначенням М. О. Бердяєва, російський народ за своєю природою – жіночий, пасивний. У справі державного будівництва він чекає нареченого, чоловіка. Символічно, що історія державності починається з покликання варягів. Державна влада приходить ззовні. З іншого боку, Росія – бюрократична держава, її інтереси посідають виняткове місце. Держава пригнічує й особистість, й станову систему. Як пише М. О. Бердяєв, ані західницька, ані слов'янофільська філософія історії так і не осягає, чому найбездержавніший народ створює наймогутнішу державність, чому найанархічніший народ підпорядковується найчисельнішій бюрократії. Колектив поглинає особистість. Колектив потребує покори. Покора виступає єдиною формою дисципліни особистості.

В. М. Ільїн наголошує, що Росія – це країна вічної громадянської війни. Російська література принципово не знає в якості позитивного типу, національного героя успішну людину, що «зриває квіти насолоди». Росія орієнтується на аскета, який служить верховному ідеалу. Питання полягає лише в тому, який цей ідеал: іманентний чи трансцендентний. Для одних верховним ідеалом є Царство Небесне, божественна благодать; для інших – Царство Земне, соціальна справедливість і добробут. Прибічники Царства

Небесного жертвують усім, що стосується особистого життя та благополуччя, проживають короткий час у стражданнях і поневіряннях, щоб блаженствувати в майбутньому вічному житті, прибічники Царства Земного також жертвують усім, що стосується особистого життя та благополуччя, але щоб безболісно та ситно блаженствувало майбутнє покоління. Першому ідеалу відповідають аскети Христової ідеї, другому – аскети Антихристової ідеї.

З точки зору Ю. М. Давидова, західноєвропейська філософія (перш за все, Д. де Сад, А. Шопенгауер, Ф. Ніцше) відкриває своєрідний «острів Смерті». Визначальним моментом такого світобачення є не просто втрата віри в Бога, а повна втрата віри в будь-які загальнолюдські ідеали та цінності, в будь-які абсолюти. Наслідком егоцентричного самоствердження стає влада смерті, тому що вона не підвладна людині. Саме смерть не дозволяє людині відчути себе Богом. На наш погляд, якщо західноєвропейська філософія і відкриває «острів Смерті», то російська філософія (перш за все, Ф. М. Достоєвський) відкриває «острів Спокуси». По-перше, людина, будучи «слабкою» та «підступною», постійно спокушається дивом, таємницею та авторитетом – затишним побутом, відсутністю свободи та відповідальності. По-друге, виникають ідеологи та ідеологія спокуси – егоцентризм, абсолютизація свободи, утвердження цінності злочину є головними життєвими принципами «обраних». Образ і подоба дають людині право на безмежну свободу, «самостійне хотіння». Право на злочин, право на кров – екзистенціальний, ціннісний вибір саме людини. По-третє, це культ самотності та руйнування. Герої Ф. М. Достоєвського руйнують і самих себе, свідомо знищуючи здатність любити, і світ довкола себе, стверджуючи виключно власне «Я», мізантропію та агресію.

Фактично, людина, яка сьогодні підтримує російську воєнну агресію, сповідує принцип Родіона Романовича Раскольнікова, який класифікує людей на «звичайних» та «незвичайних». «Звичайні» люди трактуються як нижчий розряд, матеріал, що служить єдино для народження собі подібних. Вони живуть у послуху, не маючи права порушувати закон, «бо вони, бачите, звичайні». Бути слухняними – їхнє призначення. Люди «незвичайні» – законодавці людського роду. Вони мають сказати нове слово. Виходячи з цього, вони можуть всіляко порушувати закон. «Незвичайна» людина «має право... тобто не офіційне право, а сама має право дозволити своїй совісті переступити... через інші перешкоди...», якщо в ім’я ідеї треба «переступити хоча б і через труп, через кров, то вона у собі, по совісті, може… дати собі дозвіл переступити через кров…».

У «Бісах» Шигальов озвучує основні положення нового світопорядку. В основі знаходиться принцип розподілу суспільства на дві нерівні частини: «Одна десята частина отримує свободу особистості та безмежне право над рештою дев’яти десятих». Обрані та маса, правителі та раби – така суть двох нових класів. Відповідно до положень Шигальова, повинна бути «первісна

невинність» – абсолютна рівність. Проте це рівність рабів. «Всі раби й у рабстві рівні». Для цього знижується рівень освіти, науки та мистецтва: «Цицерону відрізується язик, Копернику виколюють очі, Шекспір побивається камінням – ось шигальовщина!». Усувається всяка різниця, будь-яка індивідуальність. «Повна покора, повна безособовість, але раз на тридцять років Шигальов пускає і судому, і всі раптом починають поїдати один одного, до певної риси, щоб не було нудно. Нудьга є відчуття аристократичне; у шигальовщині не буде бажань. Бажання та страждання для нас, а для рабів шигальовщина».

Акцентуємо. На наш погляд, саме культура обумовлює російську воєнну агресію. Російська філософія та література культивує ідею обраності, елітарності, месіанства російського народу, держави та церкви: «Москва – Третій Рим». Як наслідок, інші народи та культури трактуються як другосортні, тому має місце бажання їх поглиблення «руським миром», русифікація. Бінарна структура російської ментальності породжує покору й агресію. З одного боку, пропагується образ «зайвої» та «підпільної» людини, формою екзистенції якої є смирення та страждання. Відсутні аналітика, критичне мислення, поняття честі та гідності. Колективне поглинає особистісне. «Краще смиренно грішити, ніж гордо вдосконалюватись» (М. О. Бердяєв). З іншого боку, допускається право на злочин, право на кров по відношенню до Іншого. Інший трактується як сакральний ворог, для якого передбачається тотальне знищення.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ПРИКЛАДНА ІНФОРМАТИКА

Абаровський С. С.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ПРОБЛЕМИ ВІДДАЛЕНОГО УПРАВЛІННЯ ІТ У МУЛЬТИКУЛЬТУРНИХ ТА МУЛЬТИЗОНАЛЬНИХ ВІРТУАЛЬНИХ КОМАНДАХ

Прискорений розвиток інформаційних та комунікаційних технологій, трансформація ділової активності, що стала більш глобальною та конкурентною, та переважання послуг, заснованих на знаннях та інформації, призвели до появи нових моделей віртуальної командної роботи, більш гнучких та адаптивних, що виходять за рамки класичних функціональних відомчих бар'єрів та вимагають співпраці співробітників з різними навичками, міркуваннями та досвідом. Пандемія COVID-19 прискорила впровадження цих нових моделей роботи в усьому світі в безпрецедентних масштабах. Міжкультурні віртуальні команди можна знайти у кількох областях, таких як дослідження та розробка продуктів, тестування, аутсорсинг, служби підтримки клієнтів та інше.

Інформаційні та комунікаційні технології забезпечують необхідну інфраструктуру для спільної роботи та навчання людей з різних культур та місць. Однак робота у такому форматі все ще викликає деякі складнощі. Саме цьому питанню присвячено це дослідження. У статті будуть розглянуті питання про те, як розвивається спільна робота у мультикультурних віртуальних командах, способи її полегшення та те, що робить роботу в такій команді задовільною та успішною. Також у ході статті будуть розглянуті проблеми, з якими стикаються такі команди та як вирішуються потенційні конфлікти через різне культурне розуміння.

Поняття віддаленого управління ІТ та особливості мультикультурних та мультизональних віртуальних команд

Всупереч філософії «поділу праці» Тейлора, яка характеризувала індустріальну епоху, сьогодні організації використовують більш нову філософію, яка сягає своїм корінням в інформаційну епоху, засновану на командній роботі в різних місцевих, національних, регіональних і навіть міжнародних середовищах. Поруч із драматичною зміною потреба у спілкуванні для людей також зросла в геометричній прогресії. Ця потреба дала поштовх до поширення інформаційних та комунікаційних технологій (ІКТ), а також до народження нових форм медіа, які зробили співпрацю

можливим і дедалі вільнішим від будь-яких тимчасових та просторових обмежень.

Зокрема, безліч синхронних та асинхронних веб-інструментів використовується для підтримки та полегшення співпраці між розподіленими командами та окремими людьми по всьому світу, які беруть участь у «віртуальних» спільнотах чи організаціях для навчання та роботи, які почали експоненційно процвітати. Такі спільноти, у свою чергу, постійно і по-новому пропонують можливості, які сприяють співпраці та обміну знаннями між членами команди [1].

Щодо віртуальних команд, то в літературі пропонуються різні визначення. До складу таких команд можуть входити люди з різних відділів, організацій, країн та культур. Однак спільним знаменником цих різних визначень є визнання того, що члени віртуальних команд живуть, працюють або навчаються в різних географічних областях та часових поясах, і що вони зазвичай використовують інформаційні та комунікаційні інструменти.

Натомість, віддалене управління ІТ включає в себе використання технологій комунікації для організації та керування віддаленими робочими групами. Це вимагає використання веб-платформ, спільного доступу до документів та інших інструментів, які дозволяють ефективно спілкуватися та співпрацювати на відстані.

Віддалене управління ІТ у мультикультурних та мультизональних віртуальних командах може мати багато переваг, таких як глобальний доступ до талантів, зниження витрат на офісне простір та гнучкість у роботі. Однак, існують проблеми, пов'язані з комунікаційними перешкодами, культурним контекстом, географічними відстанями та будівництвом довіри та взаємодії.

Більше того, оскільки багато людей, групи та організації з різних країн вважають за краще використовувати такі віртуальні команди для роботи та інших завдань, на їх ефективність може прямо (чи опосередковано) впливати культурний контекст, який члени команди привносять до умов навчання чи продуктивності. У цьому контексті безлічі культур використання передових ІКТ для спільної роботи пропонує потенціал для ефективної роботи та просування мультикультурного взаєморозуміння між громадянами різних країн. Отже, це дослідження зосереджено на чинниках та проблемах, які впливають успіх спільної роботи мультикультурних віртуальних команд [2].

Проблеми віддаленого управління ІТ у мультикультурних та мультизональних віртуальних командах

Щоб з'ясувати основні чинники, що впливають на успіх спільної мультикультурної командної роботи у віртуальному середовищі; було проведено вивчення великого списку літератури за такими ключовими словами, як мультикультура, віртуальні команди, співпраця, міжкультурна взаємодія, ІКТ, комп'ютерна комунікація. Таким чином, у ході дослідження виявилося сотні журнальних статей та матеріалів конференцій. У ході

вивчення були виділені основні проблеми дистанційного управління в ІТ, з якими можна ознайомитися далі [3].

2.1. Комунікаційні перешкоди та міжкультурна комунікація

У мультикультурних віртуальних командах виникають мовні бар'єри, оскільки учасники можуть розмовляти різними мовами. Різниця в культурних відмінностях також може призводити до непорозумінь та помилкового сприйняття повідомлень. Недостатня невербальна комунікація також може ускладнювати спілкування та розуміння.

У великій кількості літератури повідомляється, що культурні відмінності створюють труднощі ефективного спілкування між членами віртуальних команд. Мовний бар'єр, своєю чергою, обмежує рівень спілкування через відмінностей у нормах соціальної взаємодії всередині спільноти. На додаток до мови простір, час, жести тіла та стиль письма мають різні значення у кожній культурі. Деякі культури люблять зберігати дистанцію під час спілкування віч-на-віч, тоді як для інших тілесний контакт є дуже важливою частиною взаємодії. Різні культури по-різному визначають час і надають різного значення минулому, сьогоденню та майбутньому. З іншого боку, словниковий запас, граматика і значення часу дуже різняться у світі [3].

Варто зазначити, що ключовою проблемою для багатьох членів команди, для яких англійська не є рідною мовою, є швидкість, з якою говорять багато носіїв англійської мови. Це особливо складно, коли розмови відбуваються в Інтернеті, оскільки сигнали, на які можна покластися при зустрічі віч-на-віч, такі як мова тіла, відсутні. Члени команди, які є носіями англійської мови, повинні говорити чітко та уникати розмовних виразів чи сленгу. Якщо теми розмови пов'язані з складнішою мовою, рекомендується заздалегідь поділитися можливими допоміжними матеріалами з носіями мови, щоб вони мали можливість ознайомитися з будь-якою відповідної термінологією [3].

2.2. Культурний резонанс та управління

Розуміння культурних особливостей є ключовим аспектом управління мультикультурними віртуальними командами. Керівники повинні бути готові адаптувати свої управлінські практики до різних культур, розуміти різницю в стилях роботи та комунікації.

Один із найбільших пріоритетів для глобальних команд – зрозуміти вплив культури на те, як можуть працювати крос-культурні співробітники. Культура значно впливає на ключові галузі бізнесу, такі як ставлення до термінів, стилі спілкування, підхід до зворотного зв'язку, управління конфліктами, стилі управління та побудова відносин.

Компанії, які не знаються на цих галузях або зменшують їх важливість, швидше за все, матимуть менш продуктивні команди, проблеми з комунікацією та конфлікти; що призводить до поганої роботи віддалених та віртуальних команд.

Розуміння критичних областей культури та розуміння необхідності того, щоб члени команди оцінювали та поєднували їх, полегшить реалізацію величезних переваг міжкультурної роботи, які стають у команді на ранньому етапі, важливо усвідомлювати роль культури у таких галузях, як спілкування, підходи до конфлікту тощо. [4].2.3. Географічні відстані та часові пояси

Відстань та різні часові пояси можуть створювати справжні виклики для спілкування та координації віртуальної команди. Синхронізація робочих графіків та пошук компромісів щодо часових зон є важливими аспектами успішного віддаленого управління [4].

Рекомендації для подолання проблем віддаленого управління ІТ у мультикультурних та мультизональних віртуальних командах

Є декілька простих рекомендацій, які допоможуть віртуальним командам подолати проблеми віртуального управління. До таких рекомендацій можна віднести наступне:

1. Покращення комунікації. Для подолання комунікаційних перешкод рекомендується використовувати технології відеозв'язку та спільного редагування документів. Створення культури відкритості та взаєморозуміння також є важливим аспектом ефективної комунікації.

2. Приділити увагу культурній освіті та тренінгам. Навчання культурній чутливості та міжкультурним навичкам допоможе усунути культурні бар'єри та покращити спілкування в мультикультурній команді. Керівники повинні отримати підготовку щодо роботи з мультикультурними віртуальними командами.

3. Інтегрувати ефективне управління часом та часовими поясами. Встановлення чітких графіків роботи та спілкування допоможе уникнути конфліктів, пов'язаних з різними часовими поясами. Використання інструментів для планування та координації часових зон є необхідним. Такі інструменти, як глобальні календарі, спільні графіки роботи та засоби для розкладу зустрічей, можуть сприяти ефективному управлінню часом.

В результаті це все дозволить створити сприятливе робоче середовище. В такому випадку забезпечення можливості взаємодії та обміну ідеями є ключовим фактором успіху мультикультурних та мультизональних віртуальних команд. Командам необхідно мати доступ до інструментів спільної роботи, форумів обговорень та віртуальних просторів для спілкування. Підтримка взаємної довіри та співпраці також є важливою, і керівники повинні виконувати роль посередника та сприяти зміцненню взаємодії між учасниками команди [5].

У статті розглянуті проблеми віддаленого управління ІТ у мультикультурних та мультизональних віртуальних командах. Комунікаційні перешкоди, культурний контекст, географічні відстані та будівництво довіри є ключовими проблемами, з якими стикаються такі команди. Пропонуються рекомендації для подолання цих проблем, включаючи покращення

комунікації, культурну освіту та тренінги, ефективне управління часом та створення сприятливого робочого середовища.

Список використаних джерел:

1. Гілсон Л. Л. та Шеллі К. Е. (2004). Трохи креативності має велике значення: перевірка участі команд у творчих процесах. Журнал управління, 30 (4), 453-470.

2. Сміт Дж. та Джонсон М. (2020). Віддалене управління IT у мультикультурних віртуальних командах. Журнал міжнародного менеджменту, 26(4), 100760.

4. Лі Х. та Лю Ю. (2021). Проблеми та стратегії управління мультикультурними віртуальними командами в IT-проектах. У матеріалах Міжнародної конференції з Інтернету та електронного бізнесу (стор. 343-348).

5. Хедекар С. та Джоші С. (2019). Проблеми управління мультикультурними командами у віртуальному проектному середовищі. Міжнародний журнал науки та досліджень, 8(7), 2319-7064.

6. Тайт, М. (2018). Культурні проблеми управління віртуальними командами. У міжнародному управлінні людськими ресурсами (с. 269-293). Routledge.

Веретюк О. М.

Студент, Akademie HUSPOL s.r.o.,
м. Куновіце, Чеська Республіка

Веретюк С. М.

PhD, старший викладач, Поліський національний університет,
м. Житомир, Україна

НОВІ ТЕНДЕНЦІЇ В РОЗГОРТАННІ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ: 5G, LPWAN ТА ХМАРНІ СЕРВІСИ

Інтернет речей (IoT) перетворюється на ключову технологію в багатьох галузях, надаючи можливість збирати, аналізувати та використовувати дані з підключених пристроїв для управління та оптимізації процесів. Розгортання мереж Інтернету речей швидко розвивається за рахунок нових технологій, що покращують зв'язок, масштабованість та управління даними. Приведені тези описують останні тенденції в розгортанні мереж Інтернету речей, зокрема 5G, LPWAN та використання хмарних сервісів, їх переваги та використання в різних галузях. Розуміючи та впроваджуючи ці тенденції, організації можуть використовувати повний потенціал мереж Інтернету речей і відкривати нові можливості для інновацій та ефективності.

5G - це бездротова мережева технологія останнього покоління, яка пропонує значно вищі швидкості, меншу затримку та більшу пропускну здатність порівняно зі своїми попередниками. Технологія 5G спрямована на забезпечення безперебійного підключення для широкого діапазону пристроїв, включаючи пристрої Інтернету речей. 5G має низьку затримку між передачею даних і отриманням відповіді (латентність). Низька затримка дозволяє оптимізувати мережу 5G для обробки величезних обсягів швидкозмінних даних у реальному часі. Мережі 5G підтримують масове розгортання IoT, можуть підтримувати велику кількість підключених пристроїв, це забезпечує масштабованість для розгортання великих IoT-мереж та масивних сенсорних систем, які потребують одночасного з'єднання багатьох пристроїв, наприклад, в промисловості або міських інфраструктурних проєктах [1]. Технологія 5G завдяки своїм перевагам знаходить застосування в багатьох нових сферах, наприклад: автономні (безпілотні) транспортні засоби, промислова автоматизація, охорона здоров'я, ритейл, логістика та ін. [2].

Технології LPWAN (мережі з низьким споживанням енергії та великим радіусом дії) набувають популярності у розгортанні мереж Інтернету речей завдяки здатності забезпечувати довготривалий та енергоефективний зв'язок для пристроїв Інтернету речей. Технології LPWAN, такі як LoRaWAN,

NB-IoT та Sigfox, надають ефективний та економічний спосіб підключення пристроїв IoT на великій відстані. Ці технології пропонують великий термін служби батареї для пристроїв Інтернету речей, працюють в неліцензованому або ліцензованому діапазоні та підтримують масштабованість [3]. Застосування LPWAN успішно знайшло в різних галузях, включаючи сільське господарство (моніторинг показників грунту, стану рослин, метеостанції), логістику (відстеження активів та управління запасами), розумні будівлі (моніторинг показників лічильників, параметрів приміщень загального користування та ін.).

Хмарні сервіси відіграють важливу роль у розгортанні мереж Інтернету речей, надаючи масштабовану інфраструктуру, ресурси для зберігання даних та можливості обробки. Хмарні платформи дозволяють організаціям збирати, зберігати та аналізувати величезні обсяги даних, що генеруються пристроями Інтернету речей. Вони дозволяють моніторинг в реальному часі, прогнозуючий аналіз та віддалене управління пристроями. Хмарні сервіси також сприяють безпроблемній інтеграції з іншими системами підприємства та забезпечують масштабованість для врахування зростаючої кількості підключених пристроїв. Використання хмарних сервісів в розгортанні Інтернету речей включає в себе такі сфери, як обробка, аналітика даних, відстеження активів, прогнозування обслуговування та віддалений моніторинг. Серед хмарних сервісів що мають найбільший функціонал та можливості для IoT можна виділити Amazon Web Services (AWS) IoT Platform, Microsoft Azure IoT , Google IoT, IBM Watson IoT.

Інтеграція технологій 5G, LPWAN та хмарних сервісів відкриває нові можливості для розгортання мереж IoT. Ці технології доповнюють одна одну, надаючи комплексне рішення для різних кейсів Інтернету речей. Організації можуть використовувати швидкість та низьку затримку 5G для критичних застосунків та локацій з великою густотою кінцевих пристроїв, тоді як технології LPWAN пропонують економічний та довготривалий зв'язок для енергоефективних пристроїв Інтернету речей у віддалених місцях [4]. Хмарні сервіси надають інфраструктуру та можливості управління, обробки та аналізу даних, зібраних з підключених пристроїв. Побудова мереж та хмарних рішень дозволяє швидко реалізовувати проєкти різних напрямків та масштабів, оператори та компанії можуть втілювати як публічні рішення (розумні міста, моніторинг навколишнього середовища), так і приватні проєкти для замовників з широкого спектру секторів, включаючи промисловість, транспорт, охорону здоров'я, агропромисловість та ін.

Розгортання мереж IoT залежить від успішного вирішення викликів, пов'язаних зі збільшенням обсягу даних, безпекою та конфіденційністю. Організації повинні забезпечувати надійність мережі, резервне копіювання даних та моніторинг мережі для запобігання перебоям в роботі. Забезпечення безпеки даних, включаючи дотримання регуляторних вимог, таких як GDPR та CCPA, має вирішальне значення для захисту конфіденційності

користувачів. Необхідно знайти баланс між ідентифікацією та контролем доступу, необхідними для функціонування Інтернету речей, та правами користувачів на конфіденційність та ідентичність [5]. Крім того, організації повинні дотримуватись принципів приватності, регулярно проводити аналіз вразливостей та слідкувати за появою нових технологій безпеки для вирішення потенційних ризиків превентивно.

Узагальнюючи, IoT швидко розвивається завдяки новим технологіям, таким як 5G, LPWAN та хмарним сервісам. Ці тенденції формують майбутній вигляд мереж Інтернету речей та відкривають безліч можливостей для покращення зв'язку, ефективності та інновацій у різних галузях, дозволяють організаціям розкрити новітні шляхи підвищення ефективності та росту бізнесу. Інтеграція цих технологій дозволяє створити комплексне рішення для розгортання мереж Інтернету речей і покращити взаємодію між пристроями та системами. Повсюдне підключення до IoT може бути досягнуто для обслуговування як міських, так і недостатньо обслуговуваних віддалених районів, таких як сільські райони, шляхом розгортання мобільних мереж 5G та далекобійних, малопотужних мереж з низьким енергоспоживанням (LPWAN). Організації повинні бути свідомими при використанні цих тенденцій і адаптувати свої стратегії для використання повного потенціалу мереж Інтернету речей. Забезпечення безпеки, конфіденційності та надійності є ключовими аспектами для успішного розгортання мереж Інтернету речей.

Список використаних джерел:

1. GSMA Global System for-Mobile Communication Alliance: Internet of Things in the 5G Era: Opportunities and Benefits for Enterprises and Consumers, 2019, [online] Available: https://www.gsma.com/iot/wp-content/uploads/2019/11/201911-GSMA-IoT-Report-IoT-in-the-5G-Era.pdf.

2. Khuntia, Mitrabinda, Debabrata Singh, and Sipra Sahoo. "Impact of Internet of Things (IoT) on 5G." Intelligent and Cloud Computing: Proceedings of ICICC 2019, Volume 2. Springer Singapore, 2021.

3. Patel, Dhaval. Low power wide area networks (lpwan): Technology review and experimental study on mobility effect. South Dakota State University, 2018.

4. Ogbodo, Emmanuel Utochukwu, Adnan M. Abu-Mahfouz, and Anish M. Kurien. "A Survey on 5G and LPWAN-IoT for improved smart cities and remote area applications: From the aspect of architecture and security." Sensors 22.16 (2022): 6313.

5. Wachter, Sandra. "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR." Computer law & security review 34.3 (2018): 436-449.

Іванов М. О.

Студент, Akademie HUSPOL s.r.o.,
м. Куновіце, Чеська Республіка

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МІКРОСЕРВІСНОЇ ТА МОНОЛІТНОЇ АРХІТЕКРУТИ ПРОЕКТІВ

При побудові проектів незалежно від їхньої складно, необхідно зробити аналіз та вибрати основну архітектуру на якій буде побудована вся платформа. Архітектура програмного забезпечення системи - це набір структур, необхідних для обґрунтування система, яка містить елементи програмного забезпечення, зв’язки між ними та властивості обох [1]. Структура - це просто набір елементів які утримуються разом за допомогою відношень. Існує три категорії архітектурних структур, які будуть відігравати важливу роль у проектуванні, документуванні та аналізі архітектури:

1. Структури які розбивають системи на модулі. Їм призначаються конкретні обчислювальні обов’язки та вони є основою робочих завдань для команд розробки
2. Динамічні структури, тобто вони зосереджені на способі взаємодії елементів один до одного під час виконання для забезпечення функцій системи
3. Третій тип описує відображення структур програмного забезпечення в організаційне середовище системи, середовище розробки, розгортання та виконання.

Існує 3 найпоширеніших типи архітектури які будуються за допомогою різних структур і широко використовуються компаніями:

1. Монолітна
2. Мікросервісна
3. Сервіс-орієнтовна

Якщо узагальнити, то сервіс-орієнтована архітектура є середнім між монолітною та мікросервісною архітектурами. Сервісно-орієнтована архітектура - це підхід до проектування, при якому кілька служб співпрацюють, щоб забезпечити певний кінцевий набір можливостей. Служба тут зазвичай означає повністю окремий процес операційної системи. Зв'язок між цими службами відбувається через виклики в мережі, а не через виклики методів у межах процесу [2]. Кожен сервіс може буди достатньо великим там мати властивості моноліта, але при цьому залишатись вузькоспеціалізованим та відповідати за конкретні функції. Прикладом можуть бути такі сервіси проекту як сервіс повідомлень, фронтенд для користувача, сервіс обробки картинок. Так як цей підхід є спільним для двох інших, тому краще розглянути детально монолітну та мікросервісну

архітектури окремо і визначити їх недоліки та переваги які допоможуть зробити правильний архітектурний вибір. Для цього слід розглянути кожен підхід і що він являє собою.

Монолітна архітектура

Вперше це поняття було використане спільнотою UNIX для пояснення виникнення великих і комплексних програм які не можуть взаємодіяти із іншими програмами [3]. Монолітна програма, побудована як єдине ціле. Корпоративні програми часто складаються з трьох основних частин: інтерфейс користувача на стороні клієнта (що складається з HTML-сторінок і javascript, запущених у браузері на комп'ютері користувача), база даних і програму на стороні сервера. Серверна програма оброблятиме HTTP-запити, виконуватиме логіку домену, отримуватиме та оновлюватиме дані з бази даних, а також вибиратиме та заповнюватиме представлення HTML для надсилання в браузер. Ця серверна програма є монолітом - одним логічним виконуваним файлом [3]. Будь-які зміни в системі передбачають створення та розгортання нової версії серверної програми. Моноліти можуть бути зручними на ранніх стадіях життя проекту для полегшення керування кодом і розгортання. Це дозволяє оновити все в моноліті одночасно.

На перший погляд система виглядає як сутність в якій все дуже сильно пов'язано і незалежності структур практично не існує. Все ж таки існують механізми виокремлення специфічних частин, які можуть бути розподілені у локальні підсистеми та перевикористані у різних частинах проекту. Це дозволяє локалізувати спільну логіку для ефективного використання, виправлення чи рефакторингу.

Переваги:

- Взаємодія з іншими компонентами через виклик методів, а не через мережу
- Відносна простота у забезпеченні консистеності даних
- Обмежений набір технологій
- Легкість у повторному використанні коду
- Простота у розгортанні та моніторингу

Недоліки:

- Складніше підтримувати кодову базу в чистоті
- Вимагає більшої кількості досвідчених інженерів
- Дороге масштабування
- Довге розгортання
- Погана стійкість до відмов сервісу
- Команди можуть заважати один одному

Мікросервісна архітектура

Мікросервіси - це архітектурний стиль, який структурує програму як набір сервісів, які розгортається самостійно, слабо зв'язані, організовані навколо можливостей бізнесу, належать невеликій команді. Архітектура мікросервісу забезпечує організації можливість швидко, часто, надійно та

стабільно реалізувати великі та складні програми, що є необхідністю для конкуренції в сучасному світі [4].

Розробка програмного забезпечення найчастіше застосовується для автоматизації процесів, які існують у реальному світі [5]. Система мікросервісів не може бути відокремлена від реального світу, тому для її ефективної реалізації треба розуміння домену для якого буде виконана архітектура. Доменно-орієнтоване проектування - це основний підхід до розробки програмного забезпечення, який будується згідно із знаннями експертів із цієї області. У рамках доменно-орієнтованого проектування структура та мова програмного коду мають відповідати бізнес-домену. Тому маючи розуміння домену, можна спланувати правильну архітектуру яка буде включати відповідну пов’язаність компонентів, їх взаємодію між собою та зв’язність всередині кожної окремої структури.

Переваги:

- Команди працюють незалежно
- Швидке розгортання
- Простіші в розробці компонент
- Інструменти підібрані під потреби
- Легко масштабувати пляшкове горло

Недоліки

- Взаємодія через мережу
- Часто вимагає архітектора
- Складне інтеграційне тестування
- Складно забезпечувати консистентність
- Вимагає високого рівня автоматизації
- Складне повторне використання
- Складний моніторинг
- Зоопарк технологій

У кожного проекту існують різні стадії розвитку і в залежності від цього вибираються різні архітектурні підходи, бо в кожного із них є свої переваги та недоліки. Кодові бази з часом зростають, коли ми пишемо код для додавання нових функцій. Згодом може бути важко зрозуміти, де потрібно додати зміни, оскільки кодова база дуже велика. Незважаючи на прагнення до чітких, модульних монолітних кодових баз, занадто часто ці довільні межі в процесі руйнуються. Код, пов'язаний зі схожими функціями, починає поширюватися більше, що ускладнює виправлення помилок або впровадження. Тому на початкових стадіях часто реалізується монолітна архітектура де швидкість розробки на початку вища а із розвитком проекту, збільшенням кількості розробників та зростом навантаження на систему є доцільним перехід на мікросервісну архітектуру.

Список використаних джерел:

1. *Len Bass, Paul Clements, Rick Kazman "Software Architecture in Practice (SEI Series in Software Engineering) 4th Edition", Print2print, 2021. - 442*
2. *Sam Newman "Building Microservices, 2nd Edition", O'Reilly Media, Inc. 2021. - 500*
3. *Eric S. Raymond "Art of UNIX Programming, The 1st Edition, Kindle Edition", Addison-Wesley Professional, 2003. - 560*
4. *https://microservices.io/*
5. *Eric Evans "Domain-Driven Design: Tackling Complexity in the Heart of Software", Addison-Wesley Professional. 2004. - 534*

Курочка С. В.

Студент, Akademie HUSPOL s.r.o.,
м. Куновіце, Чеська Республіка

АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ПРОМИСЛОВОГО ПРОТОКОЛУ ЗВ'ЯЗКУ MODBUS В СИСТЕМІ РОЗУМНОГО БУДИНКУ В ПОРІВНЯННІ З ПОШИРЕНИМИ ПРОТОКОЛАМИ

Найпоширеніші на сьогодні протоколи та мережі зв’язку використовують для систем управління пристроями розумного будинку: 1-Wire, X10, KNX, Wi-Fi, Z-Wave, BLE і ZigBee.

Для розуміння ознайомимось з кожним протоколом окремо. Перший протокол 1-Wire побудований на основі двонаправленої шини зв’язку, яка в свою чергу складається лише з двох провідників, що також можуть використовуватись і для живлення пристроїв, один з них - земля, а інший - передача інформації. Зазвичай працює на швидкості 15,4 Кбіт/с, а максимальна 125 Кбіт/с [9].

Використовується для зв’язку з простими і дешевими пристроями такі як зовнішній термометр. Відстань передачі даних до 300 метрів.

Домашню електромережу використовує X10 – протокол. Передача сингалу відбувається за допомогою короткочасного радіочастотного імпульсу 120 кГц та синхронізується з моментом переходу змінної напруги через нуль [4]. Модулі передачі зазвичай підключаються до звичайної розетки. Використання мережі накладає на протокол багато обмежень, через унеможливлення проходження повз трансформатори або між фазами. Також імовірне заглушення сигналу пристроями, які в блоках живлення мають конденсатори та низький вхідний опір. Мають дуже малу швидкість, ¾ секунди іде лише передача адреси пристрою та команди. На швидкість впливає мережа, стандарт європейської 50 герц/ менша швидкість, а американської ж 60 герц/ вища швидкість [10].

KNX – децентралізована однорангова мережа з управлінням за допомогою подій. Підтримує різні середовища передачі даних, а саме – вита пара (KNX TP), IP мережа (KNX IP), радіоканал (KNX RF), силова лінія (KNX PL). Швидкість відповідно варіюється в залежності від середовища передачі даних. Для конфігурування мережі потрібно використання спеціалізованого інженерного програмного забезпечення. Має досить широкий спектр підтримуваних пристроїв, таких як різноманітні сенсори, виконуючі пристрої (різні актуатори) та системні пристрої [7].

Наступним є Wi-Fi – набір стандартів безпровідної мережі для створення локальних мереж, з великим потоком даних. Застосування та призначення набагато ширше чим просто комунікація розумних пристроїв.

Основними діапазонами вважаються 2,4 ГГц та 5 ГГц. Принцип роботи базується на використанні як мінімум одної точки доступу та клієнтських пристроїв. Швидкості варіюються від 11Мбіт/с до 30 Гбит/с в залежності від стандарту, який використовується [8]. Також достатня кількість розумних пристроїв, що можуть спокійно працювати з даними мережами, які мають як багато переваг так і певні недоліки.

Ще маємо протокол Z-Wave безпровідного зв'язку, який створений для домашнього автоматизування. Технологія використовує малопотужні і маленькі за розмірами радіо модулі. Працює в діапазоні до 1 ГГц, що надає змогу працювати в спектрі з меншою кількістю перешкод в порівнянні з частотами Wi-Fi, Bluetooth. Використовується для створення недорогої і енергоефективної електроніки, яка може працювати навіть на батарейках. Зв'язок цього стандарту строється на основі Mesh мережі [12]. Лише деякі виробники виробляють пристрої з відкритим кодом та доступним і зрозумілим API. Прикладами пристроїв з підтримкою даного протоколу можуть бути пульти управління, датчики руху, датчики вологості, датчики диму, датчики температури та інші пристрої.

Ще одним з найпоширеніших протоколів є BLE – спеціальна версія ядра бездротової технології передачі даних Bluetooth, основною перевагою якого являється дуже мале пікове енергоживлення [5]. Ця технологія дозволяє використовувати в даних пристроях батарейку як елемент живлення, та звісно не великий розмір пристроїв. Цю технологію широко використовують в галузі фізкультури та спорту, медицини, охоронних систем та домашніх розваг. Використовується в схемах які вживають ZigBee специфікацию протокола верхнього рівня. Чіпи з підтримкою технології активно застосовують в наручних смарт часах, геймпадах, датчиках, які вимірюють життєві показники, ПК, телефонах та багато іншого. Також активно послуговуються для домашньої автоматизації [6].

І останній з нашого списку протокол, це – ZigBee – специфікація мережевих протоколів верхнього рівня яка описує взаємодію пристроїв як на рівні програми, так і мережевому рівні з доступом до фізичного MAC адресу пристрою [11]. Цей стандарт орієнтований на пристрої яким необхідна гарантована безпека передачі даних і не необхідна велика швидкість, але важлива енергоефективність. Підтримує не лише прості топології мережі як «деревоподібна» чи «зіркоподібна», а й самовідновлюючу мережу типу «mach». В Європі використовують частоту 868 МГц, в Америці та Австралії 915 Мгц, а в більшості інших країн використовують 2,4 ГГц. Специфікація широкодоступна лише при некомерційному використанні. Для застосування в комерційних продуктах необхідна реєстрація в альянсі ZigBee, що не дає можливості розробникам використовувати інші програмні продукти, які розповсюджуються по ліцензіях вільного програмного забезпечення.

Тепер же перейдемо до нашого протоколу Modbus. Це відкритий комунікаційний протокол, побудований на архітектурі Master – Slave. Використовується для організації зв'язку електронних пристроїв в промисловості. Може використовувати послідовні лінії зв'язку RS232, RS422, RS485 та мережі TCP/IP. Стандарт складається з наступних частин: Modbus Application Protocol – специфікація прикладного рівня мережевої моделі OSI; Modbus over serial line – специфікація фізичного та канального рівня мережевої моделі OSI для RS323 та RS485; Modbus Messaging on TCP/IP Implementation Guide – специфікація для роботи через TCP/IP стек [3].

Перевагою даного стандарту є масовість та відкритість протоколу. Навіть на сьогоднішній день виробляється велика кількість пристроїв які використовують в своїй роботі протокол Modbus, такі як різноманітні датчики, реле, актуатори, модулі для обробки сигналів. Також всі пристрої, які використовуються для контроля в промисловості підтримують даний протокол.

Отже, на сьогодні достатня кількість пристроїв, які можна використовувати для автоматизацій будинку. Тож перевагою для використання даного протоколу є доступність великої кількості готових бібліотек для управління такими пристроями, які легко підключити при написанні програмного забезпечення, та можливість їх безоплатного використання. Але все ж таки є недоліки при використанні Modbus. Був розроблений стандарт більше ніж 40 років тому, коли потужність процесорів була значно нижчою, і тоді не був задіяний ніякий захист даних в виді шифрування, щоб не перевантажувати залізо. Тому для використання віддаленого управління такими пристроями потрібно додатково використовувати VPN – тунелі. Відсутні методи за допомогою яких Slave пристрої можуть помітити відсутність зв'язку з Master пристроєм. Не дуже приємним бонусом є проблема з неможливістю зчитувати регістри даних у довільному порядку, тому це збільшує затримки при роботі мережі. Також стандарт не має регламенту по стартовій ініціалізації пристроїв, що може викликали складнощі, якщо мережа має велику кількість пристроїв. Ще одним мінусом в порівнянні з більш новим протоколом, таким як ZigBee, є менша енергоефективність пристроїв.

Тому, якщо враховувати всі переваги і недоліки пристроїв працюючих з Modbus, цілком можливе комфортне використання в домашній автоматизації, якщо побудова системи планується власними руками.

Список використаних джерел:

1. Бібліотека Wire [Електронний ресурс] / Ардуїно в Україні – https://doc.arduino.ua/ru/prog/Wire

2. Белковский С.В. Анализ протокола в системах полевых шин // Теоретические и прикладные аспекты информационных технологий: Сб. науч. тр. / НИИУМС. – Пермь, 1999. – Вып. 48. – С. 136-138.

3. Как общаются машины: протокол Modbus [Электронный ресурс] / Хабр – https://habr.com/ru/companies/advantech/articles/450234/

4. Развернутое описание протокола X-10 [Электронный ресурс] / Новости энергетики – https://marketelectro.ru/content/razvernutoe-opisanie-protokola-x10

5. BLE [Електронний ресурс] / Вікіпедія – вільна енциклопедія – https://en.wikipedia.org/wiki/Bluetooth_Low_Energy

6. BLE под микроскопом [Электронный ресурс]/ Хабр - https://habr.com/ru/articles/319244/

7. KNX [Электронный ресурс] / Википедия – свободная энциклопедия – https://ru.wikipedia.org/wiki/KNX

8. Wi-Fi [Электронный ресурс] / Википедия – свободная энциклопедия – https://ru.wikipedia.org/wiki/Wi-Fi

9. 1-Wire [Електронний ресурс] / Вікіпедія – вільна енциклопедія – https://en.wikipedia.org/wiki/1-Wire

10. 1-Wire [Электронный ресурс] / Википедия – свободная энциклопедия – https://ru.wikipedia.org/wiki/X10

11. ZigBee [Электронный ресурс] / Википедия – свободная энциклопедия – https://ru.wikipedia.org/wiki/Zigbee

12. Z-Wave [Электронный ресурс] / Википедия – свободная энциклопедия – https://ru.wikipedia.org/wiki/Z-Wave

Трофименко О. В.

Студент, Akademie HUSPOL s.r.o.,
м. Куновіце, Чеська Республіка

АНАЛІЗ ПЕРЕВАГ І ОБМЕЖЕНЬ ВПРОВАДЖЕННЯ ШІ В УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Зі збільшенням використання технологій у цифрову епоху інформаційна безпека стала критичною проблемою для організацій. Штучний інтелект (ШІ) став потенційним рішенням для управління інформаційною безпекою. Тим не менше, такі підходи мають і свої недоліки, а отже процес прийняття рішення щодо впровадження ШІ в управління інформаційною безпекою має включати аналіз переваг і обмежень.

Проведення аналізу переваг і обмежень в процесі прийняття рішення щодо впровадження ШІ в управління інформаційною безпекою.

Штучний інтелект (ШІ) є потенційним рішенням для управління інформаційною безпекою, оскільки він має можливість аналізувати великі обсяги даних та виявляти шаблони, які можуть вказувати на потенційні загрози безпеці [1]. Використання ШІ в управлінні інформаційною безпекою також має свої обмеження. Один з них - це можливість отримання помилково позитивних (False Positive) та негативних результатів (False Negative), що може призвести до або непотрібних сповіщень, або пропущених загроз. Іншим обмеженням є ризик упередженості алгоритмів ШІ, що може призвести до неточних або дискримінаційних результатів. Крім того, існують збої щодо можливост

З огляду на потенційні переваги впровадження штучного інтелекту в управлінні інформаційною безпекою можна навести наступні приклади:

1. Моніторинг у режимі реального часу: ШІ можна використовувати для моніторингу мережевої активності та виявлення незвичайної поведінки. Наприклад, системи виявлення вторгнень, чи Network intrusion detection systems (NIDS) на основі ШІ можуть виявляти та запобігати кібератакам, відстежуючи мережевий трафік на наявність аномалій [2].

2. Автоматизація процесів безпеки: AI може автоматизувати процеси безпеки, такі як виявлення загроз і реагування на них, що може заощадити час і ресурси для команд безпеки.

3. Прогнозування загроз безпеці: штучний інтелект може аналізувати великі обсяги даних, щоб виявити закономірності та передбачити потенційні загрози безпеці. Наприклад, алгоритми машинного навчання можуть аналізувати дані журналу, щоб виявити аномальну поведінку, яка може свідчити про загрозливу кібератаку.

4. Покращене реагування на інциденти: штучний інтелект може допомогти командам безпеки ефективніше реагувати на інциденти безпеки, забезпечуючи аналіз у реальному часі та можливості прийняття рішень. Наприклад, системи безпеки на основі штучного інтелекту можуть забезпечувати автоматичні реакції на інциденти безпеки, такі як ізоляція заражених машин або блокування шкідливих IP-адрес.

5. Постійне навчання та вдосконалення: ШІ може вчитися на минулих інцидентах безпеки та адаптуватися до нових загроз, підвищуючи загальну ефективність заходів безпеки. Наприклад, системи безпеки на основі ШІ можуть використовувати машинне навчання, щоб постійно оновлювати свої можливості виявлення загроз на основі нових даних і відгуків аналітиків безпеки.

Хоча впровадження ШІ в управління інформаційною безпекою має потенційні переваги, є також деякі недоліки, які слід враховувати. Нижче наведено три пункти з прикладами:

1. Відсутність прозорості та можливості інтерпретації: складність алгоритмів штучного інтелекту може ускладнити інтерпретацію їхніх рішень, що може призвести до відсутності прозорості та підзвітності в управлінні безпекою. Наприклад, якщо система безпеки на основі ШІ блокує доступ законного користувача до системи, може бути важко зрозуміти, чому було прийнято таке рішення [3].

2. Вразливість до агресивних атак: системи безпеки на основі штучного інтелекту можуть бути вразливі до агресивних атак, коли зловмисники намагаються маніпулювати або обманювати систему, щоб обійти заходи безпеки. Наприклад, зловмисник може використовувати методи машинного навчання для створення підроблених даних [4].

Аналіз переваг і обмежень впровадження ШІ в управління інформаційною безпекою показує, що ШІ може принести значну користь, але також існують ризики та виклики, які потрібно враховувати. ШІ може допомогти забезпечити моніторинг реального часу, автоматизацію процесів безпеки, передбачення потенційних загроз, поліпшення відповіді на інциденти та постійного навчання та вдосконалення. Однак, ризики включають перенасичення на ШІ, відсутність прозорості та інтерпретовності алгоритмів ШІ та вразливість до атак. Управління інформаційною безпекою повинно враховувати ці переваги та обмеження та приймати рішення з урахуванням цих факторів.

Список використаних джерел:

1. Луїс Вейр. Enterprise API Management: Design and deliver valuable business APIs. Лондон: Packt Publishing Ltd, 2019. 270 с.

2. Алессандро Парізі, Hands-On Artificial Intelligence for Cybersecurity. Лондон: Packt Publishing Ltd, 2019, 307 с.

3. Леслі Ф. Сікос, AI in Cybersecurity. Чам: Springer International Publishing, 2018, 205 с.

4. Ішаані Пріядаршіні, Рохіт ШармаArtificial Intelligence and Cybersecurity: Advances and Innovations. Ченнаї: CRC Press, 2022, 209 с.

Roman Kryvenko

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

These technologies are transforming various industries, from healthcare to finance, by enabling machines to learn from data and make predictions or decisions without being explicitly programmed.

Artificial Intelligence (AI) and Machine Learning (ML) are no longer just concepts of the future. They have become integral parts of our daily lives, influencing everything from the way we shop online to how we diagnose diseases. These technologies have the potential to revolutionise various sectors, including healthcare, finance, transportation, and more. They are not just buzzwords, but powerful tools that are transforming our society and the way we work. The purpose of this speech is to delve into the world of AI and ML, understand their applications, discuss their challenges, and explore their future trends.

Artificial Intelligence, or AI, is a branch of computer science that aims to create systems capable of performing tasks that would normally require human intelligence. These tasks include learning from experience, understanding natural language, recognising patterns, and making decisions. AI can be categorised into two types: Narrow AI, which is designed to perform a narrow task (such as facial recognition or internet searches), and General AI, which can perform any intellectual task that a human being can do.

Machine Learning, a subset of AI, is a method of data analysis that automates the building of analytical models. It uses algorithms that iteratively learn from data, allowing computers to find hidden insights without being explicitly programmed where to look. There are three types of machine learning: Supervised learning, where the model is trained on a labeled dataset; Unsupervised learning, where the model learns from an unlabelled dataset; and Reinforcement learning, where an agent learns to behave in an environment, by performing certain actions and observing the results.

AI and ML have a wide range of applications across various sectors. In healthcare, for instance, they are used for disease prediction and drug discovery. AI algorithms can analyse medical images to detect diseases at early stages. They can also analyse patient data to predict the risk of disease. In drug discovery, AI can help in the design of new drugs and in predicting their possible effects on the human body.

In finance, AI and ML help in fraud detection and algorithmic trading. AI algorithms can analyse transaction data to detect patterns that might indicate

fraudulent activity. In algorithmic trading, ML algorithms can analyse market data to make trading decisions.

In transportation, AI and ML are the backbone of autonomous vehicles. These vehicles use AI algorithms to perceive their environment, make decisions, and navigate without human intervention.

In the field of manufacturing, AI and ML are driving the smart factory revolution, leading to more sustainable and efficient production processes. AI algorithms can analyse production data to detect anomalies, predict failures, and optimise production processes.

These are just a few examples of how AI and ML are reshaping our world. In the next sections, we will delve deeper into some specific case studies, discuss the challenges of implementing AI and ML, and explore future trends in these technologies.

Let's delve deeper into some specific examples of how AI and ML are being applied in various sectors.

In the healthcare sector, AI and ML are transforming the field. They can elevate patient care through alternative patient-specific payment models, rapid analysis of imaging modalities, and remote patient monitoring. For instance, AI algorithms can analyse medical images to detect diseases at early stages. They can also analyse patient data to predict the risk of disease. This not only improves the accuracy of diagnoses but also allows for earlier interventions, which can significantly improve patient outcomes.

In the field of manufacturing, AI and ML are driving the smart factory revolution, leading to more sustainable and efficient production processes. AI algorithms can analyse production data to detect anomalies, predict failures, and optimise production processes. This not only improves the efficiency of production but also reduces waste, leading to more sustainable manufacturing practices. A study by Cinar et al. (2020) discusses the use of machine learning in predictive maintenance towards sustainable smart manufacturing.

In the energy sector, AI and ML are being used for optimising grid management, predicting energy demand, improving energy efficiency, and more. For instance, a study by Singh et al. (2022) discusses the digitalisation of the energy sector with an inclination towards sustainability. They highlight the significance of different digital technologies such as the Internet of Things (IoT), artificial intelligence (AI), edge computing, blockchain, and big data and their implementation in the different stages of energy such as generation, distribution, transmission, smart grid, and energy trading.

These case studies highlight the transformative potential of AI and ML across various sectors. However, as we will discuss in the next section, the implementation of these technologies also presents several challenges.

While AI and ML present numerous opportunities, they also come with their own set of challenges and ethical considerations.

One of the main challenges in implementing AI and ML is data privacy. As these technologies rely on large amounts of data, ensuring the privacy and security of this data is crucial. This is especially true in sectors like healthcare, where sensitive patient data is often used.

Another challenge is the interpretability of ML models. Many ML models, especially complex ones like deep learning models, are often seen as "black boxes" because their decision-making processes are not easily interpretable by humans. This lack of transparency can be a problem in many applications where understanding the reasoning behind a decision is important.

In addition to these technical challenges, there are also ethical considerations to take into account. A study by Poon and Sung (2021) discusses the ethical principles in machine learning and artificial intelligence, highlighting points of friction across ethical principles. The study emphasizes that the selection of datasets and algorithms to create AI prognostication models must involve extensive scrutiny to avoid biases and, consequently, injustice against individuals or groups of patients.

In the field of education, a study by Almarzouqi, Aburayya, and Salloum (2022) explores the opportunities and challenges of AI and ML in higher education institutions. The study addresses critical issues like common knowledge and stance of research bases regarding AI and ML in higher education institutions; best practices regarding usage of AI and ML in higher education institutions; students ' knowledge of AI and ML; and students 'attitudes regarding AI and ML opportunities and challenges in higher education institutions.

Finally, a study by Feng et al. (2022) provides an ethical critique of AI and ML in medicine. The study proposes that physicians should neither uncritically accept nor unreasonably resist developments in AI but must actively engage and contribute to the discourse, since AI will affect their roles and the nature of their work.

The future of AI and ML is promising, with several emerging trends that are set to further revolutionise various sectors.

One such trend is the rise of explainable AI (XAI). As AI systems become more complex, understanding their decision-making processes becomes more challenging. This has led to the development of XAI, which aims to make AI decision-making processes more transparent and understandable. A systematic review by Adadi and Berrada (2018) discusses the recent developments of XAI methods and evaluation metrics concerning different application domains and tasks. The study found that XAI methods are mostly developed for safety-critical domains worldwide, and visual explanations are more acceptable to end-users

Another emerging trend is the use of AI and ML in digital twinning. Digital twinning involves creating a digital replica of a physical entity, which opens up new opportunities for predictive maintenance, remote monitoring, and product optimization.

AI and ML are also making significant strides in the field of healthcare. A study by Esteva et al. (2019) discusses the use of AI and ML in the diagnosis of skin cancer. The study highlights that AI and ML are revolutionizing healthcare by providing doctors with better insights on how to plan treatment. The researchers developed a deep learning system that can achieve dermatologist-level classification of skin cancer. This is a clear demonstration of how these technologies can assist in medical diagnosis, potentially providing less invasive and quicker diagnoses for patients.

In the field of medicine, a study by Buch et al. (2018) takes a close look at current trends in medical AI and the future possibilities for general practice. The study emphasises that AI and ML are revolutionising healthcare by helping researchers analyse larger datasets and providing faster and more accurate diagnoses.

Finally, a study by Tuli et al. (2020) discusses next-generation technologies for smart healthcare, including the challenges, vision, model, trends, and future directions. The study highlights the role of AI and ML in improving healthcare services and proposes a holistic model that leverages state-of-the-art technologies in IoT, Fog computing, AI, ML, and Blockchain.

In conclusion, Artificial Intelligence and Machine Learning are powerful tools that have the potential to transform various industries and solve complex problems. They are already making significant strides in sectors such as healthcare, manufacturing, energy, and education, among others. The case studies we have discussed today highlight the transformative potential of these technologies and their ability to drive innovation and efficiency.

However, as we embrace these technologies, we must also address the challenges they pose. Data privacy, model interpretability, and ethical considerations are among the key challenges that need to be addressed. It is crucial that we develop robust frameworks and regulations to ensure that these technologies are used responsibly and ethically.

Looking ahead, there are several exciting trends in AI and ML. The rise of explainable AI, the use of AI and ML in digital twinning, and their increasing role in healthcare are just a few examples. These trends not only highlight the potential of AI and ML but also underscore the importance of continuous research and innovation in these fields.

As we move forward, it is important to remember that the goal of AI and ML is not to replace humans but to augment our capabilities. These technologies are tools that can help us make better decisions, solve complex problems, and improve the quality of life. It is up to us to harness their potential responsibly and ethically.

References:

1. Helm, J., Swiergosz, A., Haeberle, H., Karnuta, J., Schaffer, J., Krebs, V., Spitzer, A., & Ramkumar, P. (2020). Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions. Current Reviews in Musculoskeletal Medicine. ***Link***

2. Cioffi, R., Travaglioni, M., Piscitelli, G., Petrillo, A., & De Felice, F. (2020). Artificial Intelligence and Machine Learning Applications in Smart Production: Progress, Trends, and Directions. Sustainability. ***Link***

3. Al-Rubaie, M., & Chang, J. M. (2018). Privacy-Preserving Machine Learning: Threats and Solutions. IEEE Security & Privacy. ***Link***

4. Zhu, J., Liapis, A., Risi, S., Bidarra, R., & Youngblood, G. M. (2018). Explainable AI for Designers: A Human-Centered Perspective on Mixed-Initiative Co-Creation. IEEE Conference on Computational Intelligence and Games. ***Link***

5. Islam, M. R., Ahmed, M. U., Barua, S., & Begum, S. (2022). A Systematic Review of Explainable Artificial Intelligence in Terms of Different Application Domains and Tasks. Applied Sciences. ***Link***

6. Cinar, Z., Nuhu, A. A., Zeeshan, Q., Korhan, O., & Asmael, M. B. A. (2020). Machine Learning in Predictive Maintenance towards Sustainable Smart Manufacturing in Industry 4.0. Sustainability. ***Link***

7. Singh, R., Akram, S., Gehlot, A., Buddhi, D., Priyadarshi, N., & Twala, B. (2022). Energy System 4.0: Digitalization of the Energy Sector with Inclination towards Sustainability. Sensors. ***Link***

8. Almarzouqi, F., Aburayya, A., & Salloum, S. A. (2022). Artificial Intelligence in Higher Education: A Systematic Literature Review of AI Integration in Universities. IEEE Access. ***Link***

9. Nauta, M., Trienes, J., Pathak, S., Nguyen, E., Peters, M., Schmitt, Y., Schlötterer, J., Keulen, M. V., & Seifert, C. (2022). From Anecdotal Evidence to Quantitative Evaluation Methods: A Systematic Review on Evaluating Explainable AI. ACM Conference on Fairness, Accountability, and Transparency. ***Link***

10. Poon, A. I. F., & Sung, J. (2021). Opening the black box of AI-Medicine. Journal of Gastroenterology and Hepatology. ***Link***

11. Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118. ***Link***

12. Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2019). From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices. Science and Engineering Ethics. ***Link***

13. Umbrello, S., & van de Poel, I. (2021). Mapping value sensitive design onto AI for social good principles. AI Ethics. ***Link***

14. Morley, J., Elhalal, A., Garcia, F., Kinsey, L., Mökander, J., & Floridi, L. (2021). Ethics as a Service: A Pragmatic Operationalisation of AI Ethics. Minds and Machines. ***Link***

15. Morley, J., Machado, C., Burr, C., Cowls, J., Taddeo, M., & Floridi, L. (2019). The Debate on the Ethics of AI in Health Care: a Reconstruction and Critical Review. ***Link***

16. Buch, V. H., Ahmed, I., & Maruthappu, M. (2018). Artificial intelligence in medicine: current trends and future possibilities. British Journal of General Practice. ***Link***

Yurii Maliuha

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

MAIN CONCERNS DURING THE MIGRATION THE INFRASTRUCTURE OF THE EDUCATIONAL INSTITUTIONS TO CLOUD COMPUTING

In educational institutions, on-premises infrastructure has been a significant portion of their IT budgets. On-premises infrastructure refers to the actual hardware, servers, networking equipment, and software that are hosted and administered on the premises of the institution. Historically, educational institutions invested significantly in on-premises infrastructure to support a variety of IT requirements. To store and process data locally, they constructed data centers, server rooms, and networking infrastructure. This infrastructure made it possible to host learning management systems, student information systems, email servers, file storage, and other mission-critical applications required for daily operations. Parents and students expect a more innovative and progressive learning environment from educational institutions, which are battling declining revenues and rising operational costs. Even if they could locate qualified candidates, educational institutions typically lack the resources and manpower to employ full-time technology personnel. So here is where cloud computing might resolve most of the above-mentioned problems.

The transition from traditional computing to cloud computing signifies a fundamental change in how we store, process, and access data and applications. In the early days of computing, all resources were local and constrained by the capabilities of the hardware. As technology progressed, computers became more potent and interconnected, paving the way for networking and the internet. People began to recognize the potential of remote resource sharing and data access with the advent of the internet. This led to the development of the concept of distributed computing, in which multiple computers collaborate to solve complex problems. Nonetheless, this strategy required substantial infrastructure and maintenance. In the late 1990s, the advent of virtualization paved the way for cloud computing. Multiple virtual machines were able to operate on a single physical machine, maximizing resource utilization, thanks to virtualization. This innovation paved the way for the development of massive data centers that could provide computing resources as a service. Cloud computing as we know it today arose in the early 2000s with the introduction of Amazon Web Services (AWS), which offered scalable and flexible infrastructure for computing over the internet. This initiated a revolution in the IT industry, as companies could now access computational resources on demand and pay only for what they utilized.

The nature and characteristics of cloud computing techniques distinguish them from other forms of computation. The properties of cloud computing are divided into two categories: fundamental and essential properties [1]. Let’s review these essential characteristics:

1. Accessibility of broad network: Cloud services are made accessible using common procedures that enable users to access them via a variety of platforms and applications; for instance, when sufficient IP network access is available, cloud services and resources are accessible at any time and from any location via laptops, mobile phones, and personal computers.

2. On-demand Self-service: Fundamental to cloud computing, which provides users with computing services in the form of network storage and server time, is self-service on demand. Depending on a user's request, cloud computing services can be made available at any time. Self-service on demand is applicable even in the absence of human interaction.

3. Rapid elasticity: Cloud computing provides elastic and speedy computing capacity, which enables instantaneous scaling out and rapid scaling in. The ability to only deliver on demand to consumers is insufficient. The elasticity of cloud computing enables the provision of variable quantities of services at any given time. Increasing service capacities elastically during peak periods and decreasing them during off-peak periods can reduce costs for cloud subscribers and effectively meet their quality-of-service expectations.

4. Pooling of resources: Cloud resource providers pool a variety of physical and virtual computing resources to satisfy the diverse computing requirements of users. This aggregation of resources, including storage servers and devices, is utilized by a significant number of users. To optimize service quality, cloud resource providers select the most appropriate services from a pool of resources for each cloud user's task. Sharing cloud resources enables cost reductions by enabling multiple applications to be developed in the cloud as opposed to using dedicated computing resources.

5. Service measurement is an autonomous service that monitors and optimizes the use of a service and corresponds to the type of cloud computing resources to a certain degree of abstraction. In addition, it monitors, controls, and reports on service utilization, resulting in the purchase of actual resources.

The global spread of COVID-19 had a significant impact on educational institutions, compelling them to swiftly implement cloud computing to facilitate distance education. As a result of the pandemic-induced closure of schools, colleges, and universities, educators were required to find alternative means of delivering education and maintaining continuity of learning. In this context, cloud computing emerged as a crucial technology. It provided the infrastructure and instruments required to facilitate remote instruction and learning. Educational institutions quickly adopted cloud-based solutions for the creation of virtual classrooms, the hosting of video conferences, and the delivery of online educational content to students. Recent studies indicate that approximately 60% of

corporate data is stored in the cloud, that the quantity of corporate data stored in the cloud has at least doubled since 2015, and that more than 50% of businesses store their business documents in the public cloud [2]. When analyzing cloud usage in general, the previous findings are extremely significant, however, when focusing on cloud usage only in educational institutions, modest progress is observed. After analyzing the categories of sensitive data stored in the cloud, it was determined that student records make up only 8.9% of the total amount. So, let's investigate the main obstacles for universities to cloud adoption.

There are many obstacles to implementing cloud computing in education in a manner that would enable for its significant and rapid expansion. Lack of resources/expertise, security, and compliance are the greatest obstacles to the rapid adoption of technology by educational institutions. As more colleges and universities move more duties to the cloud, the demand for specialists has increased. Training IT and development personnel will be essential to addressing this challenge. Although data centers employ robust security measures, cloud security remains a concern. Concerns regarding cloud computing security include network security, data security, compliance, and governance, among others. One of the attached researches [3] concluded that legal issues, compliance, and loss of control over data are the top three main security concerns for organizations adapting to the cloud. Apart from this, the following can be highlighted:

- Reliance on the vendor's security paradigm
- Lack of physical control
- Service quality assurances
- Service dependability of a cloud service provider
- Data security encryption, redundancy, and deletion

There are additional obstacles to rapid adoption, including the cost of administering the cloud and the rate of file uploads. Costs in the cloud could skyrocket if certain customizations to satisfy educational requirements are implemented. Large files can take a long time to submit, causing frustration and impeding normal business operations. Other obstacles include governance and control, the complexity of constructing a private cloud, determining which services should be migrated to the cloud, and performance issues. That's why it is so important to develop a strategy of moving from on-premise to cloud computing.

Successful implementation of a cloud computing strategy in education requires time and effort. Multiple aspects of educational institutions will be impacted, complex decisions must be made, and numerous stakeholders must be involved. Due to the failure to establish a cloud strategy based on the delivery of IT services linked to their outcomes, the deployment of cloud computing has been unsuccessful for numerous organizations. Typically, a school has competent IT personnel and an understanding of IT requirements. However, there is a discrepancy between the strategic vision and understanding of available technologies and the budgets available to implement this vision. In addition, many institutions are unaware of how to initiate cloud initiatives. Before deploying cloud

services in a college or university, it is necessary to identify the areas where cloud services will contribute value. Then, an approach to scalable deployment must be planned. In general, the strategy for adopting cloud services can be divided into three phases [4].

In the elementary phase, colleges and universities should begin to learn about cloud technology and conduct a thorough analysis of their applications and required services. The primary concentration of cloud computing is on services, not technology. The offered services may include automated IT duties, IT services, and automated business processes. Students, faculty, and staff should receive cloud computing services according to their requirements. Consumers submit service requests via self-service and are billed based on their usage. The most effective deployments begin with users thoroughly comprehending the desired outcomes, followed by the identification of the private and/or public cloud services.

In Phase II, schools must document and assess the internal processes that will be impacted by the selected cloud services. The school system's traditional curriculum delivery and administration network must be considered. In addition, other services, such as delivering data outside of the physical network in a secure manner so that students can access assignment files, must be evaluated. The consumers should examine the internal IT processes involved in offering the services during this analysis. This may indicate the need to compress, reconfigure, realign, refine, or eradicate inefficient processes and automate repetitive manual processes. It is also necessary to address the varieties of security that will be applied to cloud deployment. Finally, schools must turn outside of their own IT departments for assistance and partner with solution providers who can provide both initial and ongoing support. As schools think about broader effects such as data protection and security, the importance of external providers will increase.

In the third phase, users should transfer their applications and duties to the corresponding cloud services. Each workload's applicability to cloud computing and its location environment should be evaluated. Next, a comprehensive evaluation of the overall architecture of the application's duties is required. Users must determine the security profile for each assignment, such as whether it can reside offsite and whether it must be encrypted. After analyzing the burden, the user must determine the optimal cloud computing deployment model for the organization's applications and workloads.

To sum up, cloud computing has grown into a mainstream technology that is widely acknowledged to provide substantial benefits to educational institutions. Cloud solutions provide high levels of capability and dependability while reducing administrative and operational expenses. Information accessible to students, instructors, and parents using any device is available from any location. In addition, their pricing is frequently substantially lower than that of comparable on-premises solutions. Due to learning management systems and student information systems, many institutions of higher education utilize cloud-based technology. The

accelerated adoption of this technology in higher education is facilitated by advantages such as the availability of low-cost and free technology, personalized learning, 24/7 accessibility, openness, and enhanced functional capabilities. Faculty and students now have access to an entire universe of knowledge that can be accessed at any time, from any location, on any device. As with all new technologies, cloud computing confronts obstacles that must be comprehended, mitigated, and surmounted for its benefits to be fully realized in higher education. Security, compliance issues, lack of reliability, and lack of interoperability are a few of the implementation obstacles that must be surmounted. Transitioning to cloud-based services represents a paradigm change for any organization. Managing this transformation requires a partner who is familiar with higher education and the benefits the cloud can provide to constituents and the institution's mission. By partnering with a cloud service provider for the provision of central administrative functions, higher education institutions can reorganize their personnel to concentrate on unique, high-value tasks and provide key stakeholders with a higher level of service than would otherwise be possible.

***References*:**

1. Audin H. (2021) A Study of Cloud Computing Adoption in Universities as a Guideline to Cloud Migration. SAGE Journal, https://journals.sagepub.com/doi/full/10.1177/21582440211030280

2. Duarte F. (2023) Percent of Corporate Data Stored in the Cloud, Exploding Topics, https://explodingtopics.com/blog/corporate-cloud-data

3. Gonzalez, N., Miers, C., Redígolo, F., Carvalho, T., Simplicio, M., Näslundy, M., and Pourzandiy, M., (2012). An quantitative analysis of current security concerns and solutions for cloud computing. Escola Politécnica at the University of São Paulo (EPUSP)

4. Smith, D. (2016). Cloud Computing Deployments Should Begin With Service Definition. Gartner Report, https://www.oic-cert.org/en/journal/pdf/4/1/1.pdf

Mykhailo Morozov

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

TRANSFORMING OPERATIONAL MANAGEMENT: HARNESSING THE POWER OF ARTIFICIAL INTELLIGENCE

Artificial intelligence has begun to manifest itself in all areas of the changing business world. With the introduction of new technologies in the digital age, business structures have to adapt to new projects and increase the productivity of business processes.

Artificial intelligence (AI) is a broad term that can refer to various technologies. John McCarthy first put forth this idea in 1950, during the famed Turing Test. Since the early 2000s, artificial intelligence (AI) has advanced quickly, attracting new attention, and has been given another look in both research and practical applications in recent years. AI combines science and engineering to create intelligent devices.

One of the most significant impacts of AI on business operations is its ability to automate routine tasks. Many companies have implemented AI-powered chatbots and virtual assistants to handle customer queries and automate repetitive tasks. This has not only freed up human resources but has also improved customer satisfaction and response times.

There are several key areas where the use of artificial intelligence in operational management has an impact on organizational success:

- Data Analysis and Decision-Making: Traditional decision-making processes heavily relied on human intuition and the analysis of historical data. However, AI-powered systems can analyze vast amounts of data in real-time, identify patterns, and extract valuable insights that aid in informed decision-making.
- Process Automation and Optimization: Operational management involves numerous repetitive and time-consuming tasks that can be automated with AI. Robotic process automation is a prime example of how AI can streamline operations. This not only eliminates human error but also frees up valuable human resources to focus on more strategic and creative activities, ultimately increasing overall productivity and efficiency.
- Customer Relationship Management: AI-powered chatbots and virtual assistants can enhance customer service operations by providing instant responses to customer queries, offering personalized recommendations, and resolving issues promptly. They can handle a wide range of customer interactions, from basic queries to complex support issues, ultimately improving customer satisfaction, engagement, and loyalty.

- Edge Over Competitors: Keeping an eye on market trends and patterns is the secret to remaining competitive in the supply chain industry. With all the gathered information, you can more accurately assess the state of the market and anticipate future requirements for steady growth. You can modify your product portfolio and capital expenditure by utilizing AI's sensory capabilities. Currently, this is supply chain management's preferred use of Artificial Intelligence.
- Effective Risk Management: Operational management entails identifying and mitigating risks that may impact business operations.

AI plays a crucial role in risk management by analyzing vast amounts of data to detect patterns and anomalies that may indicate potential risks or fraudulent activities. By identifying these red flags in real-time, organizations can take proactive measures to prevent risks, safeguard assets, and ensure compliance with regulations.

- Market Research and Competitive Analysis: AI can automate market research processes, collecting and analyzing data from various sources to provide valuable insights into market trends, customer preferences, and competitor strategies. Businesses can leverage this information to make data-driven decisions, identify new opportunities, and stay ahead of the competition.
- Continuous Learning and Improvement: AI systems can continuously learn and improve based on data feedback. By leveraging machine learning algorithms, businesses can enhance their AI models and systems over time, resulting in more accurate predictions, better performance, and increased operational efficiency.

The use of AI is how companies will operate in the future, revolutionizing how operations are managed. AI-powered systems are evidence that technology is revolutionizing operations management and advancing companies' productivity and efficiency.

The contact between the company and its customers is crucial to corporate operations. AI allows you to integrate the workflow by providing instructions for staff. In general, robots and intelligent systems improve logical processes and facilitate quick responses to certain problems.

AI is transforming business operations in many ways, including automating routine tasks, improving decision-making, and reducing costs. Although implementing AI solutions may present challenges, businesses that invest in AI technology can gain a competitive advantage and stay ahead of the curve. By leveraging AI technologies, organizations can optimize processes, improve decision-making, enhance customer experiences, and drive operational efficiency, ultimately leading to increased competitiveness and success in today's rapidly evolving business landscape.

References:

1. Davenport, T. H. (2018). The AI Advantage: How to put the artificial intelligence revolution to work. MIT Press.

2. Masrour T. (2021). Artificial Intelligence and Industrial Applications: Smart Operation Management (Advances in Intelligent Systems and Computing Book 1193)

3. Lacity, M., & Willcocks, L. (2017). Artificial Intelligence in Business: The State of the Art and Future Prospects. MIS Quarterly Executive, 16(2).

4. Davenport, T. H., & Ronanki, R. (2018). Artificial Intelligence for the Real World. Harvard Business Review.

Pavlo Semehen

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

CREATING A PRODUCT FULLY REMOTELY FROM SCRATCH

When creating a product fully remotely from scratch, there're several important keys that contribute to its success such as building a fully-remote team, organization of development processes, choosing a stack of technologies and tools, expertise in a selected domain, and strategies for raising capital for making the product default alive.

Building a fully-remote team requires careful planning and execution to ensure effective collaboration and productivity. Defining roles and responsibilities is the most important part. The roles and responsibilities you need for your product should be clearly described. The company has to have the key positions such as developers, designers, marketers, and project managers, and outline the skills and experience required for each role. Recruitment and onboarding are crucial. There are many possible ways for advertising your job openings on remote job boards and platforms such as Linkedin, Djinni, Indeed, etc. The recruitment process has to be well organized by screening candidates thoroughly to assess their skills, experience, and remote work capabilities. Conducting virtual interviews to get a sense of their communication skills and assess cultural fit. Once hired, the company has to provide comprehensive onboarding materials and conduct virtual onboarding sessions to familiarize new hires with the company culture, values, and processes. Without good communication and collaboration tools, it is impossible to reach the goals. Select and implement the right tools to facilitate remote collaboration. Popular options include communication tools like Slack or Microsoft Teams for real-time messaging and video conferencing, project management tools like Jira, Clickup, or Shortcut for task tracking, and file-sharing platforms like Google Drive or Dropbox for seamless document sharing and collaboration. Clearly define expectations for remote work hours, communication channels, and protocols for meetings, updates, and feedback. Encourage regular check-ins and provide a platform for team members to ask questions and seek clarifications. Each company has its culture and the employee should fit it to be a perfect match. Create a remote-friendly culture that promotes collaboration, trust, and accountability. Encourage team bonding through virtual team-building activities, promote transparency in decision-making processes, and provide opportunities for informal interactions. Foster an environment where remote team members feel valued and supported.

Organizing development processes for a fully-remote team requires careful planning and effective collaboration. The team can be ineffective if the wrong development methodology was chosen. Scrum methodology is used on most products/startups, but in most cases, it's a modified Scrum methodology. Adopt an agile development approach that allows for iterative development and frequent feedback. Break down the project into smaller sprints and hold regular stand-up meetings to track progress, discuss challenges, and address any roadblocks. Use project management tools to visualize workflows, set priorities, and allocate resources effectively. A great way for moving fast is to split the large team into several small teams that will be focused on a specific domain or a specific functionality within a product. Without project development tools it is not possible to move on. Utilize project management tools like Jira, or Basecamp to plan, assign, and track tasks. These tools enable efficient task management, help prioritize work, and provide transparency into the progress of individual team members and the overall project. The product will not be a default alive without great documentation, test coverage, and knowledge sharing. Emphasize the importance of documentation and knowledge sharing to ensure team members have access to necessary information. Use collaborative platforms like Confluence or Notion to create a centralized knowledge base for project documentation, processes, and best practices. Encourage team members to document their work, share insights, and contribute to collective knowledge. Use tools like Miro for creating a roadmap. UML diagrams are also helpful to have a better vision of the product. When it goes to development code versioning and collaboration is a key points. Use a version control system like Git and host your code repository on platforms such as GitHub or GitLab. Encourage code reviews and collaboration through pull requests to maintain code quality and facilitate knowledge sharing among team members. Establish coding standards and guidelines to ensure consistency and maintainability of the codebase. The company has to organize regular sync-ups and feedback loops by scheduling regular video or voice meetings to discuss progress. These meetings provide an opportunity to align the team's efforts, clarify any ambiguities, and foster collaboration. Encourage open communication and create a safe environment for team members to voice their concerns, share ideas, and provide constructive feedback.

Currently, there's a wide range of technologies that you can choose for the development of your product. The stack of technologies depends on your requirements, needs, and goals. Also, it depends on your budget. Selecting the right stack of technologies and tools is crucial for building a successful product in 2023. While technology trends evolve rapidly, here are some popular choices worth considering. For front-end development, the most popular is React or Angular. These JavaScript frameworks enable the building of interactive user interfaces with reusable components and a rich ecosystem of libraries and tools. Here also comes TypeScript which brings static typing and improved developer productivity to JavaScript projects, reducing errors and enabling better code maintainability.

Next.js or Gatsby are the frameworks that facilitate server-side rendering and performance optimization, enabling faster page loads and improved SEO. Tailwind CSS offers efficient and customizable styling approaches, allowing for rapid UI development. If it goes around back-end development then consider Node.js, Python, Ruby, or Go. Node.js is a popular choice for building scalable server-side applications in JavaScript, while Go provides a high-performance and efficient option for backend development. If you want to follow schema-driven development then GraphQL is a perfect match. It simplifies API development by providing a flexible query language and efficient data fetching capabilities. Deployment should be well-configured and stable. Docker enables containerization, making it easier to package and deploy applications consistently across different environments. Kubernetes or AWS Elastic Beanstalk facilitate managing and scaling containerized applications in a cloud environment, providing flexibility and scalability. Among mostly used databases and data storage are PostgreSQL, Redis, and MongoDB. PostgreSQL offers a robust and feature-rich relational database solution, while MongoDB provides a flexible and scalable NoSQL option. Redis is an in-memory data store that can be used for caching, session management, and improving application performance. Amazon S3 or Google Cloud Storage services offer scalable and reliable options for storing and managing files. DevOps and Deployment make our products accessible for others via the internet. CI/CD tools make the lives of DevOps engineers easier. Among them are Jenkins, CircleCI, or GitLab CI/CD. They enable automated testing, continuous integration, and deployment pipelines to streamline the development process. Tools like Terraform or AWS CloudFormation allow for managing infrastructure declaratively, making it easier to provision and manage resources. Monitoring and Logging are tools that provide more context of what is happening with our product by analyzing user's behavior. Consider tools like Prometheus, Grafana, or ELK Stack (Elasticsearch, Logstash, Kibana) for monitoring application performance, collecting logs, and gaining insights into system behavior.

During the development phase, the focus is on implementing the product features, ensuring quality, and delivering a functional and user-friendly solution. Prioritize the features based on their importance and value to the users. Create a roadmap or backlog to track the planned features and iterate based on feedback. Break down the development process into iterative sprints. Each sprint should have a clear set of objectives and a defined timeline. Regularly review progress, address challenges, and adapt the plan as needed. Foster collaboration among team members through effective communication, code reviews, and knowledge sharing. Encourage pair programming or peer programming to enhance code quality and knowledge transfer. Implement a robust testing strategy that includes unit tests, integration tests, and end-to-end tests. Leverage testing frameworks and tools to automate the testing process and ensure the stability and reliability of the product. Implement CI/CD pipelines to automate the build, testing, and deployment

processes. This helps streamline development workflows, reduces manual errors, and ensures faster delivery of new features and bug fixes. Gather user feedback through user testing, surveys, or analytics. Incorporate the feedback into the development process, iterate on features, and continually improve the user experience.

Every company needs a budget for creating a great product. So here the raising capital topic comes in. Raising capital is an essential step for many startups to fuel growth and bring their product to market. Create a solid business plan. Develop a comprehensive business plan that outlines your product, target market, revenue model, and growth strategy. This plan will be crucial for attracting potential investors. Consider using personal savings, credit lines, or loans to bootstrap your startup. This approach gives you more control but may limit the available resources. As an option are angel investors. Seek out angel investors who are interested in supporting early-stage startups. Angel investors often provide capital, industry expertise, and valuable connections. Crowdfunding is a great option to start with. Platforms like Kickstarter or Indiegogo allow you to raise funds directly from the public. This approach can help validate your product idea and build a community of early adopters. Apply for grants programs and accelerators. Research grants and accelerator programs that are relevant to your product or industry. These programs often provide funding, mentorship, and resources to support startup growth. And don't forget about pitching and networking. Attend startup events, pitch competitions, and networking events to connect with potential investors. Craft a compelling pitch that highlights your product, market opportunity, and growth potential.

Creating a product fully remotely requires careful planning, effective communication, and utilizing the right tools and technologies. Building a remote team from scratch involves defining roles, recruiting, and fostering a remote-friendly culture. Organizing development processes requires agile methodologies, project management tools, and effective communication channels. Choosing a technology stack involves considering popular frameworks and tools for front-end and back-end development, database management, and deployment. During the development phase, prioritize features, emphasize collaboration, automate testing, and iterate based on user feedback. Raising capital can be achieved through self-funding, angel investors, venture capital, crowdfunding, grants, accelerators, and networking. Following these steps effectively it's possible to create a successful product remotely while fostering a thriving and productive team.

Artur Stepashkin

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

THE USE OF ARTIFICIAL INTELLIGENCE IN PRE-PRODUCTION

This study investigates a relatively new area — the use of AI in pre-production. Filmmakers can utilize AI in several facets of the filmmaking process before the actual movie production begins. Thus, the main focus of this paper will be addressed to the usage of AI in the development and pre-production processes that are considered a critical phase of filmmaking. Even though the stages of development and pre-production may vary due to the type of project, in big-production filmmaking and television commercial, they remain relatively consistent and include scriptwriting and script breakdown, budgeting and marketing, scheduling, crew assembling, planning calls for creation, talent scouting, and rehearsal [4].

For the moment being, filmmakers can leverage AI in the development and pre-production almost in every mentioned stage. This is certainly true in the case of using computational power in the scriptwriting process, which is gaining acceptance and popularity. Machine learning and artificial intelligence algorithms can be utilized to generate new scripts or author synopses and character names for previously released films. Moreover, AI can develop new scripts by processing massive amounts of data input into a machine-learning algorithm [6]. For instance, in 2016, AI wrote the script for a 10-minute short film —Sunspring. The AI, called Benjamin, generated the script using a recurrenxt neural network. Significantly, the film entered the top ten at the Sci-Fi London film festival [5]. In addition, AI can analyze individual scripts that will be turned into films and generate its own questions and doubts [6].

The rapid advances in natural language processing (NLP) and large language models have allowed filmmakers to expand the usage of AI in the scriptwriting process. The most recent and progressive model is Chat GPT, which is causing certain upheaval among scriptwriters. This is evident in the case of the contract discussion between the Writers Guild of America (WGA) and The Alliance of Motion Picture and Television Producers (AMPTP). They failed to reach an agreement by the final date, having contrasting opinions on the stipulation of studios' potential use of AI [9].

Regarding budgeting and marketing, there is a trove of AI services that can help large-scale production companies to estimate the perceived gains from releasing the movie. For example, Cinelytic is an AI-based startup that offers quicker and smarter solutions to independent film companies and studios through the value chain of the film. Also, Belgian company ScriptBook offers an AI-based

script analysis and financial forecasting tool. ScriptBook has developed an AI algorithm to make the process of evaluating the scenes and suggesting whether or not to promote them more automated and standardized. Another prominent example is The RealDemand AI platform by Vault analyzes numerous critical elements of the story, outline, script casting, and trailer to maximize return on investment 18 months before the release date [5]. Additionally, 20th Century Fox has developed the Merlin neural network and similar tools to assist studios in various film management and promotional tasks [2].

Currently, these services are expensive, so only prominent companies can afford them. Besides, those platforms are unable to predict incidental expenses. They can only reduce the time spent on low-value tasks and provide dollar-figure parameters regarding packaging, marketing, distribution decision, and release dates [8].

Concerning scheduling and planning, AI can help optimize pre-production processes. It can help schedule the shooting and other pre-production activities. For instance, AI serves to devise an efficient film shoot by analyzing the available for several actors dates and developing schedules based on that information. Furthermore, it can also identify the locations mentioned there and recommend real-world sites for shooting, which is very time-saving [6].

A Filmustage tool is a notable example of using AI at this stage. The platform is constantly developing and announcing more rounds of fundraising to develop even further. The platform is designed to streamline the pre-production process using a number of features. "Scheduling" and "Analysis" are the newest tools that have lately appeared on the platform [3].

Yamdu is another scheduling and planning service that optimizes the visual content creation workflow. This production management software aims to improve time management and eliminate redundant tasks [10].

The technology can be used to optimize the casting process. Therefore, AI can analyze actors' historical performances and the geographical areas where their film was successful, enabling producers to give shape to marketing campaigns and promotional material [6]. For instance, Merlin and Cinelytic tools offer casting suggestions to producers and directors to ensure the best financial returns on future films. Besides, aggregated tools like LargoAI enable stakeholders to navigate pre-production and identify the components of the movie to suggest changes [7].

In addition, AI can be utilized by actors. An actor with experience can hire an AI company to analyze the script and get insights into their suitability for this specific role. In addition, actors can record themselves, upload videos to AI SaaS platforms, and receive feedback [1].

So, using AI in pre-production has advantages, such as enhancing creativity, improving accuracy, and reducing expenses. In contrast, AI lacks creativity, offers limited perspective, makes us too dependent on technology, and can be concerning

from the ethical side. As a result, over-reliance on AI can pose possible threats to human creativity.

To conclude, the film industry can benefit greatly from AI. However, there are potential downsides and threats that must be carefully considered. It is important for filmmakers to maintain their own creative vision and intuition while using AI as a tool.

References:

1. *Davies A. How Actors Will Benefit from Using AI: Artificial Intelligence in Filmindustry. URL:* ***sofy***.
2. *Donelly J. How Artificial Intelligence Helps (and Hurts) Filmmaking. URL:* ***massive.io***.
3. *Forristal L. Filmustage leverages AI to break down film scripts, create shooting schedules and more. URL:* ***techcrunch***.
4. *Guide to Preproduction in Film: 7 Elements of Preproduction. URL: masterclass.*
5. *How AI is used in filmmaking. URL:* ***analyticsindiamag***.
6. *How can AI help the film industry. URL:* ***aicorespot.***
7. *Our AI predicted the Success of Venom with a High Degree of Accuracy. URL:* ***largofilms***.
8. *Siegel T. Warner Bros. Signs Deal for AI-Driven Film Management System (Exclusive):* ***hollywoodreporter***.
9. *Why Striking Hollywood Writers Fear an AI Future. URL:* ***rollingstone***.
10. *Yamdu. Customer Success Stories. URL:* ***yamdu***.

Kyrylo Zinovyev

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

ETHICAL AND SOCIETAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) refers to the ability of machines to perform tasks that would typically require human intelligence, such as recognizing speech, making decisions, and learning from experience. The rapid growth of AI in recent years has been driven by advancements in machine learning, neural networks, and other related technologies. Major players in the AI industry include companies like Google, Amazon, Facebook, and Microsoft, as well as startups and research institutions around the world. Recent breakthrough by OpenAI and ChatGPT took it to yet another level forcing competitors to put more efforts into AI space and now we have Bing AI Chat by Microsoft, Google Bard AI, Chatsonic.

AI has a wide range of applications across different industries and domains, including healthcare, finance, transportation, entertainment, and more. Some of the most sensitive areas where AI is used include:

- Healthcare: AI is being used to analyze medical data, diagnose diseases, and develop new treatments. This has the potential to revolutionize healthcare and improve patient outcomes, but it also raises concerns around privacy, bias, and the ethical implications of using AI to make life-altering decisions.
- Criminal justice: AI is being used to predict crime and assess the likelihood of recidivism, with the goal of improving public safety. However, this raises concerns around the potential for bias and discrimination, as well as the ethical implications of using AI to make decisions about people's lives.
- Finance: AI is being used to analyze financial data, identify patterns, and make investment decisions. This has the potential to improve financial outcomes and reduce risk, but it also raises concerns around accountability and transparency, as well as the potential for unintended consequences.
- Social media: AI is being used to personalize content and recommendations on social media platforms, with the goal of improving user engagement. However, this raises concerns around privacy, filter bubbles, and the potential for AI to manipulate user behavior.

The rapid growth of AI has raised a number of ethical and societal implications that need to be addressed. Some of the key implications are:

- Bias and discrimination: AI systems can perpetuate and even amplify biases present in the data used to train them. This can lead to discriminatory outcomes, particularly against marginalized communities. For example, facial

recognition technology has been shown to have higher error rates for people with darker skin tones, which could have serious consequences in areas such as law enforcement and border security.

- Privacy and security: AI systems can collect, process, and store vast amounts of personal data, raising concerns around privacy and security. Additionally, AI can be used to create deepfakes and other forms of misinformation, which can have serious consequences for individuals and society.
- Job displacement: As AI becomes more sophisticated, it has the potential to replace human workers in a wide range of industries, leading to job displacement and economic disruption. This could have significant social and political implications, particularly if large numbers of people are left unemployed or underemployed.
- Accountability and transparency: The complexity of AI systems makes it difficult to understand how they arrive at their decisions, raising questions about accountability and transparency. This is particularly important in areas such as healthcare and criminal justice, where AI can have life-altering consequences.
- Autonomous weapons: The development of autonomous weapons powered by AI raises concerns around the potential for these systems to be used for unethical purposes or to cause unintended harm. This has led to calls for a ban on the development and use of autonomous weapons, as well as efforts to regulate the use of AI in military applications.
- Social inequality: AI can exacerbate existing social inequalities, such as income inequality and access to healthcare, education, and other services, if not developed and deployed in a way that is fair and equitable.

The quality of the training set used to develop AI models is critical to their effectiveness and accuracy. The training set is the data used to train an AI model, and it needs to be representative of the real-world data that the model will be applied to.

If the training set is biased or incomplete, the AI model may not learn to make accurate predictions or decisions. Another issue is that AI models can learn to replicate the biases and errors present in the historical data used to train them. This is known as "algorithmic bias." If the historical data used to train an AI model includes biases or incorrect human decisions, then the model may learn to replicate those biases and errors.

For example, if an AI model is trained on data that includes historical decisions made by humans in the criminal justice system, and those decisions were based on biases or incorrect assumptions, then the AI model may learn to make similar biased or incorrect decisions.

To address these issues, it is essential to ensure that the training set is representative of the real-world data and that biases and errors are identified and addressed. This may involve using diverse data sources and incorporating ethical considerations into the design of the AI model.

Furthermore, it is important to continuously monitor the AI model's performance to identify any biases or errors that may emerge over time. This can be done through ongoing testing and validation of the AI model's performance and by engaging in a continuous feedback loop to address any issues that arise.

Overall, the quality of the training set used to develop an AI model is critical to its effectiveness and accuracy, and the historical data used to train an AI model can have a significant impact on its ability to make accurate and unbiased predictions or decisions.

AI development companies are increasingly recognizing the importance of preventing bias in their AI systems, and many are taking steps to address this issue. Here are some examples of what AI development companies are doing to prevent bias:

- Diverse data sources: One of the most important ways to prevent bias is to ensure that the training data used to develop the AI system is diverse and representative of the real world. This may involve incorporating data from a variety of sources and ensuring that the data is not skewed towards any particular demographic.
- Regular testing and validation: AI development companies are increasingly implementing regular testing and validation of their AI systems to identify any biases that may have emerged over time. This can involve testing the system on a diverse set of data and validating the results to ensure that they are unbiased.
- Ethical considerations: Many AI development companies are incorporating ethical considerations into their AI system design, including the use of ethical frameworks and guidelines to guide the development and deployment of their systems.
- Transparency and explainability: AI development companies are also increasingly focused on making their systems transparent and explainable, which can help to identify and address biases. This may involve providing explanations for the decisions made by the system or providing access to the data and algorithms used to develop the system.
- Ongoing monitoring and evaluation: Finally, AI development companies are recognizing that preventing bias is an ongoing process that requires ongoing monitoring and evaluation of the system's performance. This may involve engaging in a continuous feedback loop with users to identify any issues that arise and addressing them in a timely manner.

Regulatory efforts to address the ethical and societal implications of AI have been varied and have taken place at different levels, including international, national, and industry-specific regulations.

At the international level, the United Nations has established a number of initiatives aimed at regulating the development and deployment of AI. The most notable of these is the UN's Centre for Artificial Intelligence and Robotics, which

was established in 2017 with the aim of promoting the responsible use of AI and ensuring that it benefits society as a whole.

At the national level, many countries have established regulatory frameworks for AI. For example, the European Union introduced the General Data Protection Regulation (GDPR) in 2018, which regulates the collection and use of personal data by businesses and organizations. The GDPR includes provisions specifically related to AI, such as the right to an explanation of how decisions made by AI systems are arrived at.

In the United States, the Federal Trade Commission has established guidelines for the use of AI in advertising and marketing, with a focus on ensuring that AI is not used to discriminate against individuals based on their race, gender, or other protected characteristics.

Industry-specific regulations have also been developed in areas such as healthcare, finance, and transportation. For example, the US Food and Drug Administration has established guidelines for the use of AI in medical devices, while the Financial Stability Board has developed principles for the use of AI in financial services.

Despite these regulatory efforts, there are a number of challenges that remain in regulating the development and use of AI. One of the biggest challenges is the pace of technological change, which can outstrip the ability of regulators to keep up. Additionally, the global nature of the AI industry can make it difficult to establish consistent regulatory frameworks across different countries and regions.

Another challenge is the complexity of AI systems, which can make it difficult to understand how decisions are arrived at and to ensure accountability for those decisions. This is particularly important in areas such as healthcare and criminal justice, where the use of AI can have life-altering consequences.

The ethical and societal implications of artificial intelligence are significant and require careful consideration by policymakers, industry leaders, and the public at large. While regulatory efforts have been made at the international, national, and industry-specific levels, there remain significant challenges in regulating the development and use of AI. As AI continues to advance, it is essential that regulatory frameworks keep pace and ensure that AI is developed and deployed in a way that benefits society as a whole.

МЕНЕДЖМЕНТ ТА МАРКЕТИНГ

Абраменко Р. А.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ПРАВОВАЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

В современном информационном обществе, где технологический прогресс и цифровизация играют важную роль, вопросы конфиденциальности и защиты персональных данных становятся все более актуальными. Работники входят в контакт с различными организациями, предоставляя свои личные данные, которые могут быть использованы и обрабатываться для различных целей. В этом контексте возникает необходимость в правовой защите персональных данных работников [1].

Право на конфиденциальность и защиту персональных данных является одним из фундаментальных прав человека. Международные и национальные нормативные акты устанавливают правовые рамки, регулирующие сбор, хранение, использование и передачу персональных данных работников. Однако, в связи с постоянно меняющейся технологической средой, законодательство должно быть постоянно обновляемым и адаптированным к новым вызовам.

В рамках трудовых отношений возникают особые вопросы, касающиеся защиты персональных данных работников. Работодатели имеют доступ к различным данным, связанным с трудовыми процессами, включая информацию о здоровье, финансовом положении и привычках работников. Поэтому важно обеспечить соблюдение принципа минимизации данных, когда работодатель собирает только необходимую информацию и использует ее только в рамках трудовых целей.

В связи с развитием информационных технологий, особенно искусственного интеллекта и аналитических систем, возникают новые риски для конфиденциальности и защиты персональных данных работников. Автоматизация процессов, массовый сбор и анализ данных могут создавать потенциальные возможности для злоупотребления информацией и нарушения прав работников. Поэтому важно разрабатывать и внедрять механизмы защиты персональных данных, которые соответствуют современным технологическим требованиям [2].

Одним из основных аспектов правовой защиты персональных данных работников является необходимость согласованного законодательства. Законы и положения должны устанавливать ясные правила для сбора, хранения и обработки персональных данных, а также предусматривать меры

ответственности за их нарушение. Кроме того, необходимо обеспечить прозрачность и информированность работников о том, какие данные собираются и как они будут использоваться.

Важным аспектом защиты персональных данных является применение принципа целесообразности и пропорциональности. Сбор и использование персональных данных должны быть обоснованными и соответствовать конкретным целям, а также не превышать необходимого объема информации. Работодатели должны стремиться минимизировать собранные данные и обеспечивать их безопасность с помощью соответствующих технических и организационных мер.

Важно также учитывать международные стандарты и нормы, такие как Общая Директива ЕС о защите данных (GDPR), которые предоставляют дополнительные гарантии и права работникам в отношении их персональных данных. Эти стандарты устанавливают требования к сбору согласия работников, обеспечению безопасности данных и праву на доступ и исправление информации [3].

Органы по защите данных должны играть важную роль в обеспечении правовой защиты персональных данных работников. Они должны иметь достаточные полномочия для расследования нарушений и назначения санкций в случае несоблюдения законодательства о персональных данных. Также важно, чтобы работники имели доступ к механизмам обжалования и защиты своих прав в случае нарушения конфиденциальности и неправомерного использования их данных.

В заключение, правовая защита персональных данных работников является неотъемлемым компонентом современной рабочей среды. В условиях быстрого развития технологий и цифровизации, защита персональных данных становится все более актуальной и значимой. Работники имеют право на конфиденциальность и защиту своих данных, а работодатели обязаны соблюдать соответствующие нормы и принципы. Оптимальная защита персональных данных требует гармоничного сочетания законодательства, технических мер безопасности и осведомленности всех сторон. Необходимо создать устойчивую правовую основу, которая обеспечит справедливость, прозрачность и надежность в отношениях между работодателями и работниками. Только тогда можно достичь баланса между необходимостью использования данных в рабочих целях и защитой частной жизни и прав работников на конфиденциальность. Правовая защита персональных данных работников является фундаментальным принципом современных трудовых отношений и социальной справедливости.

Список использованных источников:

1. Hendrickx, F. 2022. Protection of workers' personal data: General principles, ILO Working Pa-per 62 (Geneva, ILO). URL:https://www.ilo.org/legacy/english/intserv/working-pape.

2. Payton. Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family / Payton, M. Theresa, C. Theodore. – Lanham, MD, 2014. – 276 c. – (Rowman & Littlefield Publishers).

3. IT Governance Privacy Team. EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide / IT Governance Privacy Team. – United Kingdom, 2019. – 406 c.

Андрійчук Я. Р.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ОРГАНІЗАЦІЯ ОПЕРАЦІЙНОЇ ДІЯЛЬНОСТІ БІЗНЕС-ОРГАНІЗАЦІЇ

Організація операційної діяльності є фундаментальним елементом успішного функціонування будь-якої бізнес-організації. Вона включає в себе комплексні процеси та стратегії, які допомагають управляти виробництвом, постачанням, якістю та обслуговуванням клієнтів. Ефективна організація операційної діяльності дозволяє забезпечити оптимальне використання ресурсів, досягти конкурентних переваг і задовольнити потреби ринку**.**

Виділяють три види діяльності компанії: операційна, інвестиційна та фінансова. Такий поділ необхідний більш точного визначення обороту капіталу бізнес-організації з метою оцінки ефективності її діяльності [7].

Найзначніша діяльність у компанії - операційна. Вона включає звернення всіх видів коштів, що витрачаються на щоденні завдання вашого бізнесу. Сюди відносяться всі разові та постійні витрати компанії. В інвестиційну діяльність входять такі операції з грошима, як купівлі, продажу, обслуговування обладнання та майна підприємства. Наприклад, витрати на уніформу для персоналу, ремонт літньої веранди кафе і т. д. Відрізнити її можна за ознакою довгостроковості, тобто інвестиції в цей час. Фінансова діяльність - це отримання чи видача кредитів. Наприклад, видача кредиту іншій компанії будуть фінансовою діяльністю, тому що ніяк не торкається операційних процесів компанії, яка видає кредит [2].

Розглянемо операційну діяльність бізнес-організації. Для того, щоб зберегти позиції на ринку в умовах жорсткої конкуренції, підприємство стежить за всіма змінами, що відбуваються на ринку, та розробляє різні способи пристосування до негативних впливів, щоб вплинути на конкурентоспроможність. Операційна діяльність підприємства націлена на отримання прибутку та/або виконання інших завдань підприємства, це може бути надання відповідного виду послуг, сільськогосподарська діяльність, виробництво промислових благ, здавання майна в оренду, продаж та транспортування товарів та інше. Інакше висловлюючись, це те, заради чого безпосередньо існує підприємство [1].

Операційна діяльність є одним з ключових аспектів успішної роботи будь-якого підприємства. Вона відображає процеси, пов'язані з виробництвом товарів або наданням послуг, а також ефективним управлінням ресурсами, щоб забезпечити максимальну продуктивність і досягти поставлених цілей.

Операційна діяльність має наступні важливі аспекти:

− операційна діяльність забезпечує виробництво та доставку товарів або послуг відповідно до попиту ринку. Це включає у себе процеси планування, закупівлі матеріалів, виробництва, контролю якості та логістики. Ефективна операційна діяльність дозволяє підприємству задовольняти потреби клієнтів вчасно та з високою якістю;

− операційна діяльність спрямована на пошук шляхів зниження виробничих витрат, оптимізацію використання ресурсів і підвищення продуктивності. Це може включати автоматизацію процесів, впровадження нових технологій, вдосконалення виробничих процедур та ефективне управління ланцюгом постачання. Чим більше ефективна операційна діяльність, тим менше витрати підприємства і більше можливостей для прибутковості;

− у сучасному бізнес-середовищі, де конкуренція є високою, операційна діяльність відіграє важливу роль у підтримці конкурентоспроможності підприємства. Здатність швидко реагувати на зм ні зміну вимог ринку, впровадження нових технологій і покращення якості допомагають підприємству займати лідируючі позиції. Висока якість продукції або послуг, а також надійність постачання, можуть стати вирішальними факторами для клієнтів у виборі між конкурентними підприємствами;

− операційна діяльність також сприяє інноваціям і розвитку підприємства. Вона забезпечує механізми для впровадження нових ідей, процесів та технологій, що дозволяють підприємству вдосконалювати свою продукцію або послуги. Інновації можуть займати різні форми, включаючи вдосконалення виробничих процесів, розробку нових продуктів або встановлення ефективних систем управління;

− операційна діяльність має прямий вплив на задоволення потреб і очікувань клієнтів. Швидке виконання замовлень, якісний продукт або послуга, вчасна доставка і гнучкість в реагуванні на зміну вимог клієнтів допомагають забезпечити їхню відданість та забезпечити повторні продажі. Задоволені клієнти також можуть стати амбасадорами бренду та рекомендувати його іншим, що сприяє росту бізнесу [8].

Операційна діяльність характеризується наступними особливостями: Саме вона являє собою головний компонент господарської діяльності фірми. Значна частина персоналу компанії, значна частка всіх активів, що формуються, йде на обслуговування цієї діяльності. Таким чином, у нормальних умовах прибуток від неї має значну питому вагу. Операційна діяльність підприємства є пріоритетною по відношенню до інших видів. З цієї причини розвиток будь-яких інших напрямків не повинен перебувати у суперечності з операційною діяльністю. Інтенсивність розвитку пріоритетного виду діяльності є основним параметром, що використовується для оцінки стадій життєвого циклу фірми.

Операційна діяльність спрямована переважно на товарний ринок, тоді як інвестиційна чи фінансова – на фінансовий ринок. Усі господарські операції, пов'язані з операційною діяльністю, мають регулярний характер. Нею частота операцій є найвищою. Саме операційна діяльність дає більшу частину прибутку та є джерелом фінансування розширення діяльності підприємства. Характер операційної діяльності, насамперед, визначається специфікою та особливостями галузі, до якої належить це підприємство. Більшість підприємств у її основі лежить торгова, виробничо-комерційна діяльність, яка може доповнюватися здійснюваною фінансовою чи інвестиційною. Операційна діяльність бізнес-організації є складовою основної діяльності. Підприємство може займатись оптовою та роздрібною торгівлею або мати розгалужену торгову мережу [3].

Отже, важливість операційної діяльності бізнес-організації полягає в тому, що вона допомагає забезпечити ефективне виробництво, зниження витрат, підвищення конкурентоспроможності, сприяє інноваціям та розвитку, а також задовольняє потреби клієнтів і підтримує стабільність та прибутковість підприємства. Ефективна операційна діяльність забезпечує потік матеріальних ресурсів, праці та інформації через усі внутрішні структури підприємства, забезпечуючи злагоджену роботу між різними відділами і функціональними областями.

Крім того, операційна діяльність впливає на репутацію бізнес-організації та сприяє його стосункам зі зацікавленими сторонами, включаючи постачальників, партнерів та громадськість. Добре організована і ефективна операційна діяльність сприяє побудові довгострокових взаємовигідних відносин із зацікавленими сторонами, а також зменшує ризики, пов'язані зі збитками, затримками в поставках або некоректною роботою підприємства [10].

Узагалі, операційна діяльність є суттєвим елементом успішного функціонування бізнес-організації. Вона впливає на його конкурентоспроможність, стабільність і рентабельність, а також визначає спроможність бізнес-організації адаптуватися до змін у ринкових умовах та забезпечувати задоволення клієнтів. Підприємства, які надають належну увагу операційній діяльності та постійно вдосконалюють її, мають більші шанси досягти успіху у своїй галузі та викликати довіру і лояльність своїх клієнтів [4].

Більшість людських і фінансових ресурсів бізнес-організації йде обслуговування цієї сфери, тому прибуток від неї має значну вагу. Тому інші види діяльності підприємства не повинні суперечити пріоритетному виду діяльності. Саме з інтенсивності її розвитку можна робити висновок про стадії життєвого циклу підприємства.

Операційна синергія відбувається, коли задля збільшення капіталу відбувається злиття підприємств. Яскравим прикладом операційної синергії

може бути об'єднання компаній «Exxon» і «Mobil». Їхня спільна робота принесла 80.3 млрд доларів.

Основна мета операційної діяльності компанії - виявити потреби для її життєздатності та подальшого вдосконалення. Операційна діяльність підприємства передбачає всі витрати, необхідні щоденної нормальної роботи підприємства.

Наприклад, ви вирішили відкрити підприємство у сфері послуг – сервіс вантажників. Операційна сфера діяльності включатиме:

- оренду офісу;
- рекламу послуг вантажників;
- прибуток від продажу;
- оплату комунальних послуг, Інтернету;
- банківську комісію за обслуговування ваших рахунків та ін.

Операційна діяльність не матиме відношення до:

- реконструкції приміщення;
- створення сайту та ін. [7].

Операційна діяльність - це основа господарської діяльності підприємства.

Принципи організації операційної діяльності включають оперування фінансовими коштами, які вже вкладені в підприємство. Кошти, які будуть інвестовані, є предметом фінансової та інвестиційної діяльності. З цього випливає, що прибуток підприємства залежить від пріоритетної діяльності. Якщо вона є неефективною, то неконкурентоспроможна компанія збанкрутує та піде з ринку. Усі витрати, що виникають у процесі виробничого циклу підприємства, є операційними.

Розглянемо виробничий цикл бізнес-організації. Тимчасовий відрізок, протягом якого відбувається оборот матеріальних активів бізнес-організації, називають виробничим циклом. Інакше висловлюючись, виробничий цикл – це час, протягом якого товар чи послуга буде зроблено, починаючи з запуску вихідних матеріалів (сировини й напівфабрикатів) у виробництво до виходу готового продукту. Виробничий цикл є основним економічним значенням під час аналізу життєдіяльності організації. Його розрахунок необхідний при аналізі роботи та подальшому плануванні розвитку компанії [12].

Головний показник виробничого циклу – його тривалість. На неї впливають три основні аспекти: технологічний, економічний та організаційний. Наприклад, час процесів збирання, обробки, транспортування деталей, вести робітників, рівень механізації, умови праці – усе це має великий вплив на тривалість циклу. Чим менша його тривалість, тим більше вивільнення капіталу ми маємо на виході. Звідси виходить, що розрахувавши тривалість циклу, ви зможете розширити виробництво товару або послуги в організації і забезпечити його розвиток і вигідне становище на ринку.

Тривалість виробничого циклу впливає виробничу потужність всього підприємства. Виробнича потужність - максимальна кількість продукції, яку підприємство може виробити за певний період часу. Тобто чим менше часу буде витрачено на виробництво одного товару, тим більша їх кількість буде виготовлена за цей період. Звідси випливає, що основне завдання підприємства – скоротити тривалість виробничого циклу [12].

Виробничий цикл бізнес-організації є послідовним процесом перетворення вхідних ресурсів у готову продукцію або надання послуги. Він охоплює всі етапи операційної діяльності, необхідні для виробництва і реалізації продукції. Основні етапи виробничого циклу включають:

- закупівля і постачання ресурсів, на цьому етапі бізнес-організація закуповує необхідні ресурси, такі як сировина, матеріали, обладнання, технології та інші компоненти. Вибір надійних постачальників, укладання контрактів і управління постачальницькими ланцюгами є важливими аспектами цього етапу;
- виробництво, цей етап включає фактичне перетворення ресурсів у готову продукцію або надання послуги. Він включає планування виробництва, організацію виробничих процесів, контроль якості та управління виробничим персоналом. Метою цього етапу є ефективне використання ресурсів для отримання якісної продукції або послуги;
- контроль якості, на цьому етапі здійснюється перевірка якості готової продукції або наданої послуги. Застосовуються методи інспекції, вимірювання, тестування та аналізу для забезпечення відповідності продукції встановленим стандартам і вимогам якості;
- упакування і маркування, на цьому етапі готова продукція упаковується та маркується відповідно до вимог і стандартів. Це включає вибір відповідної упаковки, використання підходящих матеріалів для захисту продукції під час транспортування і зберігання, а також нанесення маркування з необхідною інформацією про продукт, його склад, термін придатності, інструкції з використання та безпеки;
- зберігання і управління запасами, на цьому етапі готова продукція зберігається у складах або інших відповідних приміщеннях до моменту поставки або реалізації. Управління запасами включає планування і контроль за рівнем запасів, враховуючи попит, терміни поставок і стратегії забезпечення постачання;
- дистрибуція і реалізація, на цьому етапі продукція доставляється до кінцевих споживачів або реалізується через різні канали збуту. Це включає логістичне планування, організацію транспортування, розподіл, реалізацію та обслуговування клієнтів. Метою цього етапу є забезпечення своєчасної і ефективної доставки продукції клієнтам та задоволення їхніх потреб;
- сервіс та підтримка, після реалізації продукції бізнес-організація надає післяпродажну підтримку, сервіс та обслуговування клієнтів. Це може включати технічну підтримку, гарантійне обслуговування, навчання

користувачів та вирішення будь-яких питань або проблем, що виникають після покупки [2].

Виробничий цикл бізнес-організації є ітеративним процесом, де кожен етап виробничого циклу може повторюватись для виробництва нових партій продукції або надання додаткових послуг. Бізнес-організація має враховувати зміни в ринкових умовах, попиті споживачів і технологічному прогресі, щоб адаптувати свою операційну діяльність та покращувати ефективність виробничого циклу.

Постійне вдосконалення процесів, впровадження нових технологій, контроль якості та управління ризиками є важливими аспектами оптимізації виробничого циклу. Крім того, залучення інновацій, дослідження ринку, забезпечення ефективного управління затратами та ресурсами, а також вирішення проблем, що виникають під час виробництва, також впливають на результативність виробничого циклу.

Ефективне виконання виробничого циклу допомагає бізнес-організаціям досягати конкурентних переваг, забезпечувати високу якість продукції або послуги, задовольняти потреби клієнтів та досягати стабільної прибутковості. Крім того, оптимізація виробничого циклу сприяє збільшенню продуктивності праці, зниженню витрат, збільшенню швидкості виробництва і поліпшенню загальної ефективності бізнес-організації.

Схему формування операційного прибутку бізне-органзіації наведемо на рис.1.

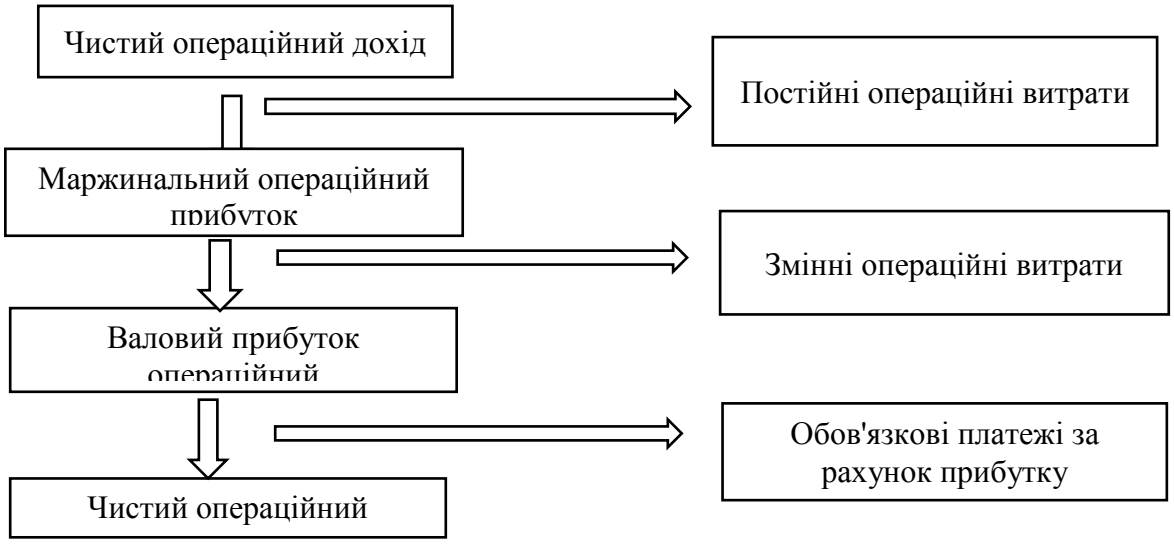


Рис.1. Схема формування прибутку бізне-органзіації [4;9;12]

Для визначення обігу коштів підприємства операційну діяльність можна поділити на кілька етапів.

Перший етап операційної діяльності зачіпає проблеми управління та контролю обсягу ресурсів для життєдіяльності бізнесу, бухгалтерські баланси, аналіз показників звіту про прибутки та збитки підприємства, інформацію з інших джерел за відповідний період. Недостатня кількість

ресурсів суттєво подовжить період освоєння виробництва, тоді як його надлишок може призвести до нераціонального використання виробничої сировини.

На другому етапі операційної діяльності відбувається виявлення потреби у певному вигляді обладнання, перерахунок показників першого етапу та вичленування чистого прибутку [4].

Третій етап операційної діяльності включає управління діями та заходами щодо організації роботи компанії.

Основні види ресурсів, що витрачаються для операційної діяльності підприємства

Ресурси – це фактори виробництва, що використовуються людиною, необхідні для нормального функціонування процесів виробництва та його розвитку.

Ресурси поділяються на:

- недостатні – ресурси, потужність яких менша, ніж потрібно (наприклад, малокваліфікований персонал, застаріле обладнання, верстати);
- обмеженої потужності – ресурси, завантаження яких йде практично на межі їх потужності, тобто без чітко спланованої роботи можуть стати недостатніми ресурсами (прикладом може служити тракторний завод СРСР, він був лише місцем збирання, деталі ж надходили в інших регіонах країни);
- надлишкові – ресурси, потужність яких перевищує потребу в них, тобто ресурси, при безперервній роботі яких, послуг буде надано більше, ніж потрібно, або виготовлено товарів у більшому обсязі, ніж потрібно (праця, капітал, природні ресурси) [9].

Організація операційної діяльності бізнес-організації є надзвичайно важливим аспектом його успіху. Чітко визначені процеси, ефективне управління ресурсами, контроль якості та уважне сприйняття потреб клієнтів допомагають підприємству досягти своїх цілей. Виробничий цикл, забезпечення постачання, контроль якості, логістика та обслуговування клієнтів є ключовими етапами операційної діяльності, які сприяють забезпеченню ефективності, прибутковості та задоволенню клієнтів. Постійне вдосконалення процесів і врахування змін в ринкових умовах є необхідними для підтримки конкурентоспроможності і досягнення успіху в сучасному бізнес-середовищі.

Список використаних джерел:

1. Бланк І. А. Фінансовий менеджмент: навчальний курс / І. А. Бланк. - Київ: Ніка-Центр Ельга, 2016. 528 .

2. Василенко О. В., Ткаченко Г. І. Виробничий (операційний) менеджмент: Навчальний посібник. К.: ЦУЛ, 2013. 532 с.

3. Карпенко Ю. В., Пєнова А. І. Теоретичні підходи до визначення поняття операційного менеджменту. Вісник соціально-економічних досліджень : зб. наук. праць. Одеса : Одеський національний економічний університет. 2020. № 3-4 (74-75). С. 88–98.

4. Коробка С. В. Теоретичні аспекти операційного менеджменту малих підприємств. Економічний простір. 2020. № 153. С.71-74.

5. Коцко Т.А. Операційний менеджмент: навчально-методичний комплекс дисципліни: навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2019. С. 120.

6. Крамарчук С.П., Лубкей Н.П. Сутність операційного менеджменту та основні етапи його розвитку. Інфраструктура ринку. 2020. №44. С. 83-86.

7. Лиса О. В., Завгородня А. О. Оптимізація операційної діяльності підприємств через застосування систем business intelligence. Ефективна економіка. 2020. № 1. – URL: http://www.economy.nayka.com.ua/?op=1&z=7591 (дата звернення: 01.06.2023).

8. Осокіна А. В., Чичкан-Хліповка Ю. М., Теоретико-прикладні аспекти управління операційною ефективністю підприємства. Чернігівський науковий часопис. Серія 1, Економіка і управління № 1 (6), 2015. с. 46-56.

9. Пєнська І. О. Організація планування операційної діяльності на підприємствах. Ефективна економіка. 2021. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=8910 (дата звернення: 10.03.2023).

10. Таранич О.В. Адаптація системи операційного менеджменту підприємств в умовах цифровізації економіки України. Економіка і організація управління. 2020. №4. С.143-151.

11. Ткачова С.С., Іванова Т.П. Операційний менеджмент. Навчальний посібник. Харків 2009. 452 с.

12. Трут О.О., Миколайчук І.П. Ефективність операційної діяльності роздрібного торговельного підприємства та методологія її вимірювання. Економічні науки. 2018. № 3. С. 26-32.

Басін А. О.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

АНАЛІЗ І ПОРІВНЯННЯ СУЧАСНИХ СЕРВІСІВ УПРАВЛІННЯ ІТ ПРОЄКТАМИ

Аналіз можливостей та інтеграцій сучасних диспетчерів завдань управління ІТ-проєктами.

У статті використано теоретичні методи дослідження, зокрема аналіз аналітичних досліджень з проблеми використання диспетчерів завдань для управління ІТ-проектами, узагальнення та систематизація інформації про можливості управління проектами, потенціал цифрових інструментів, зокрема Worksection, Jira, Asana, Trello, Monday.com і їхнє порівняння.

Останнім часом особливої популярності в управлінні ІТ-проєктами набули системи управління ідеями. Активно розробляються інноваційні та креативні методи та інструменти для стимулювання зростання ІТ-компаній, спрямованих на підвищення конкурентоспроможності та прибутковості. При управлінні розробкою ІТ-продукту використовуються нові системи управління ІТ-проєктами — цифрові інструменти, які стають інноваційними компонентами системи управління [1].

ІТ-проєкт – це комплекс завдань, спрямованих на розробку унікального продукту з чітко визначеними термінами, ресурсними обмеженнями, власними стандартами якості та концепцією успішного завершення [2]. Диспетчер завдань або система управління завданнями – це сервіс, який збирає в одному просторі всі робочі завдання ІТ-команди: організувати роботу компанії, спланувати роботу, організувати спілкування між членами команди, оптимізувати роботу з документами тощо. Враховуючи те, що роботодавці наголошують на важливості вміння користуватися цифровими інструментами, особливо диспетчерами завдань, ми вважали за доцільне розглянути ті інструменти, які зараз є найбільш популярними серед українських ІТ-компаній.

Worksection (https://worksection.com) — онлайн-сервіс для управління проєктами, створений програмістами з України. Він інтегрується з Google сервісами, CRM системами, Slack і Telegram. Згідно відкритим джерелам на цей час понад тисяча двісті компаній використовують програмне забезпечення для свого бізнесу всіх типів - цифрових агентств, вебстудій, компаній з виробництва відео тощо. Сервіс має український інтерфейс. Основні можливості Worksection включають: dashboard (розділ з ключовими індикаторами та індикаторами для аналізу задач), налаштовуваний інтерфейс, статистику часу, чат та спілкування в системі, діаграму Ганта,

Kanban, звіти про проєкти, технічна підтримка. Worksection має безкоштовну версію, що дозволяє використання до 5 користувачами, задіяних в двох активних проєктах та 100 МБ сховища.

Jira Atlassian (https://www.atlassian.com/software/jira). Це хмарний сервіс управління проєктами, який складається з трьох основних частин: Project (завдання, помилки та запити), Issues (список помилок) і Workflow (послідовність кроків). Jira має гнучкий підхід до управління проєктами. Основні функції Jira включають: планування проєкту, встановлення етапів, налаштування робочого процесу, Kanban, керування доступом і правами користувачів, аналіз проєкту та звітування. Jira Task Manager має кілька тарифних планів, включаючи безкоштовну версію з деякими обмеженнями.

Trello (https://trello.com/uk/tour) — це хмарний сервіс для спільної роботи над проєктами, який найкраще підходить для невеликих проєктів і команд. Основні функції Trello включають: сповіщення та сповіщення про крайні терміни; організацію тегів, міток, коментарів; контрольні списки прогресу; мобільну оптимізацію; Канбан, діаграми Ганта. Цей диспетчер завдань пропонує користувачам кілька тарифних планів, включаючи безкоштовну версію з обмеженими функціями.

Asana (https://asana.com). Цей диспетчер завдань доступний у веб-додатках і мобільних додатках і може використовуватися для адаптивних (гнучких) методів і персонального керування завданнями. Основні функції Asana включають: конструктор робочих процесів, діаграму Ганта, канбан, календар, інтеграцію додатків, візуалізацію робочого етапу. Цей цифровий інструмент також має безкоштовну версію на 14 днів з можливістю викодистання до 15 користувачами і добре інтегрується зі Slack, Gmail, Google Drive, Microsoft Teams, Dropbox і Zoom.

Monday.com (https://monday.com/) — це менеджер завдань, який дозволяє командам проєктів ефективно координувати свою роботу. Monday.com простий у гнучкому використанні для різних стилів команди та управління проєктами. Основні функції хмарних сервісів включають: автоматизацію робочого процесу, інтеграцію з електронною поштою, управління часом і грошима, діаграми Ганта, управління ресурсами, інформаційні панелі та спільна робота з документами. Monday.com пропонує користувачам веб-версію та мобільний додаток з безкоштовною пробною версією з обмеженим функціоналом.

НАЗВА	ВІДОБРАЖЕННЯ ЗАДАЧ	МОБІЛЬНИЙ ДОДАТОК	ІНТЕГРАЦІЯ З ІНШИМИ РЕСУРСАМИ	БЕЗКОШТОВНИЙ ТАРИФНИЙ ПЛАН
Worksection	дашбот, календар, комунікації, діаграма Ганта, Канбан-дошки, звітність	✓	✓	✓
Jira	календар, Канбан-дошки, управління доступом та правами користувачів, звітність	✓	✓	✓
Trello	Канбан-дошки, діаграма Ганта, календар, коментування	✓	✓	✓
Asana	конструктор робочого процесу, діаграма Ганта, Канбан-дошки, календар	✓	✓	✓
Monday.com	діаграма Ганта, управління ресурсами, дашботи, тайм-трекер	✓	✓	✓

Таблиця 1 Порівняльна таблиця можливостей диспетчера завдань

Порівняльний аналіз функцій управління IT-проєктами п'яти найпопулярніших таск-менеджерів представлено в Таблиці 1. Як видно з таблиці 1, кожен ресурс має свої переваги, можливості та може враховувати особливості та вимоги проєкту.

Таск-менеджери — це сучасний та перспективний цифровий інструмент, навички якого заохочуються та вимагаються роботодавцями. Кожен хмарний сервіс має свої ресурси, враховуючи методології управління проєктами та інші потреби. Слід також зазначити, що ринок цифрових інструментів постійно розвивається та збільшує свої можливості та функціонал. Тому ознайомлення із сучасними цифровими інструментами, зокрема з таск-менеджерами, їх функціональними можливостями та особливостями роботи з їх використанням у проєктній діяльності, є важливим фактором підготовки фахівців у різних галузях. Така підготовка може відбуватися в процесі вивчення спеціальностей, що відповідають потребам роботодавців, таких як управління IT-проєктами, основи дизайну та моделювання.

Список використаних джерел:

1. *Бублик М., Копач Т., Піхняк Т. Інноваційні системи менеджменту та їх інструменти для управління людським капіталом на ринку інформаційно-комунікаційних технологій. Економічний аналіз. 2022. Том 32. № 2. С. 277-285.*
2. *Сметанюк О.А., Бондарчук А.В. Особливості системи управління проєктами в IT-компаніях. Агросвіт. 2020. № 10. С. 105–111.*
4. *11 скілів, які допоможуть пережити 2022 рік. Посилання: https://laba.ua/blog/3086-11-skilov-kotorye-pomogut-perezhit-2022-god*
5. *Сайт Asana. Посилання: https://asana.com/*
6. *Сайт Jira. Посилання: https://www.atlassian.com/software/jira*
7. *Сайт Monday.com. Посилання: https://monday.com/*
8. *Сайт Trello. Посилання: https://trello.com/uk/tour*
9. *Сайт Worksection. Посилання: https://worksection.com*

Белов М. С.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ВЛИЯНИЕ ИНТЕРНЕТА И СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ НА ПОТРЕБИТЕЛЬСКОЕ ПОВЕДЕНИЕ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Думаю сегодня уже не у кого не вызывает сомнения тот факт, что влияние интернета и средств массовой информации (далее - СМИ) на общество, а особенно на современную молодежь очень значительно.

В мире уже порядка 2,5 млрд «цифровых пользователей» моложе 25 лет, которые «всегда на связи» и ежедневно проводят более пяти часов в режиме онлайн (вдвое больше, чем пользователи старше 25 лет). Более двух третей из них ежедневно посещают YouTube, почти половина используют социальные сети в качестве основной платформы для обслуживания. В этой аудитории четко просматривается тенденция перехода к «исключительно мобильному» доступу в Интернет [1].

Под понятиям потребления нужно понимать не только товары и услуги, а и знания, опыт, которые мы получаем путем потребления контента, информации. Потребление так или иначе встроено в повседневную жизнь общества и оказывает влияние на его настроение и формирование ценностей.

В современной модели потребления общества прослеживается важный критерий - индивидуализация. Каждый потребитель хочет выделиться из общества, показать свою индивидуальность, свое "внутреннее Я". Еще с 1960-х годов прошлого века уже начала развиваться тенденция об отказе массового поведения и выражении своей индивидуальности.

Эту тенденцию в частности отследили и маркетинговые компании, которые посредством интернета и СМИ влияют на потребление широкими массами нужных им вещей и товаров.

Работа с потребителем — анализ, прогноз, а по сути — управление его поведением — повседневная составляющая профессиональной деятельности каждого специалиста, занятого в сфере маркетинга.

Поведение потребителей (ПП) — относительно новая область знаний не только в России, но и в США — на родине менеджмента и маркетинга. Первые учебники по ПП появились в этой стране в 1960-е гг. В числе первых авторов — американские маркетологи Engel David Kollat, Roger Blackwell, чей учебник по ПП для университетов пережил девять изданий.

Американские специалисты *D. Hawkins, R. Best, K. Coney* предлагают концептуальную модель (рис. 1.1), вокруг которой и строится основное содержание дисциплины ПП [2].

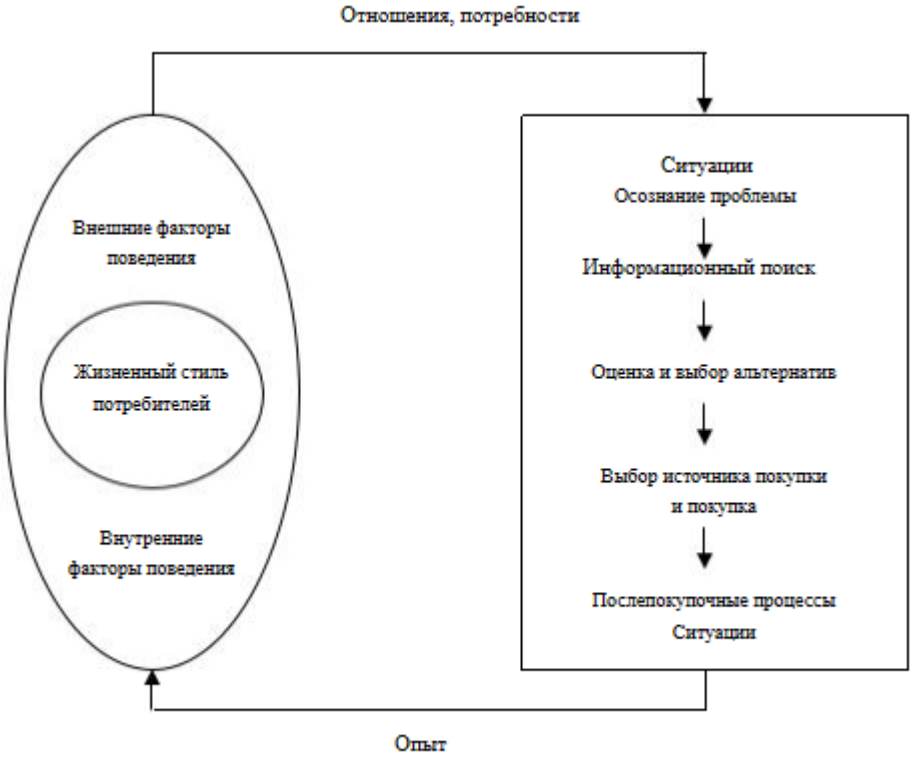


Рис.1.1. Модельпотребительскогоповедения

Таким образом учитывая развитие интернета большинство пользователей склоняются к поиску удовлетворения своих потребностей через интернет, где на них влияют маркетинговыми методами с помощью рекламы (банера, видео реклама, всплывающие окна с рекламой и др.), а так же не маловажное влияние с помощью целевой рекламы занимают СМИ (радио, ТВ, газеты, журналы).

В условиях жесткой конкуренции в сети интернет более весомым и важным для развития рыночных позиций торговых компаний и минимализации рисков является максимальное использование маркетинговыми подразделениями информации о потребительском поведении и факторах, влияющих на принятие решений о покупке. Сегодня современный потребитель отличается высокой активностью в своем рыночном поведении и становится более требовательным в выборе товаров и услуг. На рисунке ниже показана система факторов влияющих на потребительское поведение на рынке электронной коммерции в процессе принятия решения о покупке, которая объединяет внешние, внутренние, сдерживающие и мотивирующие факторы и позволяет учитывать специфику рынка е-торговли.

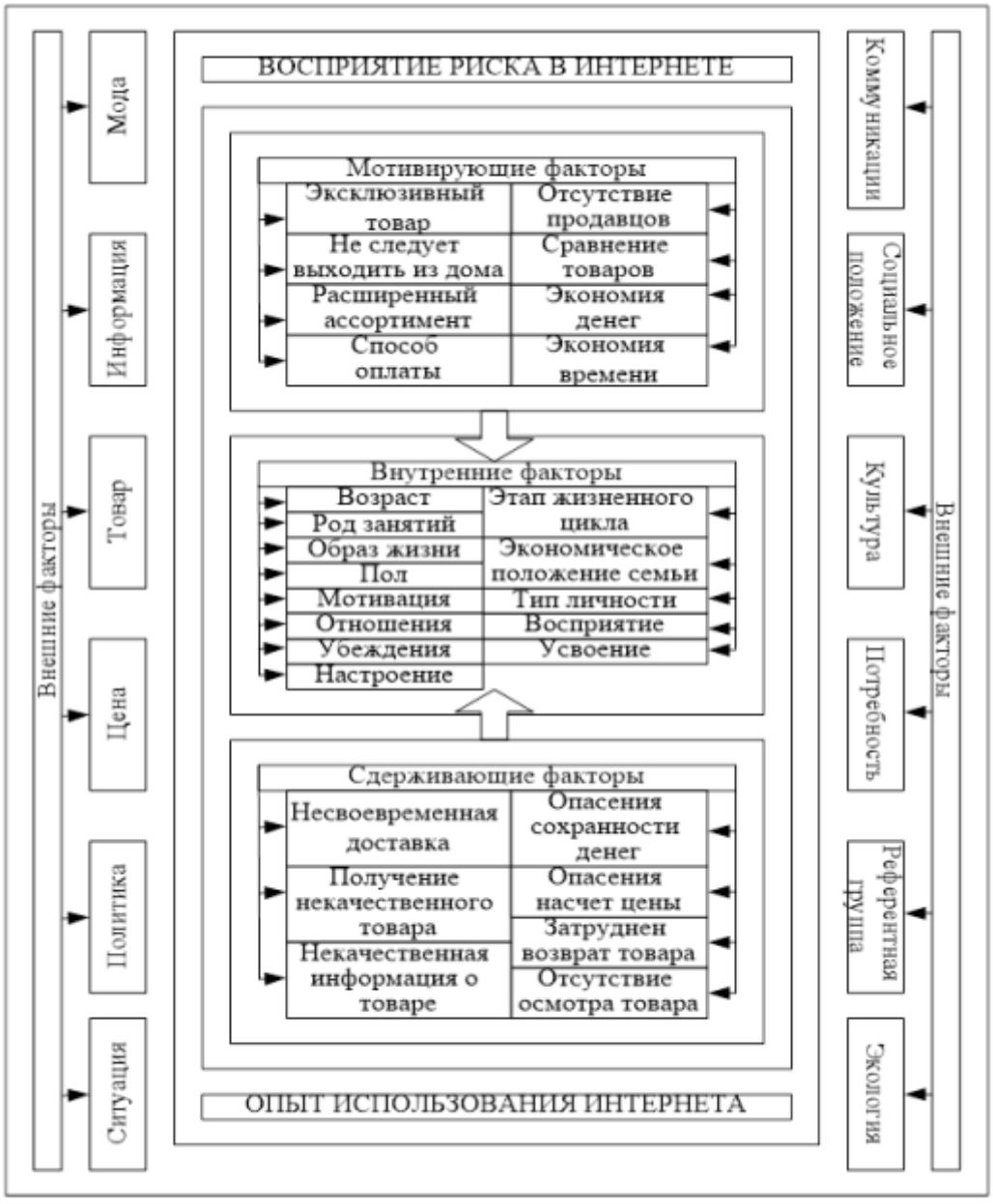


Рис. 1.2 Система факторов, оказывающих влияние на потребительское поведение на рынке электронной торговли в процессе принятия решения о покупке

Влияние интернета и СМИ более целенаправленно на молодежь, женщин и кибергражданам (Майкл Хаюбен, придумавший данный термин в начале 1990-х годов, определяет кибергражданам как людей, находящихся за рамками географических границ, которые заботятся и активно работают над развитием интернета на благо всего мира), которые уже давно тщательно изучаются предприятиями, но, как правило, в качестве отдельных клиентских сегментов. Их коллективная сила, особенно в качестве самых влиятельных сегментов цифровой эры, все еще плохо изучена. Молодежь является ранним первооткрывателем новыхпродуктов и технологий.Также молодые люди -

законодатели моды, но фрагментированы касательно трендов, которым следуют. И, наконец они те, кто меняют правила игры.

Будучи сборщиками информации и всеобъемлющими покупателями, женщины на самом деле являются одновременно и домашними менеджарами, и главными финансовыми директорами, менеджерами по закупкам, и управляющими активами семьи.

Наконец, кибергражданe являются социальными соединительными элементами, поскольку в подавляющем большинстве связываются, беседуют, и общаются со своими друзьями в интернете. Также они являются экспрессивными евангелистами, а еще - авторами контента в онлайн-мире. Все вместе - молодежь, женщины и кибергражданe являются ключом к маркетингу в цифровой экономике [3].

Подводя итоги можно сделать вывод, что влияние интернета и СМИ в современном обществе довольно высоко и продолжает увеличиваться. Этому способствует глобализация и отсутствие каких-либо границ в глобальной паутине. Интернет все больше и больше использует информационные технологии, которые значительно меняют поведение масс в вопросах потребления. Развитие сети интернет позволили потребителям получить постоянный доступ к информации и расширить свои возможности для социализации на глобальном уровне. Так же правильное влияние на потребителя может помочь в формировании новых моральных и этических ценностей, но при этом, необходимо правильно использовать способы воздействия на сознание социума.

Список использованных источников:

1. Кузнецова Т. Ф. Цифровизация и цифровая культура // Горизонты гуманитарного знания. 2019.

2. Алешина, И. В. Поведение потребителей : учебник. — М.: Экономистъ, 2006. - 525 с.

3. Айвен Сетиаван, Филип Котлер, Хермаван Картаджайа Маркетинг 4.0. Разворот от традиционного к цифровому: технологии продвижения в интернете [перевод с английского М. Хорошиловой]. — Москва : Эксмо, 2019. — 224 с.

Богомаз А. С.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНИХ ІНСТРУМЕНТІВ ПОБУДОВИ ОСОБИСТОГО БРЕНДУ

Поняття особистого бренду включає в себе набір цінностей, навичок, персональних якостей та поглядів, що асоціюються з конкретною людиною. Це те, як особистість репрезентує себе світу як з особистої, так і з професійної сторони. Аналогічно до корпоративного брендінгу, ціль особистого бренду – побудувати особливий, впізнаваний образ, що відрізняє особистість серед інших.

Термін особистий бренд першим ввів Том Пітерс – американський письменник і бізнес консультант, в статті «The Brand Called You» [1] («Бренд Називається Ви»). Там він визначає основні принципи побудови особистого бренду, що є актуальними і сьогодні, такі як самоаналіз, визначення своїх сильних сторін, пошук цільової аудиторії і стратегічне і гнучке планування свого майбутнього. Але з часом змінилися методи і їхня ефективність як для побудови особистого бренду, так і для продажів, в цілому. З появою соціальних мереж і алгоритмів просування контенту, механізми побудови особистого публічного бренду докорінно змінилися.

Існує багато досліджень, які вивчають ефективність використання особистого бренду для підвищення продажів у бізнесі [2, 3]. Багато компаній та підприємців успішно використовують особистий бренд для залучення клієнтів, збільшення своєї аудиторії та покращення іміджу свого бізнесу. Дослідження показують, що підтримка сильного особистого бренду може сприяти підвищенню довіри клієнтів, залученню нових можливостей та збільшенню конкурентоспроможності. Однак, результати можуть варіюватися в залежності від конкретного бізнесу та його цілей, тому важливо вивчати конкретний контекст та досліджувати, як найкраще використовувати особистий бренд для свого бізнесу.

Відповідно до дослідження, проведеного компанією LinkedIn, 75% покупців приймають рішення о купівлі під впливом соціальних мереж. При цьому 94% покупців проводять онлайн-дослідження продуктів перед придбанням [4]. В B2B сегменті продаж, згідно з дослідженнями 84% покупців починають процес закупок за рекомендаціями чи реферальними програмами. Ці дані вказують на важливість онлайн-присутності, упізнаваності і довіри серед потенційних клієнтів чи покупців. І побудова особистого бренду за допомоги соціальних мереж надає можливість отримати зазначені вище переваги.

Розглянемо основні соціальні мережі, що використовуються як платформи, для розбудови особистого бренду.

1. LinkedIn

LinkedIn — це професійна соціальна платформа, яка широко використовується для персонального брендингу. Вона надає інструменти і можливості для демонстрації своїх професійних досягнень, навичок та досвіду у своєму профілі, спілкуватися з колегами з галузі, приєднуватися до відповідних груп і ділитися цінним вмістом. Акцент LinkedIn на професійних мережах робить його чудовим вибором для створення особистого бренду в бізнесі та кар'єрному секторі.

Більшість користувачів у LinkedIn входять в вікові категорії 24-35 та 35-54 та репрезентують бізнес, або себе як професіоналів. Таким чином, гарно підходить для побудови власного бренду з тематикою професійного розвитку або B2B продажів.

2. Instagram

Instagram зосереджується на візуальному контенті, що робить його ідеальним для персонального брендингу, пов'язаного з творчими сферами, способом життя, модою, подорожами та іншими візуально привабливими галузями. Ви можете продемонструвати свій досвід, поділитися закулісним матеріалом і спілкуватися зі своєю аудиторією за допомогою захоплюючих зображень, відео та історій.

Instagram має велику базу користувачів, приділяючи значну увагу молодшим демографічним групам. Більше спрямований саме на B2C сегмент, проте в де-яких випадках може використовуватися і для B2B продажів, завдяки дуже великій розповсюдженності. Популярними типами контенту про побудові бренду є:

- Лайфстай та хобі: користувачі демонструють свої хобі, досвід подорожей, фітнес-мандрівки, продукти харчування та модні тенденції.
- За лаштунками: популярними є закулісні проблиски подій, творчих процесів і особистих історій.
- Інфлюенсерський маркетинг: багато користувачів співпрацюють з брендами для просування продуктів і послуг за допомогою спонсорованого контенту.

3. Twitter

Twitter надає платформу для спілкування та взаємодії в реальному часі. Це дозволяє користувачам ділитися короткими та стислими оновленнями, галузевими ідеями та спілкуватися з впливовими особами та лідерами думок. Twitter може бути корисним для побудови особистого бренду в сферах, де важливий швидкий і своєчасний обмін інформацією, наприклад у новинах, технологіях або соціальних проєктах.

Користувачі твітеру теж мають дуже широку демографію з ухилом до молодих людей, як і Instagram. Twitter не надає особливих інструментів для

створення контенту, його основна перевага – лаконічні повідомлення і швидкість їхнього розповсюдження завдяки алгоритмам рекомендацій.

4. YouTube

YouTube — це потужна платформа для створення та обміну відеоконтентом. Він дає можливість зарекомендувати себе як експерт, ділитися навчальними посібниками, інформацією про галузь або вести відеоблоги та спілкуватися з широкою аудиторією.

Зазвичай, контент на YouTube залишається актуальним довше, ніж на інших платформах, але він і значно складніший і дорожчий у виробництві. YouTube має дуже широку аудиторію користувачів а також потужні алгоритми рекомендацій, тому він підходить для дуже різних цільових аудиторій.

5. Facebook

Facebook пропонує широке охоплення та різноманітну базу користувачів, що робить його придатним для персонального брендингу в різних галузях. Ви можете створити професійну сторінку чи групу, ділитися вмістом, взаємодіяти з підписниками та використовувати рекламні функції Facebook, щоб розширити видимість свого бренду.

Незважаючи на те, що найбільшою віковою групою користувачів Facebook є 18-34 (майже половина всіх користувачів), Facebook має найбільшу частку користувачів більш літнього віку у порівнянні з наведеними вище платформами. До категорії 35-44 відноситься 19,3% користувачів, а до категорії 45-54 – 11,6% [6].

З точки зору контенту Facebook Facebook пропонує широкий спектр типів вмісту, включаючи оновлення статусу, фотографії, відео та статті. Користувачі діляться особистими новинами, життєвими подіями та досвідом зі своїми друзями та знайомими, а також об’єднуються у групи на основі спільних інтересів, хобі, професійної приналежності або місцевих спільнот.

6. TikTok

TikTok набув величезної популярності, особливо серед молодшої аудиторії. Це платформа короткого відео, яка дозволяє вам продемонструвати свою творчість, навички та особистість. TikTok може бути корисним для персонального брендингу в таких сферах, як розваги, мистецтво чи спосіб життя, де цінується привабливий і розважальний контент.

Користувачі переважно належать до вікової групи 16-24 роки, але охоплення платформи розширюється й на старші вікові групи. TikTok – це дуже молода соціальна мережа, що дуже активно розвивається. Тому якщо тип контенту підходить до стратегії розвитку персонального бренду, то треба пам’ятати, що демографія платформи змінюватиметься разом з розвитком особистого бренду.

TikTok надає платформу для створення і споживання коротких відео тривалістю від кількох секунд до хвилини. Наразі, особливу популярність

має розважальний та творчій контент: комедійні скетчі, розіграші, танці та різноманітні челенджі, суть яких полягає в тому, щоб записати незвичайне відео в заданому форматі.

При побудові особистого бренду має дуже велике значення присутність в інтернеті. Незалежно від того, чи людина розвиває власний бізнес, чи веде продажі від лиця компанії, чи представляє себе на ринку праці, як професіонала, якісна репрезентація себе в інтернеті значно підвищує шанси на успіх. При побудові бренду необхідно визначити свої цінності, аудиторію і, відповідно, інструменти. Соціальні мережі дають дуже багато можливостей для побудови якісної репрезентації себе і кожна має свої власні переваги, але якісно вести одразу всі вимагає дуже багато часу та ресурсів, тому варто обрати одну чи декілька і зосередитись на них поступово розширюючи свою присутність в інтернеті.

Список використаних джерел:

1. *Tom Peters – The Brand Called You [Електронний ресурс] – Режим доступу: https://www.fastcompany.com/28905/brand-called-you*
2. *Social Buying Meets Social Selling: How Trusted Networks Improve the Purchase Experienc [Електронний ресурс] – Режим доступу:*
3. *Why Personal Branding Is Crucial for Any Industry [Електронний ресурс] – Режим доступу: nhttps://www.business.com/articles/personal-branding-boosts-marketing/*
4. *Дослідження соціальних продажів від LinkedIn [Електронний ресурс] – Режим доступу: https://business.linkedin.com/sales-solutions/social-selling*
5. *Статистика користувачів платформи Facebook [Електронний ресурс] – Режим доступу: https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/*
6. *Дослідження демографії користувачів соціальних мереж [Електронний ресурс] – Режим доступу: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/*

Бурлака Ю. В.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

СТВОРЕНННЯ ТА РОЗВИТОК RESEARCH&DEVELOPMENT КОМАНДИ В РАМКАХ МАРКЕТПЛЕЙСУ PROM.UA

R&D (research and development) – термін, яким зазвичай описують процеси досліджень, експериментів та розробок для отримання нових знань, зменшення невизначеності, створення нових продуктів або процесів та покращення існуючи.

В кожній продуктовій компанії існує цикл розвитку продукту. На розвиток продукту впливає безліч факторів, ключовими з яких є:

1) Зміна економічного, політичного, соціального середовищ
2) Зміна на ринку й самого ринку
3) Вплив конкурентів (їх розвиток, стратегія і т.д.)
4) Зміна візії, місії самої компанії
5) Вплив непередбачуваних обставин

Ці фактори формують виклики для компанії, продукту, команд і як наслідок готовності до них та швидкої адаптації та у висновку - виживання. Виклики змушують компанії постійно експериментувати та досліджувати вплив змін на свої продукти. Тож сьогодні етап дослідження та експериментів є неодмінною і постійною частиною циклу розвитку продукту.

Історично розвиток продуктових компаній та промисловості в цілому відбувався поетапно, і усвідомлення впливу важливості досліджень чи експериментів відбувалося через набуття досвіду і перегляду принципів створення продукту і результату його реалізації. З часом компанії приходили до процесів, в основі яких, лежить глибоке розуміння потреб клієнтів і їх цілей. Вплив зовнішніх факторів прискорював цикл розробки і компанії дедалі більше відчували потребу в постійних дослідженнях, а також з прискоренням виробничого циклу дедалі частіше відчували проблему з нестачею часу. Тоді почала виникати і розвиватися потреба в дослідженнях і окремих дослідницьких командах та процесах інтегрованих у виробничий цикл. Потреба ставала системною і в результаті R&D команди зайняли ключове місце в традиційній структурі продуктових компаній.

Загалом концепцію розвитку R&D компаній можна розділити на такі етапи:

1) 20-те століття: на початку розвитку індустріалізації був обмежений фокус на дослідженнях для максимізації темпів виробництва. Разом з тим почали з'являтися нові технології та виникала потреба в зростанні науково-технічної експертизи для чого виникла необхідність в створенні окремих команд дослідження і розвитку

2) 30-ті роки: розвиваються такі галузі як фармацевтика, електроніка, авіація котрі потребують значних інвестицій в дослідження і відповідно в дослідницькі лабораторії що провокує їх ріст та розвиток в рамках традиційних структур та процесів

3) Повоєнний період: Друга світова війна спровокувала вибухове розширення наявних дослідницьких команд та лабораторій, вони починають займатися новими галузями. Приватні компанії починають вкладати значні ресурси у розвиток власних дослідницьких, R&D підрозділів

4) 70-ті роки: розробляється концепція інноваційного управління, усвідомлюється стратегічна важливість R&D команд зокрема у створенні та розвитку нових продуктів та конкурентних переваг. R&D стає основним рушієм продуктової компанії

5) Сучасність: R&D процеси та команди майже безшовно інтегровані в систему управління компаній і є неодмінною складовою кожної галузі

Тож кожна компанія з часом приходить до потреби створення спочатку R&D процесів інтегрованих в поточні команди, а згодом і відокремлення окремої R&D команди. Далі розглянемо типовий процес створення R&D команди на прикладі українського маркетплейса prom.ua.

З початку свого заснування prom.ua був стартапом. Головна відмінність стартапу від компанії – перевірка життєздатності конкретної бізнес-моделі. Тож команда стартапу змушена постійно експериментувати та досліджувати і по своїй суті це вже з самого початку R&D команда. Та згодом, коли бізнес-модель набуває усталених властивостей і продукт виходить на цикл окупності стартап набуває рис та структури традиційної компанії і цикли досліджень звужуються до окремих точкових процесів.

Звуження циклів досліджень призводить до наступних проблем

1) Продукт перестає розвиватись

2) Фокус розробки спрямований виключно на покращенні та ускладненні існуючого функціоналу

3) Бізнесові показних або перестають зростати або стають залежними від масштабування інвестицій

4) Технічна база продукту старіє та ускладнюється, тож з часом внаслідок вартості і складності розробки практично втрачається здатність швидко змінювати та розвивати продукт

Ці проблеми у висновку призводять до втрати конкурентоспроможності, долі ринку і швидкого занепаду та загибелі продукту.

Як свого часу і prom.ua, так і інші компанії помічають тривожні фактори деградації процесів дослідження та шукають драйвери їх перезапуску. В нас це відбулося в кілька болісних етапів, ми їх називаємо «зміною парадигми». І це завжди буде болісно для поточної усталеної структури, бо потребує виводу із зони комфорту всіх процесів та перебудови звичок.

Тож маємо наступні кроки до створення R&D команди

1) Усвідомлення топменеджментом тривожних факторів одного, кількох або навіть усіх одразу
2) Усвідомлення топменеджментом наслідків ігнорування цих факторів в перспективі і вплив наслідків на стратегію компанії та на її прибутки
3) Чесна комунікація на всю компанію проблематики і важливості змін
4) Проговорення в кожній команді сенсу R&D процесів, цей пункт важливий тим що R&D процеси чи команди мають бути глибоко та безшовно інтегровані в інші команди і процеси
5) Пропрацювати в кожній команді R&D цикли та етапи
6) Домовитись та погодити відповідальність і межі відповідальності
7) Моніторити результат змін та корегувати процеси відповідно до очікувань

В процесі реалізації кроків як правило виникне або не виникне потреба в окремій R&D команді. Тут більш важливими є наявність інтегрованих R&D процесів в компанії аніж створення окремої команди. А в деяких випадках інтеграція R&D процесів в поточні команди більш ефективна аніж створення нової команди.

Ключові R&D процеси в поточних командах або виділеної R&D команди в маркетплейсі:

1) Моніторинг технічного стека продукту
2) Оцінка технічної спроможності продукту з огляду на відповідність стратегії розвитку
3) Оцінка складності технічного стека та його гнучкості
4) Моніторинг розвитку технічних альтернатив на ринку
5) Дослідження та тестування технічних та продуктових альтернатив
6) Оцінка потенціалу змін в технічному стеку
7) Пошук та дослідження можливостей та інструментів розвитку для команд
8) Оцінка технічних та продуктових ризиків

Серед важливих проблем наявності R&D команди можна виділити ізольованість такої команди та розвиток культури «свій-чужий». Це вкрай негативні наслідки і сигнал до пошуку проблем та необхідних змін. Інакше, без інтеграції такої команди в процеси інших команд і без розуміння цінності іншими командами результату не буде, в гіршому випадку навіть почнуться конфлікти й демотивація.

Тож у висновку маємо розуміння цінності і від впровадження окремих R&D процесів і від створення виділеної R&D команди, але разом з тим маємо й відповідні ризики котрі можуть навпаки негативно вплинути й на сам продукт й на його розвиток.

Список використаних джерел:

1. *"The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail" - автор Clayton M. Christensen*
2. *"The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses" - автор Eric Ries*
3. *"Innovation and Entrepreneurship: Practice and Principles" - автор Peter F. Drucker*
4. *"The Myths of Innovation" - автор Scott Berkun*
5. *"The Art of Innovation: Lessons in Creativity from IDEO, America's Leading Design Firm" - автори Tom Kelley та Jonathan Littman*
6. *"Managing Innovation: Integrating Technological, Market and Organizational Change" - автор Joe Tidd та John Bessant*

Гремляцкий А. В.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

УЛУЧШЕНИЕ ЗАПАСА ФИНАНСОВОЙ ПРОЧНОСТИ КОМПАНИИ С ПОМОЩЬЮ АНАЛИЗА ТОЧКИ БЕЗУБЫТОЧНОСТИ

В операционном анализе компании, точка безубыточности является одним из ключевых элементов определения эффективности основных, системных процессов.

Показатель запаса финансовой прочности компании находится в прямой зависимости от точки безубыточностиТочка безубыточности (критическая точка, CVP-точка) (англ. break-even point) - объём производства и реализации продукции, при котором расходы будут компенсированы доходами, а при производстве и реализации каждой последующей единицы продукции предприятие начинает получать прибыль.

Точка безубыточности определяется в единицах продукции, в денежных единицах. Расчёт точки безубыточности осуществляется при известных значениях: цена за единицу товара, постоянные и переменные расходы. В случае расчёта точки безубыточности для множества товаров или услуг, которые отличаются по цене и себестоимости, - рекомендуется применять денежное выражение по всему объёму расходов и выручки. Точка безубыточности в денежном выражении имеет следующую формулу [1]:

$$BEP = \frac{TFC}{\frac{C}{P}} = \frac{TFC}{\frac{(P - AVC)}{P}}$$

где:

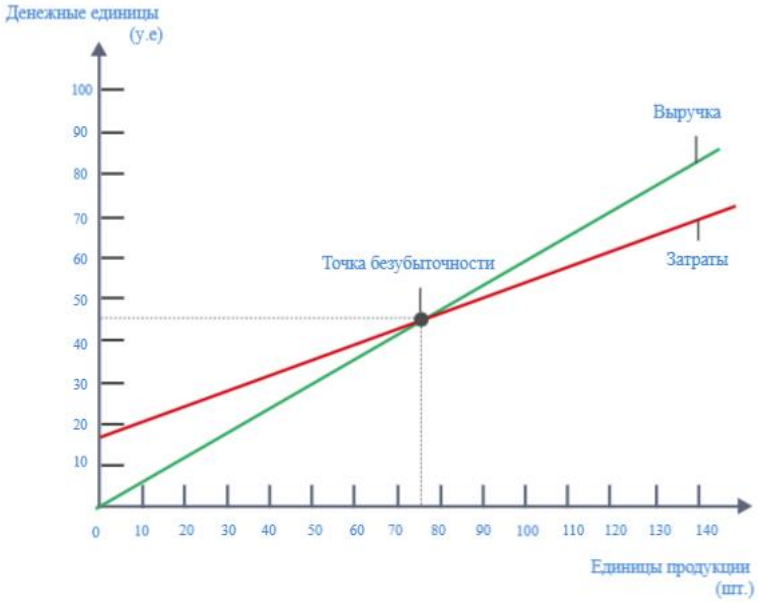
BEP (англ. break-even point) - точка безубыточности;

TFC (англ. total fixed costs) - величина условно-постоянных издержек;

AVC (англ. unit average variable costs) - величина условно-переменных издержек на единицу продукции;

P (англ. unit sale price) - стоимость единицы продукции (реализация);

C (англ. unit contribution margin) - прибыль с единицы продукции без учёта доли постоянных издержек (разница между стоимостью продукции (P) и переменными издержками на единицу продукции (AVC)).



Значение точки безубыточности даёт возможность:

- Определения оптимальной стоимости товара или услуги;
- Прогнозирования объема производства и продаж для получения рентабельности;
- Анализа обоснованности издержек;
- Контроля нижней границы финансовой устойчивости организации.

Точка безубыточности оказывает прямое влияние на запас финансовой прочности.

Запас финансовой прочности - это показатель финансовой устойчивости предприятия, который определяет до какого уровня предприятие может уменьшить свое производство (или объёмы продаж), не неся при этом убытков. Запас финансовой прочности может быть рассчитан как в абсолютном (стоимостном), так и в относительном (процентном) выражении:

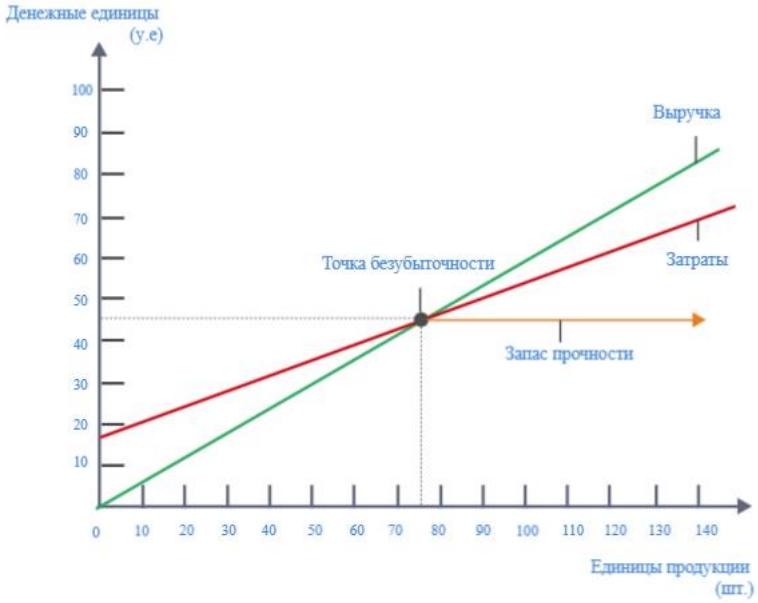
- Относительная величина, выражающаяся в процентном соотношении данной разницы к объему фактической реализации;
- Абсолютная величина - разность между объемами, которая вычисляется по формуле [2]:

$$ЗФП = \frac{(Q - BEP)}{Q}$$

где:

BEP (англ. break-even point) - точка безубыточности;

Q (англ. quantity) - объем произведенной (реализованной) продукции или их плановые показатели



В зависимости от показателя запаса финансовой прочности, положение организации может быть охарактеризовано следующим образом[3]:

Показатель ЗФП	Состояние организации
меньше 0.2	Кризисное состояние и большая вероятность банкротства
от 0.2 до 0.5	Неустойчивое состояние и есть риск банкротства
от 0.5 до 0.8	Устойчивое состояние с минимальным риском банкротства

Зная точку безубыточности и запас финансовой прочности (фактический) можно найти необходимый объем продукции (произведённой, реализованной) для достижения желаемого запаса финансовой прочности[4]:

$$Q = \frac{BEP}{(1 - ЖЗФП)}$$

где:

Q (англ. quantity) - объем произведенной (реализованной) продукции или их плановые показатели;

BEP (англ. break-even point) - точка безубыточности;

ЖЗФП - желаемый запас финансовой прочности

Способы улучшения запаса финансовой прочности следующие:

- Первый - увеличение выручки от продаж. Для этого необходимы новые маркетинговые компании или повышение цен. Возможен подход, когда это делается одновременно.

- Второй - снижение показателя точки безубыточности. Для этого компания использует методы для повышения оборота.

- Третий - уменьшение расходов. Для этого компании необходимо сократить постоянные затраты или уменьшить переменные. Возможен подход, когда это делается одновременно.

Список использованных источников:

1. *Макконнелл К. Р., Брю С. Л. Экономикс: принципы, проблемы и политика : [рус.] = Economics: Principles, Problems, and Policies. — М. : Республика, 1992. — Т. 2*

2. Финансовый Директор - Запас финансовой прочности URL:https://www.fd.ru/articles/158472-zapas-finansovoy-prochnosti-formula-rascheta-qqq-17-m2

3. Calltouch Blog - Запас финансовоф прочности URL: https://www.calltouch.ru/blog/glossary/zapas-finansovoj-prochnosti

4. *КУБ24 Точка безубыточности. Оцениваем финансовое состояние бизнеса URL:https://kub-24.ru/2023/03/14/tochka-bezubytochnosti-otsenivaem-finansovoe-sostoyanie-biznesa*

Гуменюк Р. С.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МАШТАБОВАНИХ ФРЕЙМВОРКІВ ОРГАНІЗАЦІЇ РОБОЧИХ ПРОЦЕСІВ

Результат аналізу існуючих масштабованих фреймворків для організації процесів надає розуміння того, що є два основних, найбільш популярних з них – SAFe (Scaled Agile Framework) та LeSS (Large Scale Scrum).

Почнемо з SAFe, який розроблений для масштабування методології Agile. SAFe надає структурований підхід до організації роботи команд та їхньої спільної роботи над складними проектами. Цей фреймворк дозволяє організаціям швидко реагувати на зміни та забезпечує збалансовану комунікацію між різними рівнями управління. Використання SAFe допомагає організаціям досягати більшої ефективності, зменшувати ризики та підвищувати якість продукту.

Перша особливість SAFe - його багаторівневий підхід. Фреймворк охоплює кілька рівнів масштабування, залежно від розміру організації. Кожен рівень має свої відповідності, ролі та відповідальності. Це дозволяє забезпечити узгодженість та синхронізацію між різними командами та проектами в організації.

Друга особливість SAFe - визначені ролі, процеси та артефакти. Фреймворк визначає ролі, такі як Product Owner, Scrum Master, Release Train Engineer, та багато інших, які мають чітко визначені відповідальності та обов'язки на кожному рівні масштабування. Крім того, SAFe надає набір процесів та артефактів, таких як Program Increment (PI) Planning, PI Objectives, PI System Demo, які допомагають організації розпланувати, виконувати та відслідковувати роботу згідно з масштабованими Agile-принципами.

Другий фреймворк, це LeSS. LeSS спрямований на масштабування Scrum методології розробки програмного забезпечення. Він акцентує увагу на простоті та гнучкості, забезпечуючи єдину команду розробників, яка працює над спільними цілями. LeSS сприяє швидкому реагуванню на зміни, сприяє колаборації та залученню клієнтів, що допомагає створювати цінність для бізнесу.

Перша особливість LeSS - це простота та гнучкість. Фреймворк спрощує масштабування, уникавши надмірної складності та зайвих процесів. Він ставить акцент на основні принципи Scrum, дозволяючи командам працювати самоорганізовано та заохочуючи ітеративну та інкрементальну розробку.

Друга особливість LeSS - це єдина команда розробників. Фреймворк підтримує концепцію однієї команди, яка працює над спільними цілями. Це допомагає забезпечити високу комунікацію, співпрацю та взаємодію між учасниками проекту. Замість розділення команд на багато підкоманд, LeSS сприяє колаборації та розвитку синергії серед розробників.

LeSS також надає різні рівні масштабування, що дозволяє пристосувати фреймворк до потреб організації. Він дозволяє залучати клієнтів та зацікавлених сторін в процес розробки, що сприяє створенню цінності для бізнесу та забезпечує взаємодію зі споживачами продукту.

Порівнявши дві маштабовані фреймовки - SAFe та LeSS - можна зробити наступний висновок. Обидва фреймворки - SAFe та LeSS - мають свої переваги та застосування, залежно від конкретних потреб організації.

SAFe надає більш структурований підхід до масштабування, забезпечуючи збалансовану комунікацію та ефективну роботу команд над складними проектами. Використання SAFe дозволяє організаціям мати детальну інструкцію того, як діяти у конкретних випадках, з дуже детальним проясненням кожного процесу і кроку у ньому.

З іншого боку, LeSS зосереджується на простоті та гнучкості. Він підтримує одну горизонтальне масштабування без багаторівневої ієрархії у організації, де команда спільно працює над спільними цілями. LeSS сприяє колаборації та залученню клієнтів, допомагаючи створювати цінність для бізнесу. Проте він потребує більше навчання та вищий рівень залученості працівників.

Вибір між SAFe та LeSS залежить від конкретних потреб організації. Якщо вам потрібна більш структурована та організована система для масштабування Agile-проектів, то SAFe може бути кращим варіантом. У той же час, якщо ви пріоритетно ставите на простоту, гнучкість та активну участь команди, то LeSS може відповідати вашим потребам краще. В кінцевому підсумку, вибір для побудови організації повинен враховувати контекст, розмір та потреби вашої компанії. Кращим підходом може бути вивчення обох фреймворків, їхніх принципів та прикладів успішного використання, аби опиратись на цьому.

Список використаних джерел:

1. Dean, L., & Leffingwell, D. Scaling Software Agility: Best Practices for Large Enterprises. Addison-Wesley. 2011.

2. Larman, C., & Vodde, B. Large-Scale Scrum: More with LeSS. Addison-Wesley. 2016.

Димов В. В.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

АДАПТИВНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ МАЛОГО БИЗНЕСА

Нестабильность мировой и украинской экономики, вследствие чего произошло повышение уровня неопределенности и изменчивости окружающей среды, обусловило необходимость создания новых механизмов и структур управления хозяйствующими объектами. На этом этапе в условиях постоянных внешних изменений раз налаженные хозяйственные и производственные процессы не обеспечивают высокий уровень конкурентоспособности большинства украинских организаций. Этот факт вызывает необходимость использования в организациях инструментов адаптивного управления.

Для того чтобы процесс адаптации к условиям бизнес-среды был целенаправленным, им необходимо управлять. Задача адаптивного управления – это управленческие задачи в условиях повышенного риска и неопределенности.

Первоначально понятие «адаптация» использовалось в естественных науках, и понималась она как «произведенное в процессе эволюционного развития приспособление биологической системы к условиям окружающей среды» [3].

Анализ литературных источников показал, что, несмотря на широкое применение, теоретически управление не имеет универсального определения адаптации.

Отметим, что на этот термин нет единого общепринятого толкования. В таблице 1.1 приведены некоторые определения рассматриваемого понятия.

Автор	Формулировка определения
С. Ю. Ткач и Е. В. Никулина [1]	адаптивное управление – совокупность методов теории управления, позволяющих синтезировать системы управления, имеющие возможность изменять параметры регулятора или структуру регулятора в зависимости от изменения параметров объекта управления или внешних возмущений, действующих на объект управления
О. Г. Тихомирова [2]	Адаптивное управление (адаптивный

	менеджмент) представляет собой новенькую методологию управления предпринимательскими структурами, основанную на изменении форм управления в зависимости от условий функционирования и стадии развития системы.
Б. А. Эфендиев [4]	адаптивное управление – это управление с обратной связью, имеющее блок учета внешних факторов, которые анализируются еще до того, как получен результат деятельности системы
Н. В. Зяблицкая [3]	Под адаптивным управлением мы будем понимать управление социально- экономической системой, нацеленной на скорейшее достижение системой нормативного уровня адаптивности при минимальных адаптационных затратах.

С целью данного исследования будем рассматривать традиционную систему факторов внешней среды:

- экономические (состояние мировой, гос, региональной экономик, рабочие кадры, доходы населения, занятость и т.п.);
- социальные (здоровье, демография, уровень образования, возраст, система образования, состав семьи, социальные ориентиры и ценности и др.);
- политические (внутренняя и внешняя политика государства, государственные расходы и национальные доходы, введенные санкции и антисанкции);
- технологические (развитие интернет-технологий, инноваций и др.).

Наиболее распространенными методами анализа окружающей среды являются анализ SWOT и анализ влияний.

На основании анализа воздействий на предприятия, в том числе торговые, целесообразно использовать экспресс-диагностику управленческой системы предприятия.

Экспресс-диагностика управленческой системы проводится методом экспертных оценок по основным подсистемам предприятия: общее управление, управление персоналом, финансами, маркетингом, снабжением, продажами (сбытом).

На диагностическом профиле определяется проблемное поле менеджмента с учетом следующих интервалов состояния систем:

- от 1 до 1.7 – кризисное состояние подсистемы;
- от 1.8 до 2.6 – неустойчивое состояние подсистемы;
- от 2.7 до 3.5 – состояние нормы;
- от 3.6 до 4 – идеальное состояние.

Таким образом, каждый из элементов оказывает специфическое влияние на деятельность предприятия и характеризуется определенными показателями. Их анализ позволяет отследить повышение или, напротив, уменьшение возможностей развития предприятия [5].

Эффективность адаптивного управления определяется как информативностью индикаторов и параметров состояния внутренней и внешней среды предприятия, методами их анализа, управленческими решениями, так и готовностью к реагированию на изменения во внешней и внутренней среде имеющимся набором возможных адаптивных вариантов решений. Совокупность готовых решений разрабатывается методом определения адаптивных стратегий.

В научной литературе не существует универсального понятия адаптации, но во всех определениях адаптации и адаптивного управления присутствует свойство системы приспосабливаться к изменяющимся условиям окружающей среды. Это свойство называется адаптивностью.

Адаптивность предприятия позволяет приспособиться к возмущающим воздействиям окружающей среды путем изменения организованности.

Адаптивность является важнейшим фактором реализации конкурентных преимуществ любых предприятий, в том числе торговых.

Список использованных источников:

1. Гросул В., Шинкаренко И. Доминанты и барьеры адаптивного развития системы управления предприятием розничной торговли в условиях цифровых трансформаций экономики // Scientific Collection «InterConf +». 2022. №. 28 (137). С. 8-14.

2. Горбаль Н. И., Романишин С. Б. Система управления конкурентоспособностью предприятия // Научный вестник НЛТУ Украины. 2010. Т. 20. №. 12. С. 112-117.

3. Адаптивная система управления поставками и запасами крупного металлургического предприятия // Вестник Запорожского национального университета. 2010. №. 2. С. 6.

4. Костырко Л. А. Перспективы формирования адаптивной системы управления стоимостью предприятий // Вестник Восточноукраинского национального университета имени Владимира Даля. 2014. №. Первый С. 64-68.

5. Милаш И. В. Адаптивное управление торговым предприятием: сущность и содержание // Рекомендовано к печати решением ученого совета Хмельницкого кооперативного торгово-экономического института, протокол № 5 от 21.04. 2015. С. 96.

Завгородный А. В.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

СРЕДСТВА ПРИВЛЕЧЕНИЯ И МОТИВАЦИИ СОТРУДНИКОВ В СОВРЕМЕННЫХ IT КОМПАНИЯХ ВО ВРЕМЯ ВЫНУЖДЕННОЙ УДАЛЕННОЙ РАБОТЫ

Средства привлечения и мотивации сотрудников в современных IT компаниях во время вынужденной удаленной работы включают несколько аспектов.

1. Техническая поддержка: чтобы обеспечить эффективную работу удаленных сотрудников, компании могут обеспечить им доступ к необходимому программному обеспечению и оборудованию, такому как ноутбуки, десктопы, мониторы и т.д. Кроме того, компании должны предоставлять должную техническую поддержку сотрудникам, которые могут столкнуться с проблемами в процессе удаленной работы.

Как бы не звучала печально текущая реальность, но в условиях войны в Украине, техническая поддержка сотрудников IT компаний стала особенно важной задачей. Многие компании приняли меры для обеспечения безопасности и надежности своих сотрудников, которые находились в зоне боевых действий, а также для поддержки работы компаний, которые находились в регионах с высоким уровнем напряженности.

Некоторые компании предоставляли своим сотрудникам специальные устройства и программное обеспечение, которые позволяли им работать удаленно и безопасно. Это включало в себя VPN-сервисы, устройства аутентификации с двухфакторной проверкой, защитные программы и многое другое.

Также некоторые IT-компании предоставляли своим сотрудникам мобильные телефоны с неограниченным доступом к Интернету и мобильными планами, чтобы обеспечить связь и доступ к необходимой информации в случае необходимости.

Кроме того, компании организовывали регулярные встречи с сотрудниками, которые находились в зоне боевых действий, и обеспечивали им психологическую поддержку. Некоторые компании также организовывали благотворительные акции и помощь пострадавшим от военных действий.

В целом, техническая поддержка сотрудников IT компаний во время войны в Украине была необходимой для обеспечения безопасности и надежности работы компаний. Многие компании проявили заботу и ответственность в отношении своих сотрудников и общества в целом.

2. Гибкий график работы: одной из главных привлекательных сторон работы в IT-компании является гибкий график работы. Компании могут продолжать обеспечивать эту гибкость, позволяя сотрудникам работать из дома в любое время, что может быть особенно важно в условиях вынужденной удаленной работы.

3. Обучение и развитие: мотивация сотрудников может быть увеличена, если компания предоставляет сотрудникам возможность профессионального обучения и развития навыков в области IT. Это может быть организовано как онлайн-курсы, вебинары, внутренние мероприятия и т.д.

4. Командообразование: компании должны стремиться сохранить сильный дух команды, несмотря на то, что сотрудники работают из разных мест.

Командообразование в IT компаниях во время вынужденной удаленной работы является важным аспектом для поддержания эффективной коммуникации и сотрудничества среди удаленных сотрудников.

Для создания чувства командной работы и укрепления связей между удаленными сотрудниками можно использовать следующие методы:

4.1 Регулярные онлайн-встречи: установите расписание для регулярных онлайн-встреч, которые будут проводиться сотрудниками, работающими удаленно. Это может быть ежедневное утреннее собрание, еженедельное обновление проекта или ежемесячная встреча команды. Встречи могут проводиться через видеоконференц-системы, такие как Zoom или Skype.

4.2 Использование чатов и форумов: создайте общие чаты и форумы для команды, чтобы обсуждать текущие задачи и другие важные вопросы. Это позволит сотрудникам быстро получать ответы на свои вопросы и поддерживать диалог друг с другом.

4.3 Организация онлайн-игр и конкурсов: проведение онлайн-игр и конкурсов может помочь создать командный дух и повысить мотивацию у сотрудников. Это могут быть, например, игры на скорость печати, викторины по техническим знаниям или кроссворды по теме проекта.

4.4 Совместное использование инструментов для работы: использование совместных инструментов для работы над проектами, таких как Trello или Asana, может упростить процесс командной работы и помочь сотрудникам лучше понимать, какие задачи выполняются другими членами команды.

4.5 Организация виртуальных встреч вне рабочего времени: иногда важно провести виртуальные встречи вне рабочего времени, чтобы сотрудники могли более неформально общаться друг с другом и укреплять связи между собой. Это может быть, например, виртуальная игра или вечеринка, проводимая через Zoom или другую платформу видеоконференций.

5. Поощрение: компании могут использовать различные виды поощрения, чтобы стимулировать высокую производительность

сотрудников. Это может быть бонусная система, возможность участия в конкурсах, подарки и т.д.

6. Социальные мероприятия: компании могут организовывать онлайн-мероприятия, чтобы укрепить чувство команды и социальную связь сотрудников. Это могут быть виртуальные вечеринки.

Например. Компания DataArt проводила IT talk events в условиях COVID-19 в формате онлайн-конференций. Вместо традиционных офлайн-мероприятий, таких как конференции, форумы и встречи, компания решила организовать онлайн-мероприятия, чтобы продолжить общение и обмен знаниями и опытом между экспертами и участниками.

Одним из таких мероприятий была онлайн-конференция "DataArt TechTalks", которая прошла в 2020 году. Это было совместное мероприятие, организованное DataArt и партнерами компании, где ведущие эксперты в области технологий делились своими знаниями и опытом с участниками.

Также компания проводила серию онлайн-встреч "DataArt Online Meetups", где участники могли общаться и обмениваться опытом с другими разработчиками, аналитиками и экспертами в области IT. В ходе этих встреч, которые проходили через платформы видеоконференций, участники могли узнать о новых технологиях, трендах в IT-отрасли и примерах лучших практик. Для обеспечения интерактивности и возможности задать вопросы экспертам, компания использовала специальные онлайн-инструменты, такие как чаты и форумы, где участники могли общаться с другими участниками и спикерами в режиме реального времени. В целом, компания DataArt успешно адаптировала свои мероприятия в условиях COVID-19, перенеся их в онлайн-формат, чтобы продолжить общение и обмен знаниями и опытом между экспертами и участниками.

Список использованных источников:

1. *How COVID Has Changed the Business Landscape https://www.dataart.com/blog/how-covid-has-changed-the-business-landscape (дата обращения 02.05.2023).*
2. *Исследование: корпоративный дух vs. Пандемия https://ucg.in.ua/issledovanie-korporativnyj-duh-vs-pandemiya/?fbclid=IwAR1G001mV9zJ_Ri5HgX5eu6PSTorNOCbGt3jOraEB_zaiJviC7ztnaCKJks (дата обращения 02.05.2023).*

Золотаренко А. О.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ЗНАЧЕННЯ ТА ВАЖЛИВІСТЬ ПОБУДОВИ ЕКОНОМІЧНОЇ МОДЕЛІ РОЗВИТКУ КОМПАНІЇ

У сучасному динамічному бізнес-середовищі, де конкуренція зростає і швидкість змін прискорюється, розуміння, прогнозування економічних аспектів та належне управління ними є вирішальними факторами успіху. Отже доцільно мати інструмент що може дати найбільш вечерпний аналіз та прогнозування майбутнього компанї, управління очікуваннями зацікавлених сторін, та валідації доцільності бізнесу або його частини в цільому. Для цього сучасні компанії використовють побудову економічної моделі.

Економічна модель – це аналітичний інструмент, який допомагає компанії розглядати свою діяльність з економічної перспективи. Вона враховує різні аспекти, такі як витрати, дохід, прибуток, ринкові умови, конкуренцію та стратегічні рішення, і дозволяє компанії отримати цінні інсайти та прогнози.

Побудова економічної моделі розвитку компанії має кілька ключових переваг. А саме, вона допомагає компанії розуміти рентабельність своєї діяльності, ідентифікувати області ефективності та витрат, планувати майбутні результати та ресурси, а також виявляти та управляти ризиками. Крім того, економічна модель є потужним інструментом комунікації зі зацікавленими сторонами.

Аспекти ефективності використання економічної моделі для розвитку компанії.

Економічна модель надає компанії систематичний підхід до аналізу своєї діяльності та управління економічними аспектами бізнесу. Переваг у побудові економічної моделі для компанії є багато, хотів би зупинитись на декількох основних нижче.

Розуміння рентабельності. Економічна модель допомагає компанії зрозуміти, які аспекти її діяльності є прибутковими і які можуть призводити до збитків. Вона дозволяє оцінити витрати, дохід, прибуток та маржі, що допомагає приймати рішення щодо оптимізації виробництва, управління витратами та ціноутворення.

Прогнозування та планування. Економічна модель допомагає компанії прогнозувати майбутні результати, враховуючи різні сценарії і вплив змінних факторів. Вона дозволяє планувати ресурси, інвестиції та стратегічні кроки на основі розуміння економічних наслідків.

Виявлення ризиків. Економічна модель допомагає ідентифікувати ризики, що впливають на компанію. Вона дозволяє аналізувати чинники, такі як зміни витрат, зміни в ринкових умовах, конкуренція тощо, і розробляти стратегії для зменшення ризиків та підвищення стійкості бізнесу.

Підтримка прийняття рішень. Економічна модель надає аналітичну основу для прийняття управлінських рішень. Вона допомагає оцінити альтернативи, провести економічний аналіз і вибрати найоптимальніші рішення для досягнень.

Оптимізація ресурсів. Економічна модель дозволяє компанії ефективно використовувати свої ресурси. Вона допомагає ідентифікувати області, де можна здійснити економії, покращити продуктивність і оптимізувати витрати. Це може включати оптимальне розподіл робочої сили, управління запасами, використання технологій та раціоналізацію процесів.

Моніторинг результатів. Економічна модель надає рамки для моніторингу результатів компанії і вимірювання її ефективності. Вона дозволяє порівнювати фактичні результати з прогнозами і цілями, ідентифікувати причини відхилень та вносити корективи в стратегію та тактику компанії.

Комунікація зі зацікавленими сторонами. Економічна модель надає компанії зрозумілий і об'єктивний спосіб комунікувати зі зацікавленими сторонами, такими як інвестори, банки, партнери та державні органи. Вона допомагає пояснити стратегію компанії, прогнози, фінансові показники та плани розвитку.

Артефакти економічної моделі розвитку компанії.

Для створення економічної моделі використовують рад заходів результатом яких є документально зафіксовані данні, що й слугують в подальшому як база від якої відштовхуються процесси направлені на аналіз, та досягнення цілей компанії. Основними артефактами економічної моделі є фінансові та операційні моделі, маркетингові плани, та плани щодо виробничих потужностей та персоналу. Далі роздивимось всі елемени детальніше.

Фінансові моделі. Це числові моделі, які використовуються для прогнозування фінансових показників компанії, таких як прибуток, витрати, потоки грошей та рентабельність. Іноді включають в себе юніт-економіку, що атрибуює всі фініінсові та маркетингові показники на одну одиницю продукції, сервісу, або клієнта компанії. Фінансові моделі допомагають розрахувати ризики, оцінити інвестиційну привабливість проектів та забезпечити фінансовий контроль.

Маркетингові плани. Це стратегічні документи, що описують підходи компанії до маркетингу і просування продуктів або послуг. Маркетингові плани містять аналіз ринку, цільову аудиторію, позиціонування продукту, стратегії ціноутворення та комунікації з клієнтами.

Операційні моделі. Це детальні описи процесів і операцій, що виконуються в компанії. Операційні моделі дозволяють управляти ресурсами, забезпечувати ефективність виробничих процесів та планувати ланцюжок постачання.

План щодо виробничих потужностей та персоналу. Це схеми та стратегчні документи що описують потреби компанії в робочій силі або виробничих потужностях, їх розвитку, підвищення кваліфікації та управлінню таланами.

Побудова економічної моделі для компанії.

Побудова економічної моделі для компанії це складний процес який включає багато факторів та подій. Розділимо його на декілька зрозумілих кроків:

1. Збір та аналіз даних. Почніть зі збору необхідних даних про фінансову та операційну діяльність компанії. Це можуть бути дані про витрати, доходи, обсяги продажів, ціни, ринкову інформацію тощо. Проведіть аналіз цих даних для виявлення ключових трендів та залежностей.
2. Визначення цілей та сценаріїв. Визначте основні цілі, які ви хочете досягти за допомогою економічної моделі. Наприклад, це може бути збільшення прибутку, оптимізація витрат, розширення ринків тощо. Розгляньте різні сценарії розвитку, включаючи оптимістичні, песимістичні та базові варіанти.
3. Вибір економічних моделей: Виберіть підходящі економічні моделі та методи, які відповідають особливостям вашої компанії та цілям. Наприклад, це можуть бути моделі прогнозування попиту, моделі ціноутворення, моделі оптимального розподілу ресурсів тощо. Врахуйте також наявність економічних програм та інструментів, які можуть підтримати ваш аналіз.
4. Розробка математичних моделей. Розробіть математичні моделі, які відображають взаємозв'язки між різними факторами в економічній системі компанії. Використовуйте статистичні методи, математичні рівняння та інші інструменти для моделювання і прогнозування результатів.
5. Валідація та калібрування моделі. Перевірте правильність та точність економічної моделі шляхом порівняння її результатів з фактичними даними. Виконайте калібрування моделі, вносячи коригування та уточнення, щоб підкреслити її адекватність та надійність.
6. Використання моделі для прийняття рішень. Використовуйте розроблену економічну модель для аналізу та прогнозування результатів в різних сценаріях. Враховуйте ризики та можливості, розробляйте стратегії та рекомендації для досягнення поставлених цілей компанії.

Важливо пам'ятати, що побудова економічної моделі - це ітеративний процес, який може вимагати коригування та оновлення з часом. Регулярно оцінюйте та оновлюйте модель, враховуючи зміни в економічному середовищі та стратегічні зміни в компанії.

Рекомендації щодо впровадження економічної моделі в компанії.

При впровадженні економічної моделі в компанію рекомендується враховувати наступні аспекти.

Залучення експертів. Запрошуйте кваліфікованих фахівців з економіки та фінансів, які мають досвід у побудові економічних моделей. Вони допоможуть визначити потрібні дані, вибрати відповідні методи та забезпечити правильність аналізу та прогнозування.

Збір та обробка даних. Переконайтеся, що ви маєте доступ до достовірних та повних даних про фінансову та операційну діяльність компанії. Запровадження ефективних систем збору та обробки даних допоможе забезпечити точність та актуальність моделі.

Адаптація до специфіки компанії. Забезпечте, щоб економічна модель враховувала унікальні аспекти вашої компанії, такі як особливості галузі, розмір компанії, типи товарів або послуг. При необхідності модифікуйте модель, щоб вона відповідала конкретним потребам та характеристикам вашої компанії.

Поступове впровадження та навчання персоналу. Впроваджуйте економічну модель поетапно, дозволяючи персоналу засвоїти нові концепції та інструменти. Організуйте навчальні семінари, тренінги та практичні заняття, щоб забезпечити правильне розуміння та використання моделі всіма зацікавленими сторонами.

Оцінка та оновлення. Регулярно оцінюйте ефективність та точність економічної моделі. Проводьте регулярні оновлення, враховуючи зміни в бізнес-середовищі, розширення компанії та стратегічні зміни. Забезпечте постійний моніторинг та аналіз результатів, щоб впевнитися, що модель відповідає поточним потребам та завданням компанії.

Впровадження економічної моделі в компанію - це процес, який вимагає зосередженості, планування та співпраці між різними відділами компанії. Дотримуючись цих рекомендацій, ви зможете створити потужний інструмент для прийняття обґрунтованих та ефективних рішень для розвитку вашої компанії.

Побудова економічної моделі розвитку компанії вимагає систематичного аналізу, збору та обробки даних, використання економічних теорій та методів. Вона вимагає залучення кваліфікованих фахівців з економіки та фінансів, які зможуть створити модель, відповідну специфіці компанії.

Таким чином, побудова економічної моделі розвитку компанії є необхідною умовою для досягнення успіху та стійкого розвитку. Вона допомагає компанії аналізувати, прогнозувати та оптимізувати свою діяльність, вирішувати складні завдання та приймати обґрунтовані рішення. Вона є своєрідним компасом, який дозволяє компанії орієнтуватися в непередбачуваних умовах і зберігати конкурентну перевагу.

Економічна модель розвитку компанії це інструмент, що надає компанії системний підхід до аналізу своєї діяльності, планування майбутнього та прийняття обґрунтованих рішень напралених на досягнення цілей бізнесу. Він може і повинен ставити компанію на більш вищий рівень економічного успіху, надаючи новий рівень відповідальності яка, в підсумку перетворюється на винагороду.

Список використаних джерел:

1. Solitaire Townsend, (2023). The Solutionists. How Businesses Can Fix the Future. C. 121-156

2. Tien-Anh Nguyen, (2011). www.openviewpartners.com. The Importance of Developing Your Company's Economic Model.

3. Sam Ouliaris, (2011). www.imf.org. What Are Economic Models? Vol. 48, No. 2

Кирилко І. В.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

УПРАВЛІННЯ ПІДПРИЄМСТВОМ НА ЗАСАДАХ МАРКЕТИНГУ

В сучасних умовах становлення ринкових відносин перспективний розвиток та ефективне функціонування підприємств неможливі без застосування сучасних управлінських концепцій. З огляду на існування різноманітних підходів до організації управління підприємством, Арустамов Е.А. із низки сучасних підходів відокремлює важливість процесного підходу, який базується на засадах взаємопов'язаних та безперервних функцій, що реалізуються для забезпечення розвитку і здійснення діяльності підприємств. Розглядаючи підхід застосування концепції управління якістю на підприємствах, слід зауважити, що результати, отримані в ході такого застосування, дозволяють не тільки підвищити якість виготовленої продукції та/чи послуг, але і провести загальний моніторинг діяльності підприємств із визначенням відповідності такої діяльності до міжнародних стандартів ISO.

В основі функціонального підходу має лежати функціональна спеціалізація, завдяки якій забезпечуватиметься здійснення найнижчих витрат з поміж можливих для виконання бізнес процесів. Інтеграційна концепція менеджменту підприємства дозволить не тільки визначати перспективні шляхи підвищення ефективності діяльності підприємств, але і пристосовувати підприємства до впливу змін та умов невизначеності середовища функціонування. Що стосується досвіду застосування концепцій менеджменту зарубіжними підприємствами, то згідно з інформацією, поданою Казущик А.А., досить ефективними є: концепція ощадливого виробництва, концепція реінжинірингу бізнес процесів, концепція бенчмаркінгу, концепція управління ефективністю бізнесу, концепція збалансованої системи показників (індикаторів).

Якщо говорити про вітчизняні підприємства, то на сьогодні в Україні ефективно застосовуються підприємствами концепція управління ефективністю бізнесу та концепція збалансованої системи показників (індикаторів). У ході розкриття специфіки застосування сучасних концепцій менеджменту на підприємствах, слід зауважити, що зараз підприємствами досить активно використовується модель управління діяльністю, побудована на засадах тайм менеджменту. Відповідно до інформації, поданої Дурович А.П., основу ризик менеджменту становлять такі компоненти: стратегічне управління, впровадження управлінських рішень, моніторинг і аналіз, покращення бізнес процесів.

Дослідження також показують, що компанії часто впроваджують концепцію гнучкого менеджменту, оскільки сьогодні їх діяльність відбувається в умовах діджиталізації та швидкого розвитку техніки та технологій. Впровадження бренд менеджменту сприяє успішній реалізації цінової, збутової, товарної та комунікативної політик підприємств, в результаті чого досягаються як тактичні, так і стратегічні цілі діяльності підприємств, які передбачені метою їх функціонування. Застосування концепції реінжинірингу бізнес процесів підприємства сприятиме відходу від неефективних та застарілих правил і процедур ведення бізнесу до більш нових, інноваційних. Сьогодні існує міцний взаємозв'язок підприємств та вищих навчальних закладів, які здійснюють підготовку майбутніх менеджерів.

Огляд видів та специфіки сучасних концепцій менеджменту, які застосовуються на підприємствах, дозволяє їх узагальнити в єдину цілісну систему управління діяльністю підприємств. За результатами представлення концептуальних основ формування та розвитку сучасних управлінських концепцій та їх застосування на підприємствах встановлено, що сьогодні підприємства активно використовують такі концепції управління, як концепція управління процесами, концепція управління цілями, концепція контролінгу, концепція управління якістю, проектно-орієнтована концепція, управління командою, концепція реінжинірингу бізнес-процесів, концепція знань, концепція логістики, концепція ресурсів, концепція управління якістю, концепція фінансового управління, концепція управління кайдзен, концепція повного контролю, концепція порівняльного аналізу, концепція технології LEAN, концепція збалансованої системи показників, гнучка концепція управління часом, ризик концепція управління, концепція управління брендом.

Маркетинговий менеджмент (анг. marketing management) – це процес, основними складовими якого є аналіз, прогнозування, реалізація планів та контроль за здійсненням заходів, спрямованих на встановлення, зміщення і підтримання взаємовигідних обмінів з цільовими ринками для досягнення цілей підприємства. Оскільки маркетингове управління реалізується через виконання певних функцій, маркетинговий менеджмент розглядають як управління всіма функціями підприємства. Управління маркетингом як управління бізнесом полягає в тому, що підприємства розглядаються як відкрита система. Для цього потрібна зміна мислення. Підхід до маркетингового менеджменту як управління функціями полягає у забезпеченні тісних зв'язків на ринку через виконання різних функцій фірми: маркетингу, постачання, інновацій, виробництва, фінансів та інших.

У своєму становленні маркетинговий менеджмент пройшов ряд етапів. На думку П. Друккера маркетинг вперше з'явився у Японії в 1650 році. Це перший етап маркетингового менеджменту і його можна назвати початковим, локальним і зразковим. Другий етап маркетингового менеджменту

пов’язаний з виходом маркетингу і маркетингового менеджменту за національні межі. На цьому етапі було необхідно створити на підприємствах маркетингові організаційні структури управління. Третім етапом є етап сучасного ефективного маркетингового менеджменту, який ґрунтується на філософії холістичного (цілісного) маркетингу.

Його основу складають:

1. Інтегрований маркетинг. Відповідно до нього, перед суб’єктами маркетингового менеджменту стоїть завдання розробки маркетингових заходів, які б були інтегровані в маркетингову програму;

2. Внутрішній маркетинг. Він полягає в забезпеченні діяльності кожного співробітника компанії, включаючи і вище керівництво, на маркетингових принципах;

3. Маркетинг партнерських відносин. Він має на меті встановити довготривалі сприятливі стосунки між основними ринковими партнерами;

4. Соціально-відповідальний маркетинг. Він вимагає врахування при здійсненні маркетингового менеджменту не тільки інтересів виробника і споживача товарів, але й соціального, етичного, екологічного та правового характеру здійснюваних маркетингових заходів.

Багато концепцій і моделей, розроблених вітчизняними та зарубіжними маркетологами, сьогодні зазвичай вже не актуальні. В таких умовах виникають не досить адаптовані маркетингові концепції на кшталт «латерального маркетингу» і «маркетингу відчуттів», а підприємства, керуючись в основному інтуїцією, лише експериментують, намагаючись методом спроб і помилок віднайти своє місце на ринку. Зі збільшенням глибини та широти асортименту продукції та зростанням конкуренції успіх чи невдача бренду залежить від багатьох факторів, включаючи випадкові, які майже не контролюються продавцем. Варто зазначити, що звичайний ринок товарів і послуг існує насправді скоріш віртуально, для аналізу, а ніж реально, де потенційні споживачі приймають рішення про купівлю, виходячи з потреб, обмежених рівнем платоспроможності.

Ефективне впровадження та використання маркетинг-менеджменту компанії вимагає перш за все чіткого розуміння сутності та змісту маркетингового менеджменту, а також цілей його застосування, функцій та етапів його формування. Маркетинг в умовах ринкової економіки є засобом підвищення ефективності системи управління, методології функціонування ринку, що визначає стратегічні та тактичні цілі фірми в умовах ринкової конкуренції. Багато науковців користуються визначення менеджменту, що зазначений у тлумачному Оксфордському словнику англійської мови, де це поняття характеризується як: спосіб, манера спілкування з людьми; особливого роду вміння й адміністративні навички; влада й мистецтво управління; орган управління, адміністративна одиниця.

Маркетинг-менеджмент – це управлінська діяльність, пов’язана з плануванням, організацією, координацією, контролем, аудитом і

стимулюванням заходів по інтенсифікації процесу формування і відтворення попиту на товари і послуги, збільшення прибутку. Згідно з визначенням і загальними поняттями функцій менеджменту до основних функцій маркетинг-менеджменту належать: аналіз ринку, планування, організація, мотивація, контроль і аналіз виконання маркетингових планів. Цілі маркетинг-менеджменту визначають і формують на основі загальних цілей фірми, і насамперед її місії. Орієнтуючись на місію, можна визначити цілі маркетинг-менеджменту в загальній системі цілей менеджменту фірми.

З позиції маркетинг-менеджменту перелік цілей можна доповнити такими, як завоювання нових ринків, підвищення конкурентоспроможності фірми та її товарів, успішне впровадження нових товарів, поліпшення обслуговування споживачів, підвищення ефективності, тощо. Маркетинг-менеджмент є цілеспрямованою діяльністю, що пов’язана з процесом забезпечення стійких конкурентних переваг підприємства на ринку, що включає такі стадії, як аналіз зовнішнього середовища, ситуаційний аналіз, прогноз ринку і можливостей організації, розробка цілей і стратегій поведінки на ринку, планування маркетингових цілей і тактики поведінки організації в конкретній ситуації, розробка плану «маркетинг-мікс», організація, управління, контроль за реалізацією маркетингових заходів і оцінку результатів маркетингової діяльності.

У функціональному значенні маркетинг-менеджмент розглядається як діяльність або процес формування, організації будь-якого рішення, а потім його здійснення. В якості інструментарію розробки стратегії і тактики маркетинг- менеджменту виступають комплекс «маркетинг-мікс» і методи мотивації всіх суб’єктів, що входять до системи маркетинг-менеджменту. Підводячи підсумок вищесказаного, слід зазначити, що маркетинговий менеджмент відіграє ключову роль у господарській діяльності підприємства. Маркетинговий підхід до прийняття управлінських рішень дозволяє розробити цілі, стратегії, тактику діяльності підприємства на ринку та його товарну, цінову, збутову, комунікативну стратегії. Використання маркетингового менеджменту дозволяє компаніям краще адаптуватися до змін внутрішнього та зовнішнього середовища та забезпечити стратегічний розвиток підприємства.

Список використаних джерел:

1. Абчук В. О. Аналіз комерційної діяльності організацій: навчальний посібник / В. О. Абчук. // Москва: Інфра-М. – 2014. – С. 320.

2. Арустамов Е. А. Організація підприємницької діяльності / Е. А. Арустамов, Р. С. Андрєєва. // Москва: Ексмо. – 2014. – С. 36.

3. Афанасьєва О. П. Інтернет-маркетинг: Опорний конспект лекцій / О. П. Афанасьєва. // . Харків, Харківський державний університет харчування і торгівлі. – 2019. – С. 42.

Коваленко В. В.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

РОЛЬ ИННОВАЦИОННЫХ МЕТОДОВ АНАЛИЗА В ПОВЫШЕНИИ КОНКУРЕНТОСПОСОБНОСТИ IT-КОМПАНИЙ

IT-индустрия является одной из самых динамично развивающихся отраслей в современном мире. С постоянными технологическими изменениями и растущей конкуренцией IT-компании должны стремиться не только к созданию инновационных продуктов и услуг, но и к разработке эффективных стратегий для их монетизации и удовлетворения потребностей клиентов. В этом контексте роль инновационных методов анализа становится критической для повышения конкурентоспособности IT-компаний. Рассмотрим, какие инновационные методы анализа существуют и как они могут быть применены для достижения успеха в IT-индустрии.

Инновационные методы анализа рынка:

а) Исследование рынка и анализ трендов: Систематическое исследование рынка и анализ трендов помогает IT-компаниям понять существующую конкуренцию, определить потребности клиентов и предугадать будущие изменения на рынке. Использование инновационных методов, таких как машинное обучение и анализ больших данных, позволяет обрабатывать большие объемы информации и выявлять скрытые паттерны, что обеспечивает компаниям конкурентное преимущество.

б) Анализ пользовательского опыта: Оценка пользовательского опыта становится все более важной для IT-компаний. Инновационные методы, такие как анализ эмоций и сенсорные технологии, позволяют оценить удовлетворенность пользователей, выявить их потребности и предоставить рекомендации для улучшения продуктов и услуг.

Инновационные методы анализа конкурентов:

а) Анализ конкурентов и их стратегий: С помощью инновационных методов анализа IT-компании могут изучать деятельность своих конкурентов, выявлять их сильные и слабые стороны, анализировать их стратегии и предугадывать их будущие шаги. Это позволяет IT-компаниям принимать обоснованные решения и разрабатывать конкурентные стратегии, учитывая действия конкурентов.

б) Мониторинг изменений в отрасли: Инновационные методы анализа также помогают IT-компаниям отслеживать изменения в отрасли, включая появление новых технологий, изменения в регулировании и требованиях рынка. Анализ данных и использование автоматизированных инструментов позволяют компаниям оперативно реагировать на изменения и адаптироваться к ним, что способствует их конкурентоспособности.

Инновационные методы анализа внутренних процессов:

а) Анализ эффективности производства и разработки: IT-компании могут применять инновационные методы анализа для измерения эффективности своих производственных и разработческих процессов. Использование данных и аналитических инструментов позволяет выявить слабые места, оптимизировать процессы и повысить производительность, что способствует улучшению конкурентоспособности компании.

б) Анализ данных и прогнозирование: Использование инновационных методов анализа данных, таких как машинное обучение и искусственный интеллект, позволяет IT-компаниям анализировать большие объемы информации, выявлять закономерности и прогнозировать будущие тренды. Это помогает компаниям принимать обоснованные решения и прогнозировать потребности рынка, что способствует их конкурентоспособности.

Инновационные методы анализа играют важную роль в повышении конкурентоспособности IT-компаний. Они позволяют компаниям получать ценную информацию о рынке, пользовательском опыте, конкурентах и внутренних процессах. Анализ данных и применение современных технологий позволяют выявлять паттерны, прогнозировать тренды и принимать обоснованные решения. Это помогает IT-компаниям разрабатывать конкурентные стратегии, улучшать продукты и услуги, оптимизировать производственные процессы и адаптироваться к изменениям в отрасли.

Одним из основных преимуществ инновационных методов анализа является их способность обрабатывать и анализировать большие объемы данных, что ранее было невозможно. С использованием современных инструментов и технологий, таких как машинное обучение, анализ больших данных, нейронные сети и алгоритмы прогнозирования, IT-компании могут получить ценные инсайты и предсказания, которые помогут им принимать более обоснованные и эффективные решения.

Однако, необходимо отметить, что успешное применение инновационных методов анализа требует не только наличия технических средств, но и компетентности и аналитической культуры внутри компании. Важно, чтобы IT-компании инвестировали в обучение своих сотрудников, развитие аналитических навыков и умений работы с инновационными инструментами.

В заключение, роль инновационных методов анализа в повышении конкурентоспособности IT-компаний нельзя недооценивать. Эти методы позволяют компаниям получать ценные данные, выявлять тенденции и предсказывать тренды, анализировать конкурентов и оптимизировать внутренние процессы. Они являются неотъемлемой частью стратегического планирования и принятия решений в сфере IT и способствуют успеху и росту компаний в современном конкурентном окружении.

Список использованных источников:

1. Akis, E. (2015). Innovation and competitive power. Procedia - Social and Behavioral Sciences

2. Beltyukov, Y., & Tkachuk, T. (2020). Teoretichni osnovy formuvannya strategiji innovacijnogo rozvytku promyslovogo pidpriemstva [Theoretical bases of formation of strategy of innovative development of the industrial enterprise]. Bulletin of Khmelnytsky National University Series: Economic Sciences

3. Bischi, G. I., Lamantia, F., & Sbragia, L. (2004). Competition and cooperation in natural resources exploitation: an evolutionary game approach. Game practice and the Environment,

4. Byczkowska, M., Poplavska, Z., Komarynets, S., Stukalina, Y., Majzel, A., & Zięba, K. (2020). Entrepreneurship today: Selected aspects. https://mostwiedzy.pl/pl/publication/entrepreneurship-today-selectedaspects,154353-1

5. Afuah, A. (1998). Innovation Management: Strategies: Implementation and Profits, Oxford University Press, New York, NY.

6. Александров А. Ф. (2015) Цифровые методы анализа будущего

Ковтуненко С. В.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ПРЕДУПРЕЖДЕНИЕ ЭМОЦИОНАЛЬНОГО ВЫГОРАНИЯ В УПРАВЛЕНИИ МОТИВАЦИЕЙ ПЕРСОНАЛА

Ценность и значимость человеческого капитала растет с каждым годом, поэтому для бизнеса одним из решающим факторов успеха является качество этого ресурса. В условиях экономической глобализации и вызовов современного мира актуальными и востребованными являются качественные знания, навыки, креативность, вовлеченность и предпринимательские способности сотрудников, которые рассматриваются как основные ресурсы для улучшения эффективности и конкурентных преимуществ бизнеса.

Вместе с тем, с глобализацией бизнес-процессов серьёзной проблемой современного общества является эмоциональное выгорание персонала компаний, влекущее за собой снижение мотивации, эффективности работы и, как следствие, ухудшение конечного результата ведения бизнеса.

Сложная и без того социально – экономическая ситуация в стране усугубилась полномасштабным вторжением России в Украину, что крайне негативно отразилось на психоэмоциональном состоянии населения Украины. Релокация коснулась многих компаний, которые вынуждены были принимать незамедлительные решения для спасения своего бизнеса и сохранения рабочих мест, многие другие, к сожалению, просто лишились рабочих мест.

Стрессовая ситуация в стране, на рабочем месте, взятие на себя большой ответственности приводит к тому, что рано или поздно человек сталкивается с эмоциональным истощением или выгоранием. Именно тогда он испытывает безразличие к своей работе, близким, да и к жизни в целом.

Понятие «Синдром эмоционального выгорания» введенное американским психиатром Гербертом Фрайденбергером в 1974 году, характеризуется, проявляющимся и нарастающим эмоциональным истощением, разочарованием и деморализацией [3].

Согласно исследованию Международного аналитического центра «HeadHunter Украина», в котором приняли участие 857 респондентов из разных регионов Украины, считают, что в ТОП-5 профессий, представители которых больше всех рискуют пережить состояние эмоционального выгорания, по сравнению с другими, входят учителя, медики, банкиры, социальные работники и продавцы, т.е. те, кто особенно тесно задействованы в коммуникативном процессе в процессе своей работы (рис.1) [5].

Рис. 1. Профессии, подверженные эмоциональному выгоранию (данные аналитического центра «HeadHunter Украина»)

Всемирная организация здравоохранения сообщила, что «Эмоциональное выгорание» включено в 11-й пересмотр Международной классификации болезней (ICD-11) как профессиональное явление и не классифицировано как болезнь». В ICD-11 эмоциональное выгорание определяется как синдром, возникающий из-за хронического стресса на работе, с которым человек не может справиться и характеризуется тремя показателями: ощущением потери энергии и истощением, психологической отстраненностью от работы, чувством негативизма или цинизма к своей работе, а также уменьшенной профессиональной эффективностью [6].

Из вышесказанного можно увидеть, что эмоциональное выгорание относится именно к профессиональной деятельности или работе и не может применяться к другим сферам жизни для характеристик и описаний пережитого опыта, поэтому и стоит рассматривать эффективную мотивацию персонала путем предотвращения от эмоционального выгорания на рабочем месте.

В формировании психологического комфорта в профессиональной деятельности ключевую роль играет социально – психологический климат в коллективе, который определяется частотой стрессовых и конфликтных ситуаций, правильностью принятия управленческих решений, коммуникативным процессом. Наличие неблагоприятных факторов может вызывать психологические перегрузки у сотрудников, стрессовые ситуации и, следовательно истощение нервной системы с последующим эмоциональным выгоранием, а ведь именно эмоциональная составляющая, является одной из главных критериев мотивационного процесса, который выводит сотрудника на новые высоты карьеры, дает мощный призыв к саморазвитию и самодисциплине, повышению ключевых показателей

эффективности и, в конечном счете, к повышению результатов финансово - хозяйственной деятельности самой бизнес структуры.

Причинами профессионального выгорания не всегда являются переработки, достаточно важным фактором может быть неудовлетворение от проделанной работы и не менее важной составляющей умение самого сотрудника вовремя переключаться с работы на отдых, а именно на качественную составляющую этого отдыха.

Пожалуй, одними из самых изматывающих и тревожных состояний являются конфликтные ситуации, психологическое давление, токсичное руководство и жесткие дедлайны работы, которые создают напряжение.

Причинами выгорания может быть обесценивание персонала и, как следствие, ощущение бесполезности, не понимания цели и конечного результата работы сотрудником. Несправедливое отношение с лишением бонуса или премии в виде наказания, накладывании штрафных санкций и отсутствие коммуникативных процессов между сторонами для предоставления обратной связи и адекватной оценки работы, все это триггеры, которые зарождают в сотруднике стресс, нежелание работать, усталость, апатию и в дальнейшем полное выгорание.

Если взглянуть на термин «выгорание», то можно сказать, что он от слова «гореть» и это не удивительно, поскольку, как правило, выгоранию наиболее подвержены сотрудники, которые «горят» или «загораются» идеей работы, проекта. Они настолько увлекаются своим делом и работают на полную мощь, не контролируя время, отведенное для работы и отдыха. По мере усложнения задач и увеличения трудовой нагрузки в режиме нон-стоп, с нехваткой ресурсов сотрудник приближается к стрессовой ситуации и здесь начинается начальная стадия эмоционального выгорания.

На следующем этапе у сотрудника формируется стойкая усталость, тревожность, нехватка сил, проблемы со сном, депрессия, часто нарушения пищевого поведения. Затем может наступать стадия психофизического истощения, с проявлением раздражительности и агрессивности, ухудшением памяти и концентрации внимания.

И, наконец, наступает финальная стадия, а именно - эмоциональное выгорание, когда у сотрудника снижается продуктивность, он становится безразличным к работе, возникают трудности в общении с коллегами, апатия ко всему, могут развиваться хронические болезни и ухудшаться качество жизни.

В научной литературе можно встретить несколько моделей эмоционального выгорания, которые достаточно схожи между собой. Рассмотрим некоторые из них, а именно модель Д. Гринбергера, которая наиболее полно описывает этапы эмоционального выгорания, модели К. Маслач и В. Бойко (табл.1) [1, 2, 4].

Модель Д.Гринберга	Модель К. Маслач	Модель В. Бойко
1.Этап «Медовый месяц» - сотрудник с удовольствием берется за работу, но по мере возрастания нагрузки, теряет интерес к профессиональной деятельности	1. Этап – идеализм и чрезмерное требование к себе. Несоответствии между ожиданиями от работы и действительностью	1.Этап – Напряжение. Ощущение эмоционального напряжения, усталость
2.Этап «Недостаток топлива» - у сотрудника появляется усталость, отрешенность, нарушение сна, опоздания на работу	2. Этап – эмоциональное и психическое истощение. Физическое и эмоциональное утомление и, как следствие истощение ресурсов организма.	2.Этап – Резистенция. Выносливость психики и адаптационные возможности личности
3.Этап «Хронические симптомы» - у сотрудника наблюдается агрессия, раздражительность, проблемы в коммуникациях, нарушения памяти	3. Этап – дегуманизация, как способ защиты. Проявление со стороны сотрудника цинизма, бездушности к окружающим и негативизма	3.Этап – Истощение. Неудовлетворенность собой, состояние интеллектуального и эмоционального ступора, состояние неудовлетворения работой, тревога и депрессия
4.Этап «Кризис» - у сотрудника могут развиваться хронические болезни, теряется трудоспособность, снижается самооценка	4. Этап – синдром отвращения к себе, к другим, ко всему миру. Преуменьшение собственного достоинства, обесценивание собственных достижений	
5.Этап «Пробивание стены» - опасность обострения физических и психологических проблем, угрожающих здоровью и жизни человека		

Таблица 1. Этапы эмоционального выгорания (обобщено автором)

Предупредительные или профилактические меры по предотвращению эмоционального выгорания должны проводиться как на личном уровне, где каждый сотрудник в зависимости от собственной осознанности может принимать меры по избеганию проблемы, так и организационном уровне, что, собственно, и является главным вопросом данной темы исследования.

При правильно выбранных инструментах воздействия, мотивации и стимулировании работы персонала, риск демотивации, а значит и эмоционального выгорания минимален. Не существует универсальных систем мотивации, так как в различных средах, при различных условиях и группах персонала, каждый инструмент будет иметь абсолютно разную эффективность и результативность.

Первостепенной задачей менеджера является создание комфортных условий для работы в коллективе, здоровой атмосферы для повышения производительности труда, а также необходимого уровня материального дохода, но кроме того, для формирования и поддержания у персонала необходимого уровня активности и избегания ситуаций, провоцирующих эмоциональное выгорание, требуется определённая система мотивации и стимулирования труда, а также четкая постановка задач и целей для персонала, которая сводит к минимумам факторы неопределенности, возникающей из-за этого тревожности, а значит и возможность возникновения стресса.

Налаживание рабочих конфликтов посредством проведения специализированных тренингов, тимбилдингов, которые укрепляют командную работу, семинаров, фокус групп, сессий с психологами, которые, кроме этого, могут обучать персонал работе с эмоциями, тревогой и стрессом, что в будущем поможет минимизировать выгорание сотрудника.

Кроме того, повысить уровень мотивации персонала возможно системой не только материальных, но и нематериальных поощрений, в виде похвалы и признания за результаты достижений, бонуса в виде дополнительного обучения, стажировки, дополнительных выходных дней, карьерного роста, поздравление со значимыми датами и другие системы и методы мотивации и стимулирования труда.

Подводя итоги отметим, что от уровня мотивации зависит качество работы сотрудников, их производительность и эффективность, что в результате оказывает прямое влияет на конечный результат бизнеса. Постоянно растущее количество публикаций по проблеме эмоционального выгорания говорит о том, что проблема современного общества актуальна и растет с геометрической прогрессией, а анализ научной литературы о том, что эта тема недостаточно разработана с точки зрения научного интереса.

Список использованных источников:

1. Бойко В. В. Энергия эмоций в общении: взгляд на себя и на других – М: Информационно-издательский дом "Филинъ", 1996. – 472 с.

2. Гринберг Д. Управление стрессом. — СПб.: Питер, 2002. – 238 с.

3. Freudenberger H. J. Staff burnout // J. of Social Issues. 1974. Vol. 30. P. 159–165.

4. Maslach C. A. Multidimentional Theory of Burnout // Theories of Organizational Stress. Oxford, 1994. P. 68–85.

5. Эмоциональное выгорание: какие профессии под прицелом – опрос [Электронный ресурс] – Режим доступа: https://news.liga.net/society/news/emotsionalnoe_ vygoranie_kakie_professii_pod_pritselom_opros

6. Выгорание как «профессиональный феномен»: Международная классификация болезней [Электронный ресурс] – Режим доступа:https://www.who.int/news/item/28-05-2019-burn-out-an-occupational-phenomenon-international-classification-of-diseases

Лупаненко А. Ю.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

МОДЕЛИРОВАНИЕ И СИМУЛЯЦИИ В ОПЕРАЦИОННОМ МЕНЕДЖМЕНТЕ

В данной научной статье исследуется применение моделирования и симуляций в операционном менеджменте. Операционный менеджмент играет ключевую роль в эффективном функционировании организаций, и использование моделей и симуляций является важным инструментом для анализа, оптимизации и принятия решений в операционных процессах. В статье рассматриваются принципы моделирования, основные типы моделей и методы симуляции, а также примеры их применения в операционном менеджменте для анализа процессов, оптимизации ресурсов и прогнозирования результатов.

Операционный менеджмент включает в себя управление операционными процессами в организации с целью достижения эффективности и высокого качества продукции или услуг. Моделирование и симуляции предоставляют возможность создания абстрактных моделей операционных систем и процессов, чтобы анализировать их работу, оптимизировать ресурсы и прогнозировать результаты различных решений.

Принципы моделирования.

Моделирование в операционном менеджменте основано на определенных принципах [1,2].

Абстрагирование. Принцип абстрагирования заключается в упрощении модели путем выбора наиболее значимых и релевантных аспектов реальной системы. Это позволяет сфокусироваться на ключевых элементах и связях между ними, что облегчает анализ и понимание системы.

Формализация. Формализация представляет систему в виде математических уравнений, структурных моделей или алгоритмов. Она позволяет конкретизировать и описать взаимодействия и свойства системы в формальном виде, что обеспечивает ясность и позволяет проводить анализ и эксперименты.

Проверяемость. Модель должна быть проверяемой, что означает, что ее результаты и прогнозы должны соответствовать реальности. Проверяемость достигается путем сравнения результатов моделирования с данными из реальных наблюдений или экспериментов. Если модель соответствует данным, то она считается достоверной и может использоваться для принятия решений.

Гибкость. Модель должна быть гибкой и способной адаптироваться к изменениям в системе или условиях. Она должна позволять изменять

входные параметры, структуру модели и алгоритмы, чтобы анализировать различные сценарии и варианты решений. Гибкость моделирования позволяет оценить эффект различных стратегий и принять наилучшее решение в изменяющихся условиях.

Ограничения и предположения. Моделирование в операционном менеджменте должно учитывать ограничения и предположения, связанные с реальной системой. Это может включать ограничения по ресурсам, времени, стоимости, а также предположения о поведении и взаимодействии элементов системы. Учет этих ограничений и предположений позволяет создать реалистичную модель, которая будет полезна для анализа и принятия решений.

Одним из ключевых принципов я хочу выделить абстрагирование, то есть упрощение и учет только наиболее значимых аспектов реальной системы. Другим важным принципом является формализация, то есть представление системы в виде математических уравнений, структурных моделей или алгоритмов. Кроме того, моделирование должно быть проверяемым и гибким, чтобы позволять анализировать различные сценарии и варианты решений.

Типы моделей в операционном менеджменте.

Существует несколько типов моделей, используемых в операционном менеджменте. Статические модели предназначены для анализа структуры системы и связей между ее компонентами. Динамические модели описывают изменение системы со временем и позволяют проводить прогнозирование и анализ долгосрочных эффектов. Статистические модели используют статистические методы и данные для анализа и прогнозирования операционных процессов. Эконометрические модели применяются для изучения взаимосвязи между экономическими переменными и операционными показателями. Оптимизационные модели используются для определения оптимальных решений, учитывая ограничения и целевые функции.

Методы симуляции в операционном менеджменте.

Симуляция является мощным инструментом, который позволяет воссоздать работу операционных систем и процессов в виртуальной среде. Она позволяет проводить эксперименты с различными вариантами решений и анализировать их эффект на производительность, качество и другие ключевые показатели. Примерами методов симуляции являются дискретно-событийное моделирование, системная динамика и агентное моделирование.

Примеры применения моделирования и симуляций.

В данной части статьи рассматриваются конкретные примеры применения моделирования и симуляций в операционном менеджменте. Приводятся примеры моделирования и оптимизации производственных процессов, управления запасами, планирования проектов и прогнозирования спроса. Также обсуждаются случаи использования симуляции для анализа

пропускной способности систем, управления качеством и оптимизации планирования ресурсов [3].

Преимущества и ограничения моделирования и симуляций в операционном менеджменте.

В заключительной части статьи рассматриваются преимущества и ограничения использования моделирования и симуляций в операционном менеджменте. Указывается на их способность предоставлять качественные прогнозы, улучшать планирование и принятие решений, а также на возможность проводить виртуальные эксперименты. Однако также отмечаются ограничения, связанные с точностью моделей, необходимостью достоверных данных и сложностью разработки и поддержки моделей.

Применение моделей позволяет лучше понять систему, предсказать результаты различных стратегий и улучшить производительность и эффективность операционных процессов. Симуляции, в свою очередь, предоставляют возможность проводить виртуальные эксперименты и оценивать эффект различных переменных на результаты операций.

Однако, следует отметить некоторые ограничения моделирования и симуляций. Во-первых, точность моделей зависит от доступности достоверных данных и правильной интерпретации входных параметров. Во-вторых, разработка и поддержка моделей требуют определенных знаний и навыков, а также времени и ресурсов. Наконец, моделирование не может полностью учесть все аспекты реальной системы, и поэтому результаты моделирования могут иметь ограниченную применимость в реальном мире.

Список использованных источников

1. Banks, J., Carson, J. S., Nelson, B. L., & Nicol, D. M. (2005). Discrete-event system simulation. Pearson Prentice Hall.

2. Slack, N., Brandon-Jones, A., & Johnston, R. (2019). Operations Management. Pearson Education Limited.

3. Sterman, J. D. (2000). Business dynamics: systems thinking and modeling for a complex world. Irwin/McGraw-Hill.

Луцків Т. Р.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ВИБІР МАРКЕТИНГОВИХ КОНТАКТІВ З ЦІЛЬОВОЮ АУДИТОРІЄЮ В ПОБУДОВІ ЕФЕКТИВНИХ РЕКЛАМНИХ КАМПАНІЙ

Стратегічна діяльність, спрямована на задоволення потреб і бажань клієнтів через створення, просування і постійну підтримку обміну цінностями є маркетингом і цей напрям є надзвичайно важливим у сучасному бізнес-середовищі оскільки він відповідає за:

а) залучення клієнтів - маркетинг допомагає звернути увагу потенційних клієнтів до вашої компанії, продуктів або послуг, він допомагає побудувати знання про ваш бренд і відокремити вашу пропозицію серед конкурентного оточення;

б) збільшення продажів - ефективні маркетингові стратегії допомагають збільшити обсяг продажів, вони дозволяють залучати та зберігати клієнтів, збільшувати середній чек і стимулювати повторні покупки;

в) розвиток бренду - маркетинг допомагає побудувати та розвинути сильний бренд, він дозволяє передати цінності, ідеї й унікальність компанії своїм клієнтам, а сильний бренд допомагає залучати й утримувати лояльних клієнтів;

г) дослідження ринку - маркетингові дослідження дозволяють зрозуміти свою цільову аудиторію, їхні потреби, а це надає цінну інформацію для розробки продуктів або послуг, які відповідають потребам ринку;

ґ) конкурентну перевагу - ефективний маркетинг допомагає вирізнятись серед суперників й отримати перевагу, дозволяє визначити свою унікальність і сприяє розробці стратегій, які дозволяють зайняти сильну позицію на ринку…

Передача повідомлення цільовій аудиторії, які розкривають маркетингові ініціативи здійснюється за допомогою рекламних кампаній. Наведемо декілька основних способів встановлення контакту з аудиторією для акцентування її уваги до продукту або послуги:

а) використання прямих рекламних каналів, таких як телебачення, радіо, преса, інтернет, соціальні медіа й зовнішня реклама;

б) відправлення персоналізованих листів або брошур безпосередньо до потенційних клієнтів;

в) встановлення контакту з потенційними клієнтами за допомогою телефонних дзвінків для презентації продукту або послуги;

г) відправлення розсилок електронних листів або інформаційних бюлетенів, щоб тримати аудиторію в курсі новин, пропозицій або акцій;

ґ) використання платформ соціальних медіа, таких як Facebook, Instagram, Twitter і LinkedIn, для публікації цікавого та корисного контенту безпосередньо та за допомогою блогерів;

д) створення веб-сайту з інформацією про продукт чи послуги, контактні дані та можливість взаємодії з аудиторією через форми зворотного зв'язку або чат-боти;

е) організація або участь у тематичних конференціях, виставках, семінарах або вебінарах, де можна зустріти цільову аудиторію яка безпосередньо буде споживати чи розповсюджувати вашу продукцію, чи послугу.

Звісно існують й інші контакти які відрізняються від аудиторії споживачів до аудиторії та від категорії продукту/послуги до категорії. Надзвичайно важливо мати можливість відстежувати результати й ефективність маркетингових зусиль які передаються повідомленнями. Кожне повідомлення здійснює певний вплив на аудиторію та результати рекламних кампаній та відповідно маркетингових ініціатив. За допомогою аналітики та метрик можна виміряти вплив рекламних кампаній на продажі, знання про бренд, залучення клієнтів та інші ключові показники. Враховуючи ці фактори, реклама виступає важливим елементом стратегії маркетингу, допомагаючи компаніям досягати своїх цілей і сприяючи успішному розвитку бізнесу.

Вимірювання маркетингових інвестицій є важливим процесом для оцінки ефективності маркетингових зусиль і прийняття обґрунтованих рішень щодо розподілу бюджету. Існує ряд ключових метрик та підходів для вимірювання маркетингових інвестицій. Для прикладу декілька з них: ROI (Return on Investment) - співвідношення прибутку до витрат; ROMI (Return on Marketing Investment) – показник вимірює віддачу від маркетингових інвестицій; CPA (Cost Per Acquisition) - показник, який вимірює середні витрати на залучення одного нового клієнта; CLV (Customer Lifetime Value) - показник, який вимірює прибуток, який приносить один клієнт протягом його життєвого циклу взаємодії з вашою компанією; Conversion Rate - показник, який вимірює відсоток відвідувачів, які виконують бажану дію та інші показники які встановлюються перед початком маркетингових чи безпосередньо рекламних ініціатив.

Однією з найважливіших переваг цифрового маркетингу є можливість точного вимірювання результатів у реальному часі. Можна аналізувати ефективність своїх кампаній, вимірювати конверсії, кількість взаємодій, їхню ефективність в різних соціальних медіа та багато іншого що безумовно дозволяє оптимізувати свої інвестиції та стратегію онлайн. Це дозволяє зменшити витрати порівняно з традиційними формами реклами, такими як телебачення або преса, і одночасно досягати кращих результатів. На жаль не

всі рекламні кампанії можуть здобувати встановлені результати в інтернет середовищі. Є категорії для яких, на цей час, є більш ефективні канали комунікації та безумовно кожен учасник знаходиться в постійному пошуку найбільш ефективних для себе рішень яким чином донести своє повідомлення до цільової аудиторії, щоб вплинути на її рішення щодо відповідного товару чи послуги в майбутньому.

Маркетингові інструменти та відповідно ті контакти з аудиторією через які вони передуються також можна класифікувати за тривалістю їхнього ефекту на:

а) короткострокові (до одного року) - контакти в пошукових системах таких як Google AdWords, використання SMS-повідомлень чи електронних листів, промо-акції та інше;

б) середньострокові (від року до трьох) - можна вважати використання платформ Facebook, Instagram, Twitter де відбувається побудова спільноти клієнтів/прибічників та майбутня взаємодія з ними, створення та поширення ціннісного та цікавого контенту, такого як статті, блоги, відео з позиціювання компанії як експерта у своїй галузі;

в) довгострокові (від трьох років) - можна віднести брендування, керування репутацією, інновації та дослідження, а де та в який медіа каналах про це говорити аудиторії буде залежати від її складу.

Вдале «жонглювання» контактами з цільовою аудиторією відповідно до поставлених маркетингових завдань та відповідно побудова рекламних кампаній, їх вимірність на предмет постійного удосконалювання ефективності є метою багатьох компаній та невпинним пошуком правильних рішень маркетинговими командами та рекламними агенціями.

Список використаних джерел:

1. *Philip Kotler, Kevin Keller - Marketing Management, 2014*
2. *Al Ries, Jack Trout - Positioning: The Battle for Your Mind, 2001*
3. *Dave Chaffey, Fiona Ellis-Chadwick - Digital Marketing, 2019*
4. *Jonah Berger - Contagious: How to Build Word of Mouth in the Digital Age, 2014*
5. *Mark W. Schaefer - Marketing Rebellion: The Most Human Company Wins, 2019*

Онишко В. О.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ВСЕОСЯЖНА РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНОМУ МАРКЕТИНГУ ТА УПРАВЛІННІ

Штучний інтелект (ШІ) виступає як трансформаційна технологія, що значно впливає на різні аспекти бізнес-операцій, включаючи маркетинг та управління. Він прискорює процеси прийняття рішень, покращує досвід споживачів і впливає на стратегічні підходи до управління. Ця стаття має на меті проаналізувати вплив ШІ на практики маркетингу та управління, зосереджуючись на оперативній ефективності, взаємодії зі споживачами та стратегічному прийнятті рішень.

ШІ революціонує сферу маркетингу, дозволяючи персоналізовану та цільову рекламу, таким чином оптимізуючи споживчий маршрут. Машинне навчання, підрозділ ШІ, використовується для аналізу поведінки споживачів і вподобань, тим самим сприяючи доставці персоналізованого контенту. Прогнозна аналітика, заснована на ШІ, допомагає бізнесу антиципувати потреби споживачів, дозволяючи їм розробляти маркетингові стратегії, які задовольняють ці потреби проактивно. Такий рівень налаштування збільшує взаємодію зі споживачами, покращує лояльність до бренду і сприяє зростанню доходів.

Більше того, ШІ допомагає компаніям управляти і інтерпретувати великі обсяги даних, які генеруються з різних джерел. Аналіз даних на основі ШІ дозволяє отримувати відомості в реальному часі, які сприяють стратегічному прийняттю рішень і управлінню ризиками. Наприклад, компанії використовують ШІ-алгоритми для ідентифікації шаблонів і тенденцій в даних про продажі, які менеджери можуть потім використовувати для прийняття обґрунтованих рішень.

Стосовно управління, ШІ-інструменти спрощують адміністративні процеси, автоматизують рутинні завдання та покращують ефективність робочого процесу. Вони допомагають в таких областях, як планування, бюджетування та розподіл ресурсів, звільняючи менеджерів для зосередження на більш складних, високорівневих завданнях. Більше того, ШІ-чат-боти та віртуальні помічники покращують обслуговування клієнтів, надаючи миттєву підтримку 24/7, таким чином підвищуючи задоволеність клієнтів та їх утримання.

Однак впровадження ШІ приносить певні виклики, такі як питання конфіденційності даних та етичні розгляди. Це вимагає ефективного

управління та регулятивних заходів, щоб гарантувати, що додатки ШІ поважають приватність користувачів і дотримуються етичних стандартів.

У заключенні, роль ШІ в маркетингу та управлінні є глибокою та продовжує рости. Бізнес, який ефективно використовує потужність ШІ, може досягти вищої оперативної ефективності, покращити взаємодію зі споживачами і приймати кращі стратегічні рішення. Однак обережне управління конфіденційністю даних та етичними питаннями є важливим для забезпечення успішної інтеграції ШІ.

Список використаних джерел:

1. Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W.W. Norton & Company.

2. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach. Science and Engineering Ethics, 24(2), 505-528.

3. Chui, M., Manyika, J., Miremadi, M., Henke, N., Chung, R., Nel, P., & Malhotra, S. (2018). Notes from the AI frontier: Insights from hundreds of use cases. McKinsey Global Institute.

4. Davenport, T., & Ronanki, R. (2018). Artificial Intelligence for the Real World. Harvard Business Review, 96(1), 108-116.

5. Huang, M. H., & Rust, R. T. (2021). Artificial intelligence in service. Journal of Service Research, 24(1), 5-22.

6. Kumar, V., & Reinartz, W. (2012). Customer Relationship Management: Concept, Strategy, and Tools. Springer.

Павлив Е. В

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ БИЗНЕС-ПРОЦЕССАМИ

Цель исследования состоит в исследование теоретических основ и формирование практических рекомендаций по усовершенствованию системы информационного обеспечения управления бизнес-процессами на предприятии.

С учетом приведенного цели необходимо изучить сущность и задачи системы информационного обеспечения управления бизнес-процессами предприятия; исследовать методические аспекты оценки эффективности информационного обеспечения управления бизнес-процессами предприятия; провести оценку современного состояния и эффективности процесса информационного обеспечения управления бизнес-процессами предприятия; осуществить обоснование направлений развития информационного обеспечения управления бизнес-процессами предприятия; представить прогноз в оценке в эффективности реализации предложенных мероприятий.

В современных условиях, для субъектов хозяйствования, внедряющих процессный подход к управлению, определяющим следует считать вопрос использования новейших технологий развития собственной бизнес-системы, а также использования современных методов оценки ее эффективности. В целях эффективного управления бизнес-процессами современные предприятия внедряют информационные системы диагностики и моделирования бизнес-систем с точки зрения определения конкретных процессов, необходимых для достижения стратегических целей предприятия [11, с. 20].

По нашему мнению, под бизнес-процессом целесообразно понимать непрерывную систему связанных между собой упорядоченных и управляемых действий, которая выступает составным элементом механизма создания добавленной стоимости в ходе трансформации ресурсов компании, направленная на формирование значительной производительности и эффективности предприятия в целом и обеспечение мультипликации. потребительской ценности для целевого рынка, используя бизнес-модель предприятия.

В современных условиях ведения бизнеса основной задачей управления бизнес-процессами на предприятии является обеспечение его устойчивого развития. В этой связи необходима своевременная и

комплексная оценка результатов работы путем проведения качественного анализа параметров функционирования такого предприятия [3, с. 135].

Эффективным направлением усовершенствования управления бизнес-процессами на предприятии является внедрение современных информационных систем и технологий, позволяющих повысить скорость, качество и надежность процессов сбора, хранения и обработки информации; значительно сократить управленческий состав предприятия, готовящего информацию для формирования и принятия управленческих решений; своевременно обеспечивать руководство и административный персонал предприятия качественной информацией; своевременный и качественный анализ и прогнозирование экономической деятельности предприятия; принимать быстрые и качественные решения на всех уровнях управления.

Современные условия трансформации функций управления обновляют исследование информационного менеджмента предприятия, что не только отражает экономические явления и процессы, но позволяет аналитически анализировать их природу и влияние на эффективность управленческих решений [16, с. 197].

Информационная система (ИС) – это целостный набор понятий, методов, технологий, аппаратных средств и программного обеспечения, используемых для автоматизации сбора, регистрации, обработки, хранения и раскрытия информации потребителям с целью достижения этой цели [36, с. 245].

В некоторых специализированных областях технологической основой информационных систем системы обработки информации (ИС), ориентирующаяся на деятельность компании, организации, учреждения.

Предметной сферой каждой деятельности является часть реального мира, которую нужно исследовать, чтобы организовать управление процессами и объектами для достижения бизнес-результатов. Предмет можно разбить на фрагменты.

По результатам ретроспективной оценки литературных источников [8; 13; 20; 26; 37; 40] считаем целесообразным описать природу информационной системы, как показано на рис. 1.

Из приведенных выше определений и изложений сущности ИС управление бизнес-процессами вытекает из его основной задачки, которая заключается в подготовке и предоставлении информации, нужной для обеспечения управления всеми ресурсами компании либо организации методом сотворения информационно-технических сред для управления бизнес-процессами.

Основной задачей информационной системы управления бизнес-процессами на предприятии предлагается рассматривать как совокупность таких составляющих [35, с. 23]:

сбор информации из разных источников;

регистрация, обработка и передача информации, характеризующая производство и управление;

распределение и обособление информации между специалистами и руководителями, подразделениями и отдельными поставщиками услуг в соответствии с их участием в производственных или управленческих процессах.

Сегодня на рынке программного обеспечения имеется много автоматизированных информационных систем, которые удовлетворят самых требовательных пользователей и имеют следующие характеристики: основываются на общих стандартах корпоративного управления, охватывают всю корпоративную деятельность на основе эталонных моделей [40, с. 271].

Разнообразие способов применения современных информационных систем и их классификации, которая обобщена по литературным источникам [22; 26; 28; 41] в Приложении А.

Информационные системы компании, системы поддержки решений и экспертные системы (индикаторы и значимость) показывают новый уровень автоматизации управления бизнес-процессами в компаниях.

Информационные системы предприятия для управления бизнес-процессами предприятия – это идеология управления, которая сочетает бизнес-стратегию предприятия с передовыми информационными технологиями.

Характерные особенности современных операционных информационных систем для управления бизнес-процессами в компании приведены на рис. 2.

Список использованных источников:

1. Андрейчіков О. О. Використання сучасних інформаційних технологій в процесі розробки регламентів довільної складності. Науково-технічний збірник «Комунальне господарство міст» ХНУМГ імені О. М. Бекетова серія «Технічні науки та архітектура». 2013. №110. С. 259–265.

2. Батюк А. Є. Інформаційні системи в менеджменті: навч. посіб. Львів: Інтелект-Захід, 2014. 520 с.

3. Босак І. П. Інформаційне забезпечення управління розвитком підприємств. Квалілогія книги. 2019. № 2. С. 134−136.

4. Будько О. В. Класифікація обліково-аналітичної інформації з метою інформаційного забезпечення управління сталим розвитком підприємства. Інноваційна економіка. 2015. № 1. С. 207−212.

Петрунь А.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

СУЩНОСТЬ И ЗНАЧЕНИЕ ИННОВАЦИЙ КАК ОСНОВЫ КОНКУРЕНТНОГО РАЗВИТИЯ ПРЕДПРИЯТИЯ

Инновации и нововведения обычно представляются как направление научно-технического прогресса (его высокотехнологичная составляющая) и как процесс, связанный с внедрением исследований и разработок в практику. Сфера инноваций обширна, она включает в себя не только практическое применение научно-технических разработок и изобретений, но и изменения в продукте, процессах, маркетинге и организации. Инновация выступает как явный фактор изменений в результате встраиваемой в новый или усовершенствованный продукт деятельности, технологические процессы, новые услуги и новые подходы к удовлетворению общественных потребностей [18, с. 67].

Совокупность происходящих на предприятиях различных отраслей экономики процессов и явлений можно разделить на две группы традиционные и инновационные. Традиционные процессы и явления характеризуют нормальное функционирование национальной экономики, отраслей и компаний и их инновационное развитие на качественно новом уровне. Долгое время, когда экономика функционировала и развивалась в основном за счет экстенсивных факторов (использование растущих общественных человеческих ресурсов, производственных мощностей), в производстве преобладали традиционные процессы и явления. Поскольку экстенсивные факторы почти исчерпаны или их действия стали экономически невыгодными, развитие и интенсификация современного производства должны базироваться, прежде всего, на новых решениях в технологиях, организационных формах и методах хозяйствования. Подготовка, принятие и реализация таких решений есть содержание так называемых инновационных процессов [24, с. 116].

В целом инновация – это нововведение в инженерии, технологии, организации труда или управлении, основанное на использовании достижений науки и передового опыта. Инновация это конечный результат нововведения, т.е. деятельности, связанной с превращением исследований и разработок, других научно-технических достижений в новый или усовершенствованный продукт, поступающий на рынок, новый или усовершенствованный технологический процесс, используемый на практике, или новый подход к социальным услугам.

Термин «инновация» ввел в научное обращение в 1912 г. австрийский экономист и социолог Й. Шумпетер. Он определил понятие инновации „как

новое научно-организационное сочетание использования факторов производства, мотивированного предпринимательством“. То есть, по его мнению, инновациями могут являться новые продукты, новые технологии, новая организация промышленного производства и управления, а также открытие новых рынков. Они являются источником корпоративного развития, усовершенствования внутренних процессов, извлечения новых ресурсов и производственных факторов.

Термин „инновация“ не имеет единого конкретного определения.

Таким образом, анализируя определение понятия «инновация», можно заключить, что это конечный результат инновационной деятельности по изменению цели управления и влияния на экономическое, социальное, экологическое, научно-техническое или другое состояние.

Исследование позволило сформулировать следующие ракурсы научной категории „инновация“ [34; 39; 67]:

1. Инновация как ценность является результатом нового образа мышления и реализации стратегии, ведущей к созданию нового продукта, открывающего новую рыночную нишу и выделяющегося среди конкурентов;

2. Инновация как специфический принцип социальной ответственности, связанная с поиском рыночных возможностей, исследованием рынка, финансовым менеджментом, использованием ресурсов, привлечением инвестиций и социально ответственным управлением;

3. Инновация как инструмент современного стратегического управления предприятием способствует динамичному саморазвитию компании и обеспечивает конкурентоспособность на всех иерархических уровнях экономики [50, с. 206].

Список использованных источников:

1. *Дука А.П. Теорія та практика інвестиційної діяльності: навч. посіб. К.: Каравела, 2013. 423 с.*
2. *Ілляшенко С.М. Управління інноваційним розвитком: проблеми, концепції, методи: навч. посіб. Суми: ВТД «Університетська книга», 2018. 581 с.*
3. *Кучеров А.П. Объектное управление: новационый и инновационный менеджмент в туризме. М.: Издательство «Спутник+», 2014. 208 с.*
4. *Малюта Л.Я. Оцінювання рівня інноваційного розвитку промислового підприємства. Соціально-економічні проблеми і держава. 2021. Вип. 1 (4). С. 56-63.*
5. *Скалюк Р.В., Декалюк О.В. Ефекти та ефективність інноваційної стратегії підприємств. Вісник Хмельницького національного університету. 2020. № 1. С. 149-154.*
6. *Пересада А.А., Смірнова О.О., Онікієнко С.В., Ляхова О.О. Інвестування: Навч.-метод. посібник для самост. вивч. дисц. К.: КНЕУ, 2015. 251* с.

Сердюк М. А.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

PR ОСНОВНОЙ КОМПОНЕНТ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ: ФУНКЦИИ, ЗАДАЧИ

В современных условиях использование только основных средств представления и продвижения товара на рынке недостаточно. Каждый новый товар или услуга подразумевает разработку нового маркетингового хода, позиционирования на общем рынке. Информация должна быть уникальной, интересной и оригинальной.

Удачное построение коммуникационных стратегий зависит от маркетинговых исследований.

Согласно определению Американской ассоциации маркетинга, маркетинг - это деятельность, совокупность институтов и процессов, обеспечивающих создание, информирование, доставку и обмен предложений, имеющих ценность для потребителей, клиентов, партнеров и общества в целом [4, с. 16].

Вместе с тем, необходимо указать, что цель маркетинга — сделать усилия по сбыту ненужными. Его цель — так хорошо познать и понять клиента, что товар или услуга будут точно подходить последнему и продавать себя сами.

Необходимо анализировать общий рынок, проводить мониторинг современных технологий, разрабатывать план действия по улучшению товара или услуги. Конечно, все это влияет на общую презентацию фирмы, установление связей с общественностью.

Также обратимся к дефиниции «маркетинговые коммуникации – это «процесс эффективного донесения информации о продукте или идее до целевой аудитории» [6, с. 19]

Все стратегии определяют популярность конкретного продукта и поддержку на общем рынке. Необходимо акцентировать внимание на тех свойства товара, которые станут основой для мощной кампании продвижения.

Так, либо по-другому, маркетинг – это двусторонний процесс, взаимодействие. Предприятия ничего не могут создавать и планировать без изучения потребностей потенциальной аудитории. Соответственно, и наоборот – клиенты не получат удовлетворения своих потребностей.

Необходимо работать над формированием благоприятного общественного мнения об организации и продукции, которое называется «public relations» . Связи с общественностью – установление связей с определенными социальными группами.

Подобным образом определение подает теоретик В. Королько: «паблик рилейшнз – это функция управления, способствующая налаживанию или поддержанию взаимовыгодных связей между организацией и общественностью, от которой зависит её успех или неудача» [5, с. 28]).

Наряду с этим обратимся и к описанию С. Блэка, который формулирует PR как «искусство и науку достижения гармонии посредством взаимопонимания, основанного на правде и полной информированности» [2, с. 103].

Из этого следует, что паблик рилейшнс обязательно должен охватывать общественные отношения, взаимодействие, контакт, коммуникацию.

При этом важно разграничить понятие между PR и рекламой. Весь процесс PR направлен на формирования позитивного восприятия продукта или услуги компании, основная цель рекламы — продать. Часто рекламу формирует сама компания от себя, PR проводят другие.

Рассматривая основные цели паблик рилейшнз, И. В. Алёшина указывает на следующих позициях:

- привлечение внимания потенциальной аудитории;
- стимулирование интереса;
- формирование потребности;
- обеспечение правильного понимания сообщения аудиторией;
- интерпретацию информации в ключе, выгодном коммуникатору;
- обеспечение запоминания сообщений аудиторией [1, с. 39].

Профессор Дж. Марстон описывает оригинальное определение PR, обращая внимание на функции. Таким образом выделяет систему RACE [9, с. 14]:

1. Исследование (Research);
2. Действие (Action);
3. Общение (Communication);
4. Оценка результатов (Evaluation).

Использование технологий подразумевает влияние на общественность. В общей системе PR массы (аудиторию) делят на внутренние и внешние группы.

Как описывают А. Романова и А. Панько, функциональные составляющие PR выглядят следующим образом:

- Media relations – построение отношений со СМИ;
- Government relations – взаимодействие с властными структурами; Investor relations – взаимоотношения с инвесторами;
- Corporate affairs – управление корпоративным имиджем;
- Special Events – организация и проведение специальных мероприятий;
- Employee communications – взаимодействие с персоналом;
- Crisis management – управление кризисными ситуациями [7, с. 19].

Таким образом наблюдаем постоянное взаимодействие всех участников PR-коммуникации. Важно не только оказывать влияние на потребителей, но и повышать квалификацию персонала. Также детально выбирать канал, по которому будет проходить основной поток трансляции данных.

Изучая интерес к товарам и услугам организации, выделяют следующие формы PR-мероприятий [8]: брифинг, пресс-конференция, презентация (в том числе день открытых дверей), деловые PR-мероприятия (конференция, круглый стол, форум), благотворительные и спонсорские мероприятия, фестивали, семинар, лекция, выставки, Promotion; Интернет-коммуникации, социальные проекты и другие.

Становится понятным, что мероприятия проходят согласно плану и часто зависят друг от друга.

Например, брифинг – это мероприятие, на котором представители любой организации сообщают важную информацию для прессы. Пресс-конференция подразумевает активные действия представителей СМИ (формат «вопрос-ответ»). Презентацию организовывают в целях рекламы новых направлений предприятия, нового объединения, проекта и т. п.

Выставки и ярмарки с точки зрения связей с общественностью тоже представляют собой комплексные мероприятия, объединяющие целые группы достаточно эффективных PR-акций по взаимодействию с аудиториями [3, с. 75].

Деловые мероприятия больше обращены к коммуникации с партнерами, а не с общественностью. На конференциях, семинарах, дебатах, круглых столах обсуждают актуальные проблемы.

Становится понятным, что такие составляющие непременно повлияют на установление связей с обществом. Следовательно, цель PR – достижение взаимопонимания, выявления и формирования общих представлений, ценностей, интересов и преимуществ на основе достоверной и достаточной информации. Связи с общественностью подразумевают массовую коммуникацию, которую планируют на длительный период.

Список использованных источников:

1. *Алёшина И. В. Паблик Рилейшнз для менеджеров: курс лекций. М.: ЭКМОС, 2002. 480 с.*
2. *Блэк С. Паблик Рилейшнз. Пер. с англ. М. : Сирин, 2003. 202 с.*
3. *Варакута С. А. Связи с общественностью. М. : ИНФРА. 2004. 207 с.*
4. *Друкер П. Ф. Бизнес и инновации М.: «Вильямс», 2007. 432 с.*
5. *Королько В. Г. Основы паблик рилейшнз: учебник для студентов вузов; авторизиров. пер. с укр.; науч. ред. О. В. Некрасова; отв. ред. С. Л. Удовик. Киев: Релф-бук: Ваклер, 2003. 528 с.*
6. *Разумовская А. Л. Маркетинг услуг. Настольная книга российского маркетолога-практика. М.: Вершина, 2006. 120 с.*
7. *Романов А. А., Панько А.В. Маркетинговые коммуникации. М.: Эксмо, 2006. 432 с.*
8. *Толкачев А. Н. Организуя PR своего бизнеса. Издательство: Эксмо, 2008 г. URL: https://bookshaker.net/r/organizuya-pr-svoego-biznesa-andrey-nikolaevich-tolkachev (дата обращения: 01. 06.2023)*
9. *Marston J. The Nature of Public Relations. N. Y., 1963. 393 p.*

Топчій О. Д.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ПЕРЕВАГИ ВПРОВАДЖЕННЯ ІНТЕРНЕТ-МАРКЕТИНГУ ТА ЙОГО ІНСТРУМЕНТАРІЙ ДЛЯ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА НА РИНКУ НЕРУХОМОСТІ

Сучасний розвиток економіки вимагає нових підходів до конкуренції на ринках збуту. Для поліпшення конкурентоспроможності підприємств потрібно застосовувати не лише традиційні офлайн-маркетингові інструменти, але й нові онлайн-методи. Зміна споживчих настроїв та орієнтація національної економіки ставлять питання ефективного управління рекламною конкурентоспроможністю підприємств в Інтернеті у першій черзі. [1]

Переваги цифрового маркетингу для забудовників:

Глобальна охопність та точна націленість: він дозволяє компаніям досягати потенційних клієнтів у будь-якій точці світу, а також таргетувати рекламу на конкретні групи користувачів з урахуванням їх інтересів, поведінки та демографічних характеристик. Такий підхід дозволяє суттєво підвищити ефективність маркетингових кампаній та оптимізувати бюджет.

Рентабельність: Цифровий маркетинг пропонує порівняно нижчі ціни, ніж традиційний маркетинг, тому не дивно, що маркетологи в галузі нерухомості повністю використовують ефективність затрат.

Підвищена експозиція: враховуючи численні житлові проекти, які різняться за розміром, місцем розташування та вартістю, наявність цифрової маркетингової стратегії дозволяє розширити загальний обсяг та навіть налаштувати його на обраний цільовий ринок. [2]

Аналіз ефективності: Цифровий маркетинг пропонує безліч способів відстежувати ефективність реклами на конкурентному ринку, що полегшує забудовникам зрозуміти, яка техніка маркетингу найкраще підходить для їх продукції.

Креативна ліцензія: будь то квартира, незалежний будинок, вілла чи земельна ділянка, розробники мають численні способи продемонструвати свою продукцію на інтернет-ринку.

Побудова торгової марки: щоб досягти успіху у величезній галузі, яка є нерухомістю, розробникам потрібна сильна та поважна присутність. Присутність в Інтернеті вважається однією з найкращих технік побудови бренду. [3]

Інструменти інтернет-маркетингу для ринку нерухомості:

1. Базова SEO-оптимізація - повномасштабне пошукове просування для об'єкту не буде ефективним, тому що потенційне семантичне ядро буде дуже невеликим, а часу на вихід в ТОП знадобиться чимало. А ось базову SEO-оптимізацію провести необхідно. Тому що без цього навіть за самою назвою ЖК сайт буде складно знайти в пошуку. При цьому можна експериментувати з різними комбінаціями запитів.

2. Просування в Olx – раніше ця мережа використовувалась лише фізичними особами для того щоб продавати непотрібні речі. Але зараз платне просування в Olx стало одним з найефективніших методів продажу квартир для забудовників.

3. Розміщення на картах Google - додавання нових фотографій у процесі будівництва, контакти для зв'язку з офісом, коментарі та оцінки від користувачів – все це теж позитивно позначається на залученні уваги з боку потенційних покупців.

4. Сторінка та таргетована реклама у Facebook - він має детальне націлювання за демографією, віком та поведінкою. Крім того, можна також націлюватися на відвідувачів свого веб-сайту та тих, хто мав взаємодію з вашою публікацією, щоб оголошення відображалося більш конкретному та нішевій аудиторії, що робить ймовірність продажу об'єкта нерухомості навіть вищою, ніж раніше. [4]

5. Оголошення на регіональних мовах почали набувати популярності, й маркетологи почали включати цю концепцію у свої маркетингові стратегії, щоб охопити свою цільову аудиторію. Коли потенційний покупець читає рекламу на своїй регіональній мові, він розвиває довіру до продавця і, швидше за все, зробить покупку або хоча б рекомендує цей товар другові.

6. Агрегатори нерухомості - це тематичні портали, які агрегують на своїх сторінках пропозиції від різних забудовників, а для багатьох користувачів вони є відправною точкою під час пошуку майбутнього житла. Найбільші такі агрегатори в Україні – Dom.ria.com і Lun.ua. Тут можна створювати сторінки окремих об'єктів, об'єднувати їх під загальним профілем компанії, додавати інформацію про наявність квартир, про їх планування, відзначати ЖК на карті та багато іншого.

7. Профіль в Instagram - на візуальну складову під час вибору майбутньої новобудови і покупки квартири потенційні клієнти звертають увагу в першу чергу. А в якості інструменту для візуальної комунікації Instagram підходить якнайкраще. [5]

Існує дійсно велика кількість інструментів інтернет-маркетингу. Забудовники можуть використовувати їх для просування своїх ЖК або комерційних проектів та успішного продажу квартир через Інтернет.

Швидкий розвиток електронної комерції робить інтернет-маркетинг необхідним інструментом для компаній. Він дозволяє їм залучати нових клієнтів та збільшувати продажі через онлайн-магазини та платформи. Крім

того, інтернет-маркетинг забезпечує можливість проводити різноманітні маркетингові дослідження, аналізувати дані та приймати обґрунтовані рішення на основі цифрових показників.

В цілому, в сучасному світі компанії не можуть нехтувати інтернет-маркетингом, оскільки він є ефективним інструментом для залучення, утримання та взаємодії.

Список використаних джерел:

1. Центр маркетингових досліджень, онлайн-опитувань та інтеграції даних: Дослідження аудиторії з інтересом до покупки нерухомості бізнесі [Електронний ресурс] – Режим доступу: https://research-me.com/

2. Академія інтернет-маркетингу [Електронний ресурс] – Режим доступу: webpromoexperts.net

3. Стратегії цифрового маркетингу нерухомості [Електронний ресурс] – Режим доступу: https://www.innoservdigital.com/blog/

4. Digital-інструменти для ринку нерухомості у 2022 році [Електронний ресурс] - promedia.io/blog

5. Блог новин про бізнес та Digital-marketing [Електронний ресурс] – Режим доступу: thepage.ua

Чорний С. С.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ЛИДЕРСЬКІ ТА ПРОФЕСІЙНІ ЯКОСТІ ОПЕРАЦІЙНОГО МЕНЕДЖЕРА

Як правило, операційний менеджер – це друга особа у компанії. Якщо генерального директора (так само як і власника) можна назвати «спринтером», то операційного менеджера – «марафонцем». Власники швидко спалахують якоюсь ідеєю і починають вкладати в неї всю енергію. Але щойно вона приносить перші плоди, власнику стає нудно. Йому важко дається щоденна рутина – хочеться рухатися далі та вигадувати нові проекти. Рутина компанії складається з багатьох процесів. Без аналізу та грамотного управління вони сплітаються в клубок з розмитими зонами відповідальності та поганим результатом. Тому бізнесу потрібна людина, яка створює порядок у бізнес-процесах і знає, як їх покращити. Операційний менеджер - це топ-менеджер, який відповідає за управління постійними бізнес-процесами: їх забезпечення, аналіз, контроль, автоматизацію та покращення. Це фахівець, який забезпечує підвищення ефективності роботи компанії.

Хоча й загальноприйнятого чіткого визначення посади «операційний менеджер» немає (в одних компаніях операційний менеджер відповідає за виробництво, маркетинг та продажі, в інших – за дослідження та розробки, у третіх – за фінанси та наймання співробітників), все ж таки, окрім аналітичного складу розуму та управлінського досвіду, для операційного менеджера важливі такі характеристики:

- лідерські якості. Ця посада передбачає постійний контакт з людьми та організацію їхньої роботи, тому важливо мати компетенції лідера та здібності до управління та керівництва;
- стратегічне мислення. Операційний менеджер має бути відкритий для нових перспектив, прагнути далекоглядності, щоб прораховувати результат кожного рішення на 2 кроки вперед;
- орієнтація на результат. Кожен процес оптимізується для досягнення конкретних цілей та вирішення пріоритетних завдань;
- фінансова грамотність. Операційний менеджер часто взаємодіє з фінансами, тому навички фінансового менеджменту будуть не зайвими, а іноді й зовсім необхідними;
- комунікація. Операційний менеджер має вміти спілкуватися з різними людьми, вирішувати їхні проблеми, впливати на їхню результативність, регулювати конфлікти — все це неможливо без розвинених комунікативних навичок.

Існує цікава точка зору, що ідеальний генеральний директор повинен проводити всередині компанії та її процесів лише 20% часу, а решта 80% він має займатися пошуком можливостей, корисної інформації, контактів, людей та ресурсів для розвитку бізнесу. А ідеальний операційний менеджер забирає на себе все те, що є слабкими сторонами генерального директора чи те, що заважає генеральному директору зосереджуватися на стратегічних завданнях.

Оскільки операційний менеджер орієнтований на підвищення ефективності всіх бізнес-процесів підприємства, а його робота, насамперед, пов'язана зі складанням планів, продумуванням стратегій, відстеженням та аналізом даних, саме аналітичне мислення, на мій погляд, є основним критерієм відповідності професії. Аналітичні здібності, як одна з найголовніших якостей - це здатність думати, розмірковувати, аналізувати ситуацію в принципі, здатність розкласти ситуацію на складові. Аналітичний стиль мислення орієнтований на систематичний та всебічний розгляд питання чи проблеми в тих аспектах, які задаються об'єктивними критеріями, схильний до логічної, методичної, ретельної (з акцентом на деталі) манері вирішення проблем.

Всесвітній економічний форум поставив аналітичне мислення на перше місце серед 10 навичок, які будуть потрібні серед роботодавців к 2025 року. При аналітичному способі мислення людина розкладає інформацію на складові, структурує дані та з'ясовує їх співвідношення між собою. Такий підхід дозволяє приймати найкраще серед усіх можливих рішень. Англійські вчені Харрісон та Бремсон кажуть, що таким людям властива логічна, детальна та обережна манера вирішення проблем. Щоб ухвалити рішення, вони подумки складають докладний план.

Як правило, вирішення задачі аналітичним шляхом розбивається на кілька кроків:

- отримати інформацію та побачити завдання повністю;
- розкласти її на кілька складових;
- виконати аналіз кожного елемента: виділити позитивні та негативні моменти;
- розставити пріоритети;
- вибрати найбільш підходящий варіант або спосіб вирішення задачі.

Щодо лідерських якостей, слід розуміти, що проблеми лідерства є ключовими для досягнення організаційної ефективності. З одного боку, лідерство розглядається як наявність певного набору якостей, що приписуються тим, хто успішно впливає на інших, з іншого, лідерство - це процес переважно не силового впливу у напрямку досягнення групою чи організацією своїх цілей. Лідерство є специфічний тип управлінської взаємодії, заснований на найбільш ефективному поєднанні різних джерел влади і спрямований на спонукання людей до досягнення спільних цілей.

Також слід розуміти, що природа лідерства може бути зрозумілою, якщо його порівнювати з керівництвом. Бути менеджером і бути лідером в організації - це не одне й те саме. Менеджер у своєму впливі на роботу підлеглих і побудові відносин з ними, перш за все, використовує та покладається на посадову основу влади та джерела, що її живлять. Лідерство ж, як специфічний тип управління, ґрунтується більше на процесі соціального впливу, а точніше взаємодії в організації. На відміну від керівництва лідерство передбачає наявність в організації послідовників, а не підлеглих. Відповідно відносини «начальник - підлеглий», властиві традиційному погляду управління, замінюються відносинами «лідер - послідовник».

Практика показує, що жоден фактор не забезпечує більшої вигоди та користі для організації, ніж ефективне лідерство. Лідери необхідні для визначення цілей і завдань, для організації, координації, забезпечення міжособистісних контактів із підлеглими і вибору оптимальних, ефективних шляхів вирішення тих чи інших проблем.

Отже, перш за все, операційний менеджер - людина з розвиненим системним та аналітичним мисленням. Він моментально помічає найдрібніші помилки, має професійну чесність і цілеспрямованість. Вміє здійснювати управління людськими ресурсами, швидко знаходить спільну мову з колективом та здатний набути авторитету. Схильний до безперервного навчання, наполегливий та відповідальний.

Список використаних джерел:

1. *Филонович С.Р. Лидерство и практические навыки менеджера, 2004;*
2. *Олексієв А.А., Громова Л.О. "Зрозумійте мене правильно...", Економічна школа, 1993;*
3. *Артёмов А.С. Курс лекций по психологии. Харьков, 1958;*
4. *Веб-сайт Всесвітнього економічного форуму* https://www.weforum.org.

Ievgenii Doroshenko

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

OVERCOMING COMMON MARKETING CHALLENGES IN THE IT INDUSTRY

In this report, we will explore the marketing challenges faced by IT companies, including issues related to product differentiation, lead generation, branding, and customer engagement. Through case studies of companies that have successfully navigated these challenges, we will identify best practices and strategies for overcoming common marketing obstacles in the IT industry.

Marketing challenges in the IT industry can arise from a variety of factors, including the fast pace of technological change, the need to stand out in a crowded marketplace, and the difficulty of effectively reaching and engaging customers. In order to successfully market their products and services, IT companies must have a deep understanding of their target audience, be able to clearly differentiate themselves from competitors, and create engaging content that resonates with customers.

The IT industry encompasses a wide range of businesses involved in the development, manufacturing, and distribution of technology-related products and services. It includes hardware, software, telecommunications, internet services, and consulting companies. The industry is characterized by rapid technological advancements and innovations, which significantly impact marketing strategies.

Consumer Behavior:

Understanding consumer behavior is crucial for effective marketing in the IT industry. Consumers' purchasing decisions are influenced by factors such as product quality, brand reputation, pricing, ease of use, and technological advancements. Marketers need to identify and analyze their target audience's needs, preferences, and purchasing patterns to develop targeted marketing strategies.

In the highly competitive IT industry, product differentiation is a significant challenge. IT companies often face the task of standing out among numerous competitors offering similar products or services. They must showcase the unique features, value proposition, and benefits of their offerings to attract customers. Differentiation strategies may involve highlighting technological advancements, customization options, superior performance, or exceptional customer support.

Generating high-quality leads is a common marketing challenge for IT companies. The complex and technical nature of IT products often requires a targeted approach to identify and attract potential customers. IT marketers need to leverage various channels, such as content marketing, search engine optimization

(SEO), social media marketing, and events, to capture leads. Nurturing and qualifying leads through effective lead management processes is crucial for successful conversions.

Building a strong brand presence is essential in the IT industry, but it can be a challenge. Establishing a reputable brand requires consistent messaging, visual identity, and customer experiences. Branding challenges in the IT industry may include overcoming negative perceptions, differentiating from competitors, and creating brand loyalty in a rapidly evolving market. Strategies such as thought leadership, testimonials, case studies, and community engagement can help enhance brand recognition and reputation.

Engaging customers effectively is crucial for IT companies to build relationships, retain customers, and drive sales. However, the complex and technical nature of IT products can make customer engagement challenging. IT marketers need to communicate product features and benefits in a clear, understandable manner. Additionally, creating personalized experiences, providing exceptional customer support, and leveraging customer feedback channels are essential for successful customer engagement.

Let’s overview the best practices for IT companies seeking to overcome common marketing challenges. It focuses on key areas such as lead generation, brand awareness, content creation, and measuring marketing ROI. By implementing these best practices, IT companies can optimize their marketing efforts and achieve better results.

Improving Lead Generation:

Develop targeted buyer personas to understand the needs and preferences of your target audience.

Create compelling content offers, such as whitepapers, e-books, or webinars, to capture leads.

Optimize your website for lead capture by using clear and prominent call-to-action buttons and forms.

Leverage social media platforms and paid advertising campaigns to expand your reach and attract potential leads.

Implement lead nurturing strategies, such as personalized email campaigns and automated workflows, to engage and convert leads into customers.

Building Brand Awareness:

Define your brand positioning and value proposition to differentiate yourself in the market.

Develop a consistent and visually appealing brand identity across all marketing channels.

Engage with your target audience through thought leadership content, guest blogging, or speaking opportunities at industry events.

Leverage social media platforms to amplify your brand message and engage with your audience.

Establish partnerships with complementary businesses or influencers to increase brand exposure.

Creating Engaging Content:

Conduct thorough research to understand the pain points and interests of your target audience.

Develop a content strategy that aligns with your audience's needs and the buyer's journey.

Create a mix of content formats, including blog posts, videos, infographics, and podcasts, to cater to different preferences.

Optimize your content for search engines using relevant keywords and SEO best practices.

Encourage audience interaction through comments, social sharing, and user-generated content.

Measuring Marketing ROI:

Define clear marketing objectives and key performance indicators (KPIs) to measure success.

Implement robust analytics tools to track and measure the performance of your marketing campaigns.

Regularly analyze data and metrics to gain insights into the effectiveness of your marketing efforts.

Use A/B testing to experiment with different strategies and optimize your campaigns.

Continuously refine and improve your marketing strategies based on data-driven insights.

By understanding the common marketing challenges in the IT industry and exploring best practices and emerging trends, companies can develop effective strategies to overcome obstacles and achieve marketing success.

Key Findings:

IT companies face common marketing challenges such as product differentiation, lead generation, branding, and customer engagement. These challenges can be addressed through targeted strategies and approaches.

Successful IT companies have employed innovative marketing strategies, embraced emerging technologies, and adopted customer-centric approaches to overcome challenges and achieve their marketing goals.

Data-driven marketing has become increasingly important, allowing companies to leverage customer insights and personalize marketing campaigns for better results.

Influencer marketing has emerged as a powerful tool to increase brand awareness and engage with target audiences, especially through social media platforms.

The use of AI and machine learning in marketing enables more targeted and personalized campaigns, enhancing customer experiences and optimizing marketing efforts.

Recommendations:

Embrace data-driven marketing by leveraging analytics tools to gain insights into customer behavior and preferences. Use the data to personalize marketing campaigns and optimize strategies.

Explore influencer marketing by identifying influential individuals or organizations in the IT industry to partner with. Leverage their credibility and reach to promote products or services.

Embrace emerging technologies like AI and machine learning to automate marketing processes, enhance customer experiences, and optimize ad targeting and content recommendations.

Continuously monitor industry trends and stay updated on the latest marketing strategies and tactics to remain competitive in the ever-evolving IT industry.

Regularly assess and refine marketing strategies based on data-driven insights and performance metrics to ensure continuous improvement.

References:

1. Kotler, Philip, and Kevin Lane Keller. Marketing Management. Pearson, 2016.

2. Farris, Paul W., et al. Marketing Metrics: The Definitive Guide to Measuring Marketing Performance. 2nd ed., Pearson Education, 2010.

3. Jeffery, Mark. Data-Driven Marketing: The 15 Metrics Everyone in Marketing Should Know. Wiley, 2010.

4. Cialdini, Robert B. Influence: The Psychology of Persuasion. HarperCollins, 2006.

5. Ellis, Sean, and Morgan Brown. Hacking Growth: How Today's Fastest-Growing Companies Drive Breakout Success. Crown Business, 2017.

6. "6 Marketing Challenges Faced by Tech Companies and How to Overcome Them" by Asha Saxena, published on MarTech Advisor, https://www.bbpress.co.uk/news/marketing-challenges-and-how-to-overcome-them

7. The Top 10 Challenges of Marketing in the Technology Industry" by Jessie Coan, published on Marketing Insider Group.

Stanislav Fedorenko

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

THE IMPORTANCE OF ENGAGEMENT MODEL AND WORKFORCE STRATEGY FOR BUILDING A DELIVERY TEAM IN IT OUTSOURCING

The IT Services (ITS) market is primarily dominated by IT Outsourcing (ITO), which refers to the practice of hiring external service providers for IT-related tasks instead of relying solely on in-house resources. [1]

While project management methodologies provide frameworks and guidelines for managing projects and establish effective processes (for example Scrum [2], Scaled Agile Framework (SAFe) [3], Prince2 [4], PMBOK [5]), they may not explicitly address the specific considerations of building teams in the context of IT outsourcing.

It is crucial to grasp the key factors that influence this process to comprehend the intricacies of team building in ITO. In this article two important factors are proposed to be considered: Engagement models and Client Workforce Strategy.

Engagement models

In the IT business, an engagement model is a framework of guidelines that defines the client-supplier relationship. It outlines the responsibilities, obligations, commitments, rules, tasks, and duration of the engagement. These details are documented in a contract that is legally binding and signed by both parties.

Organizations often evaluate their specific needs and objectives to select the most suitable engagement model for their IT outsourcing initiatives. It is proposed to pay attention on 3 main models listed din the table below as the distribution of responsibilities between the client and the supplier significantly influences the approach to team formation and further management.

	Team extension (Staff Augmentation)	**Capacity Based (Manager/Fixed Capacity)**	**Services Based (Managed Services)**
Client Responsibility	• Scope of work, priority and system development life cycle (SDLC) • Project management	• Scope of work, priority, and system development life cycle (SDLC) • Project management	• Business vison and required deliverables

	• Quality standards • Identification of required resource • People management	• Quality standards	
Supplier Responsibility	• Provision of high-quality resources with guaranteed quality and committed time.	• Resources with guaranteed quality • Committed capacity. • Timelines for recruitment and staff warranties • Mitigating attrition • Maintaining high code quality • People management	• Resources with guaranteed quality • Managing product and service delivery • Managing software development • Commitment for delivery • Ensuring delivery quality • Monitoring delivery performance • Maintaining quality in support services
Specifics	• The majority of delivery risks lie with the client • High total cost of ownership (TCO) in the long run	• Project executed by an experienced project team • Shared delivery risks between the Client and Supplier • Quality as a shared responsibility	• Comprehensive services within a specific business domain • Supplier assuming all delivery and support risks • Low total cost of ownership (TCO) in the long term • Shared responsibility for the book of work

Client workforce strategy

Workforce strategy refers to the comprehensive plan and approach adopted by an organization to effectively manage its workforce and align it with its overall business goals and objectives. It involves making strategic decisions and implementing initiatives to attract, develop, retain, and optimize the talent within the organization. In accordance with Gartner, the current landscape of rapid change and uncertainty places added pressure on HR departments to ensure that the organization possesses the necessary talent to adapt and support evolving business priorities. [6]

The terms "workforce" and "organization" are inherently interconnected, as an organization represents a structured and managed workforce that strives to achieve a shared objective. [7]

There is a three-level perspective, as proposed by Wagner and Hollenbeck (2015) [8]

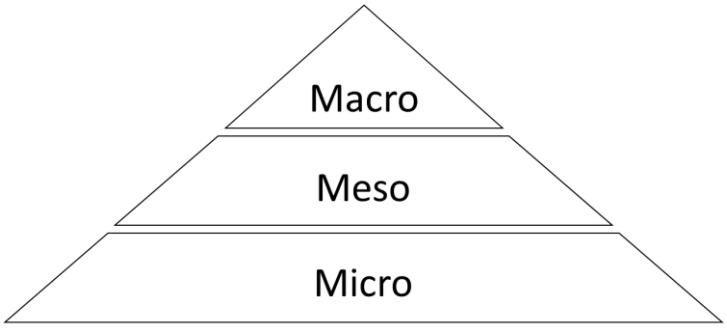


Figure 1 The segments from bottom to top are labeled micro, meso, and macro.

- **Macro.** This is the level of the organization as a whole
- **Meso.** These are the component levels within an organization.
- **Micro.** This is the level of the individual teams.

It is important for ITO suppliers to be consistent with Meso and Micro levels to select the correct approach for building development teams.

Workforce planning involves evaluating the composition of an organization's workforce to determine if it has an adequate number of employees with the necessary skills and qualifications, positioned in the right roles, locations, and at the appropriate times as well as with the required level of cost-effectiveness. There are seven elements to workforce planning that are usually considered by organizations: the right size, the right location, the right time, the right cost, the right risk, and the right shape. [7][9]

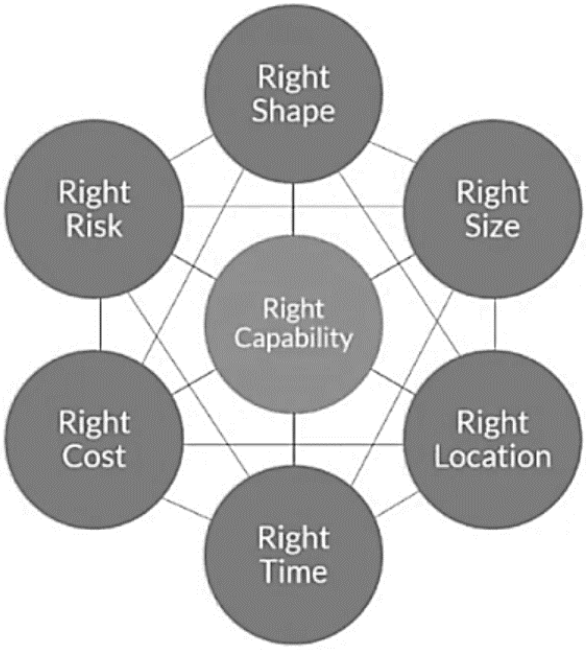


Figure 1.2 Seven rights of workforce planning

By adhering to the client's workforce strategy, IT outsourcing vendors can establish a strong collaborative foundation. This entails delivering services from preferred locations, assembling teams with the desired seniority and skill set, and offering cost-effective solutions. Such alignment fosters client satisfaction, efficient project delivery, and long-term partnerships based on mutual trust and shared objectives.

When building a team in IT outsourcing, the combination of an engagement model, workforce strategy, and project management methodology can be applied effectively. Let's consider an example:

Engagement Model: The client and the service provider agree to a staff augmentation engagement model, where the client retains control over team management while leveraging the service provider's expertise in talent acquisition and resource management. This model allows for flexibility in scaling the team size based on project needs.

Workforce Strategy: The workforce strategy focuses on acquiring skilled professionals with expertise in the required technologies and domain knowledge specific to the client's industry. The strategy emphasizes attracting and retaining talent through competitive compensation packages, career growth opportunities, and a supportive work environment.

The project management methodology, such as Agile or Scrum, is implemented to ensure efficient task management, collaboration, and delivery. It provides a framework for iterative development.

By integrating the engagement model, workforce strategy, and project management methodology, the team is built with the appropriate mix of skills, experience, and cultural fit. This collaborative approach enables efficient project execution, improved productivity, and successful delivery, all while maintaining a strong alignment with the client's goals and requirements.

References:

1. *https://www.statista.com/outlook/tmo/it-services/it-outsourcing/worldwide*
2. *https://www.agilealliance.org/agile101/12-principles-behind-the-agile-manifesto/*
3. *https://scaledagileframework.com/#*
4. *https://www.prince2.com/eur/what-is-prince2*
5. *https://www.pmi.org/pmbok-guide-standards/foundational/pmbok*
6. *https://www.gartner.com/en/human-resources/insights/workforce-planning*
7. *Adam Gibson (2021), Agile Workforce Planning Edition: 1, Kogan, New York*
8. *Wagner, J A and Hollenbeck, J R (2015) Organizational Behavior: Securing competitive advantage, Routledge, New York*
9. *Vetter, E W (1967) Manpower Planning for Hight Talent Personnel, University of Michigan, Ann Arbor*

Vitalii Ivanov

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

THE ROLE OF TECH LEAD IN MODERN REMOTE AGILE DEVELOPMENT TEAMS: FINDING THE RIGHT PLACE AND ACHIEVING BALANCE

As remote work becomes increasingly common in the software development industry, the role of the tech lead has taken on new significance. The significance of a role is based on its purpose and responsibilities within a particular context. In the software development industry, roles are typically defined based on the needs of a particular project or team. The purpose of a role is to provide structure and clarity around the specific responsibilities and expectations for an individual or group within a larger organization or project. Roles can be defined based on a variety of factors, including technical expertise, leadership ability, or functional area of expertise. A tech lead role may be defined based on the need for technical leadership and guidance within a software development team, while a Product Manager role may be defined based on the need for strategic planning and decision-making related to a particular product or project. A well-defined role that is aligned with the goals and objectives of a project or team can provide clarity and direction for team members, while also enabling effective collaboration and communication.

The first known definition for a tech lead role is: “a senior software developer responsible for designing and developing complex software solutions” [1]. Definitely, we can approve that a technical lead is a senior leading role for a software engineer. A tech lead is a decision maker and is necessary in bigger companies where the roles and skills are not easily interchangeable. Tech leads are responsible for ensuring that all team members comprehend and adhere to critical technical decisions. They establish programming guidelines, the most frequently used libraries, and technologies. Additionally, they play a managerial role, guiding the team with company values and helping to resolve conflicts. Tech leads must also comprehend customer needs and prioritize work accordingly [2].

A team may have one tech lead or separate ones for the back-end and front-end. The position is typically filled by the person with the most development expertise, and it's more of a leadership role than a formal title. Depending on the project, the role can be rotated among different team members, but each project should have at least one designated tech lead [2].

The short definition can be: “a tech lead is a senior software engineer responsible for leading a team and hands-on alignment of the technical direction” [3].

The longer definition [2]: “A tech lead is a software engineer responsible for leading a team and alignment of the technical direction. To establish a strong technical direction, it is necessary to define a technical vision, address any technical disagreements, and oversee the technical quality of team deliverables. Successful technical leadership involves ensuring that the team utilizes suitable engineering practices, prioritizes ongoing improvements to the tooling and technical debt, and adapts the system to meet its evolving requirements and surroundings. A tech lead is also responsible for mentoring and coaching team members, as well as providing technical guidance and direction when needed.”

A tech lead is critical to the success of a typical software development team. The place of a tech lead within a typical software development team is at the forefront of technical decision-making. They are responsible for coordinating the work of the team members and providing guidance to them on technical matters. In this role, they serve as the main point of contact for other members of the team when they have technical questions or concerns. A tech lead also plays a key role in the software development process, from the planning stage to deployment. They work closely with other members of the team, including project managers, software developers, and quality assurance specialists, to ensure that the project is on track and that everyone is working toward the same goals and objectives.

Sometimes team leadership is shared but rarely technical leadership. A tech lead may co-lead a team with other roles like a product manager or a team lead. Where a product manager focuses on the “What“, a tech lead focuses on the “How.” Where a team lead focuses on “People and Team Growth“, a tech lead focuses on “Technical Growth” of team members and the system. The unique focus for a tech lead is leading the technical direction and quality for the team. They may also have added responsibilities depending on the specific team [3].

Leadership is shared between the three roles, but each provides a different focus. In this situation, the Tech Lead focuses more on the technical part. Their involvement in architecture discussions and decisions will increase. They will oversee and maintain the quality of the evolving codebase and the technical development of the team.

A tech lead should always consider his skills simultaneously in three dimensions: development, architecture and leadership [3]. Development - a tech lead's background should include experience as a developer to be effective. They need to possess the knowledge and expertise necessary to write quality code and assist their team with technical challenges, regardless of their area of expertise. Architecture - In addition to development, tech leads must have a comprehensive understanding of how the software integrates into a larger system. They should be knowledgeable about the deployment, management, and operation of software in a production environment. Leadership - a successful tech lead must possess strong leadership abilities, even if they are not responsible for direct line management.

Essential leadership skills such as coaching, influencing, and delegation are essential for achieving success.

Tech lead role expectations can vary across companies, projects, and teams [4]. These expectations may differ with respect to the level of direct and indirect contribution expected from the tech lead towards the codebase. It is important for the tech lead to have a clear understanding of the specific expectations for their role in order to effectively fulfill their responsibilities and ensure successful project outcomes. Additionally, regular communication with team members and project stakeholders can help ensure that expectations remain aligned and that the tech lead is able to effectively contribute to the project in the manner expected of them [5].

To balance the expectations related to direct and indirect contribution in the code base, it is recommended to adopt the following models. To accommodate the varying expectations and conditions of tech lead roles in different projects and teams, it is recommended to adopt a model that includes three variations based on the ratio of direct and indirect contribution. This allows for greater flexibility in meeting project and team expectations, while also balancing the technical and leadership responsibilities of the tech lead role.

There exist three models: technical expertise, technical guideline, and technical mission.

Model of technical expertise: indirect contribution - 0-30%. Sometimes, a tech lead may be brought in to handle specific technical challenges in a project or to manage a small team of 1-2 engineers. In this model, the focus should be on problem-solving rather than carrying out a lot of team activities.

Model of technical guideline: indirect contribution - 30-70%. The model is the most widely recognized and accepted one for the tech lead role. It aims to balance both technical and leadership activities for a team of 3-7 engineers. This model recognizes that the tech lead needs to be not only a technical expert but also a team player and a mentor. Therefore, the tech lead must find a balance between direct and indirect contributions, and between individual and team responsibilities. The success of this model largely depends on the tech lead's ability to prioritize tasks, manage time effectively, and communicate clearly and collaboratively with the team members. It is also recommended demonstrating flexibility and adaptability to the project's needs and constraints.

Model of technical mission: indirect contribution - 70-100%. The technical mission model is characterized by an absolute leadership role and is best suited for leading multiple medium-sized teams or a single large team with 8 or more engineers. In this model, the tech lead's focus should remain on technical aspects while creating a better infrastructure to achieve desired results. It is crucial to ensure that the team is aligned with the mission and objectives of the project. The tech lead should have excellent communication skills to effectively delegate responsibilities and monitor progress. Flexibility is also essential in this model as it may require adapting to rapidly changing circumstances.

In the agile development context, the choice of the tech lead model should align with the principles of agility, including flexibility, collaboration, and continuous improvement. The model should be chosen based on the project/team expectations and conditions, and the tech lead's strengths and weaknesses, in order to adapt to changing requirements and maximize team efficiency. It is important to find the right balance between technical and leadership responsibilities to ensure the success of the project and the team, while also promoting agile values such as self-organization and continuous learning. The tech lead should continuously evaluate and adjust their role in order to support the agile process and contribute to the team's success.

***References*:**

1. Gorlin, Jeffrey M. (1998). Defining the Technical Lead Role. Computerworld, 32(27), 93-94.

2. Tech Lead. 2019. URL: https://developerexperience.io/articles/tech-lead.

3. The Definition of a Tech Lead. 2020, Pat Kua. URL: https://www.patkua.com/blog/the-definition-of-a-tech-lead.

4. Dienhart, J. R. (2010). The Effective Technical Leader: An Essential Guide to Leadership for Technical Professionals. CRC Press.

6. Alshammari, M., & Aljohani, N. R. (2020). Challenges and solutions in remote software development teams. Journal of Software: Evolution and Process, 32(10), e2207.

Artem Kozlov

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

COMPETITION AS A METHOD OF CONFLICT RESOLUTION

Competition as a method of conflict resolution in a team: analysis, advantages and recommendations.

In today's IT industry, where dynamism and competitive environments are an integral part of daily work, conflict management is becoming a key aspect of successful team functioning. One approach that can be used to resolve conflict in teams is competition. In this scientific publication, we will analyze the role of competition in the context of team conflict resolution, consider the advantages of this approach and offer recommendations for its effective use.

Competition in an IT team can be defined as a competitive process in which participants strive to achieve better results, surpass each other and attract the attention of management or customers. Conflicts, on the other hand, arise from differences in opinions, interests, or goals among team members. However, competition can be used to overcome conflicts, create an incentive for growth and development, and improve productivity.

Competition in an IT team can have several positive aspects. First, it stimulates innovative thinking and creativity of team members. Competition encourages each team member to look for new and effective ways to accomplish a task, which promotes the development of new ideas and technical solutions.

Secondly, competition contributes to the development of professional skills and increasing competence. When team members see their successes and achievements being evaluated and compared to others, they are motivated to improve and learn to become better in their field. [1]

Competition can greatly influence the motivation of team members and increase their productivity. When there is competition in the team, each member strives to show the best result and surpass the others. This creates a healthy atmosphere of competition, which contributes to higher efficiency in the performance of tasks and achievement of goals.

Competition in the IT team stimulates innovative thinking and the search for new solutions. When team members compete with each other, they seek unconventional approaches and come up with new ideas to stand out and achieve better results. [2] This contributes to the development of new products, technologies and the improvement of work processes.

Competition in the IT team creates an incentive to improve the professional skills and competence of the participants. When each team member sees his or her achievements being evaluated and compared with others, he or she strives to improve his or her knowledge and skills in order to be competitive. This leads to

an increase in the level of professionalism in the team and contributes to its overall development.

Competition in an IT team can improve communication and cooperation. When team members compete with each other, they are forced to actively communicate, exchange information and ideas. This contributes to the development of communication skills and strengthening of interaction between colleagues. In addition, competition can stimulate cooperation within a team to achieve common goals.[3]

Competition in an IT team can help participants develop leadership qualities and management potential. In a competitive environment, each team member can show leadership skills, take initiative and lead others. In addition, competition requires effective management of resources and time, which contributes to the development of management and organizational skills.

To effectively use competition in a team, it is necessary to establish clear rules and goals. Each participant must understand that competition is a means to achieve common team goals, not a means of division or confrontation. Competition rules must be clear and fair to minimize the possibility of wrongdoing or conflict.

It is important to create an atmosphere of healthy competition where team members can compete on equal terms and be fairly evaluated. Team management should provide fair and objective criteria for evaluating success, and provide regular feedback and support to participants in their individual efforts.

It is important to conduct regular feedback and performance evaluation for team members. This will help them understand their strengths and weaknesses, identify areas for improvement and development. Feedback should be constructive and supportive to help participants grow and develop. [4]

Competition should not completely exclude teamwork. Although competition can be beneficial, it is important to encourage and support cooperation and teamwork. Team projects, joint tasks, and the sharing of experiences among participants can contribute to more effective use of competition and conflict resolution.

Competition in an IT team can be an effective way to resolve conflicts and stimulate the growth and development of members. Well-managed competition can foster innovation, develop professional skills, improve communication and cooperation, and develop leadership and management potential. However, it is necessary to establish clear rules, maintain fair and healthy competition, conduct regular feedback and performance evaluation, and encourage cooperation alongside competition. Using competition as a conflict resolution tool can lead to improved team effectiveness and success.

References:

1. *Bruce Tolgan , The Art of Being Indispensable at Work, 2020, p. 84.*
2. *Bruce Tolgan, It's Okay to Manage Your Boss, 2007, p. 75.*
3. *Tom DeMarco, Deadline. 1997, p.52.*
4. *Byron Sharp, How brands grow, 2010. P.71.*

Sergii Levchenko

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

HUMAN-ORIENTED COMPANY STRUCTURES IN THE ERA OF GLOBALIZATION

The theme of globalization is quite widely debated, drawing both supporters and opponents, each trying to support their own arguments as convincing. But regardless of what is claimed by supporters and opponents, globalization is already an ongoing process, and organizations cannot ignore it. Whether globalization is an advantage or a drawback for an organization, depending on the political and economic situation of the society in which it operates, the process itself cannot be ignored [1].

In the era of globalization, human-oriented company structures have become increasingly important as organizations recognize the significance of placing people at the center of their operations. These structures prioritize the well-being, development, and engagement of employees, considering them as valuable assets rather than just resources. Here are some key elements of human-oriented company structures in the context of globalization [2]:

1. Empowerment and Autonomy: Human-oriented companies empower employees by giving them a sense of ownership and autonomy over their work. They encourage individuals to take initiative, make decisions, and contribute their unique skills and perspectives. This fosters a culture of innovation, creativity, and continuous learning.

2. Flat Organizational Structures: Traditional hierarchical structures can impede communication, slow down decision-making, and limit individual contributions. Human-oriented companies often adopt flatter organizational structures, where there are fewer layers of management and more opportunities for collaboration and direct communication across the organization. This promotes agility, flexibility, and the free flow of information.

3. Focus on Work-Life Balance: Globalization has blurred the boundaries between work and personal life, often leading to increased stress and burnout. Human-oriented companies prioritize work-life balance by offering flexible work arrangements, promoting a healthy work environment, and encouraging employees to take time off for personal well-being. They recognize that a well-rested and fulfilled workforce is more productive and engaged.

4. Continuous Learning and Development: To thrive in a globalized world, companies need to adapt to rapidly evolving markets, technologies, and customer needs. Human-oriented organizations invest in the growth and development of their employees by providing opportunities for training, upskilling, and knowledge

sharing. They foster a culture of continuous learning and encourage employees to explore new ideas and acquire new competencies.

5. Diversity and Inclusion: Globalization brings together people from different cultural backgrounds, experiences, and perspectives. Human-oriented companies embrace diversity and inclusion, recognizing that it fuels innovation and enhances decision-making. They create inclusive environments where individuals feel valued, respected, and empowered to contribute their unique insights.

6. Purpose-Driven Approach: In the era of globalization, companies that prioritize their purpose beyond profit tend to attract and retain top talent. Human-oriented organizations have a clear sense of purpose that goes beyond financial success. They align their mission with societal and environmental goals, contributing to the well-being of communities and promoting sustainable practices.

7. Employee Well-being and Support: Human-oriented companies prioritize employee well-being by providing support systems and resources to address physical, mental, and emotional needs. They offer comprehensive benefits, promote work-life integration, and foster a culture of care and empathy. This approach helps create a supportive and healthy work environment where employees can thrive [3].

Human-oriented company structures in the era of globalization recognize the value of employees as essential contributors to the organization's success. By empowering individuals, fostering collaboration, promoting work-life balance, and prioritizing diversity, learning, and purpose, these structures enable companies to adapt and thrive in a rapidly changing global landscape.

In the first Global Information Technology Report published by the World Economic Forum in collaboration with INSEAD business school in 2002 [4], a close connection between the level of information technology (IT) development and the economic prosperity of countries was recognized. The report highlighted the pivotal role of IT in fostering innovation, increasing productivity, enhancing competitiveness, diversifying economies, and stimulating business activity, thereby contributing to an improved standard of living. Information technology has become one of the most crucial factors driving economic growth, and the IT sector itself has become a driving force in the global economy. Today, in many developed countries, the IT sector is rapidly evolving and serves as a catalyst for sustainable economic development, making a significant contribution to their GDP.

The Global Information Technology Report also provides a ranking of countries based on their readiness for a networked society. This readiness index comprises four components: environment, readiness, usage, and impact of information technologies. Each component encompasses several indicators that assess the political, regulatory, market, and innovation environment; the readiness of the population, businesses, and government bodies to adopt IT; the utilization of

IT by the population, businesses, and government bodies; and the economic and social impact of IT [5].

According to the World Economic Forum's Global Information Technology Report in 2014, digital information technologies have a direct correlation with economic growth and job creation. For instance, widespread adoption of digital information technologies in developing markets could potentially create over half a billion jobs in the next decade alone. Numerous studies have shown that new information technologies significantly influence all sectors of the economy, ranging from healthcare to agriculture.

Finland ranks first in the Global Information Technology Report due to its favorable business environment and one of the best education systems globally. Finland leads the world in the number of patent applications per capita in the field of IT, and 90% of Finnish households have Internet access. Overall, the Finnish economy is focused on maximizing the benefits derived from the use of new IT [6].

Countries in Northern Europe and the so-called "Asian tigers" (Singapore, Hong Kong, South Korea, and Taiwan) dominate the 2014 ranking due to their creation of a favorable business environment, investment climate, highly skilled workforce, and other factors conducive to the adoption of IT.

Globalization has brought about significant changes in economic, political, and cultural landscapes, leading to the resurgence of local identities in various regions. Organizations face new pressures to expand into new markets to survive as economic and national borders dissolve. To navigate this globalized environment, organizational culture plays a crucial role. US multinational companies, for example, have shifted from having international divisions to adopting a more "global" approach. Similarly, European multinational companies, due to smaller domestic markets and historical colonial legacies, are also seeking to become more international.

Globalization has facilitated the spread of ideas, attitudes, and cultural elements across borders while simultaneously generating new economic, political, and cultural demands in different regions. Some organizations rely on a small number of local branches staffed by foreign employees, highlighting their openness to globalization through a multinational management team. Others use organizational culture to promote coordination and consistency.

To address the challenges of organizational culture in global integration, organizations need to pay attention to several factors:

1. Differentiation vs. Integration: Organizations must determine the extent to which their organizational culture can overcome national and cultural differences to create a global organization. They need to strike a balance between global practices and local preferences while striving for integration into a global entity.

2. Control vs. Autonomy: Using organizational culture as a control mechanism to ensure conformity can have unintended consequences.

Organizations should consider the delicate balance between control and autonomy, as overemphasis on conformity may limit individual initiative.

3. National vs. Corporations: The development of an international framework with frequent transfers can lead to a loss of identification with one's home community and family. Organizations should be cautious about creating a corporate culture that supersedes personal and cultural identities.

Globalization can bring about changes that are difficult to control, as interconnected systems are sensitive to the ripple effects of events. As organizations expand beyond their borders, it becomes essential to identify and address factors that may lead to conflicts. National and organizational cultural differences can act as barriers to organizational development. However, gathering information and understanding the cultural contexts of new markets can help mitigate these barriers.

In summary, globalization necessitates organizations to carefully manage their organizational culture to navigate the challenges of global integration. Balancing differentiation and integration, control and autonomy, and national and corporate identities is crucial for success in a globalized world.

***References*:**

1. Mihaela Vlăsceanu, Organizaţii şi comportament organizaţional, (Iaşi: Polirom, 2003), 25-26.

2. Zygmunt Bauman, Globalizarea şi efectele ei sociale, (Bucharest: Antet, f.a.), 5.

3. Doina I. Popescu, Comportament organizaţional, (Bucharest: ASE, 2010), 109.

4. Doina I. Popescu, cit.ed., 110-112.

5. Brozhik L.L. The problem of integration to the light informational space of the warehouse of national politics / L.L. Brozhik // Ekonomichny chasopis-XXI. – 2010. – No3–4. – pp. 42-46.

7. The Global Information Technology Report 2014 [Electronic resource]. – Mode of access: http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf.

Anton Voronko

Student, Akademie HUSPOL s.r.o.
Kunovice, The Czech Republic

COMMON PRACTICES FOR AGILE PLANNING AS OVERCOMING OF THE OPTIMISTIC BIAS

One of the powerful shifts in management approaches influenced by Agile movement was empowering the team. We can find it both indirectly mentioned within agile principles (Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done. [1]) and explicitly stated in related literature [2, p. 5][3, pp. 119-120][4, p. 108]. Empowerment implies the sharing of the decision-making power with those who are actually doing the work. Historically in manufacturing industry, that triggered creation of the modern management approaches, all the authority was put on the manager who organized the work deconstructed to the smallest operations to be served by individual with no expertise. Unlike that, peculiarities of the IT industry, where agile movement takes its roots, relies on qualified workers, and therefore requires work-specific information for better decisions [3, p. 216]. The amount of that information is overwhelming for one person, like a manager, therefore its processing slows down or even makes impossible proper decisions.

Team's empowerment also implies that a team plans its work. But, alongside the specific domain knowledge, that team members possess, some systemic practices should be used. Otherwise, feeling the pressure of product owner and stakeholders, and having no group baseline for forecasting a team tends to fall into a trap of optimistic bias. This bias was observed by Daniel Kahneman and Amos Tversky and formulated as the phenomena of the underestimation of the possibility of the plan failing [5, p. 248]. Inability to create plans with relevant level of predictability causes micromanagement and higher pressure on a team, what in its turn diminishes trust and breaks the safety environment mandatory for team's self-organization.

To understand the complexity of that issue, we need to notice that at least 2 books are dedicated to that topic specifically: Planning Extreme Programming (2000) by Kent Beck and Martin Fowler, and Agile Estimating and Planning (2006) by Mike Cohn [6][7]. It shows that during many years community experimented with different practices trying to come up with valid toolkit for teams.

Daniel Kahneman in his book proposed the sequence of steps to make unbiased general prediction [5, p. 187]:

1. Start with an estimate of the average.
2. Determine the evidence of the deviation from the average.

3. Estimate the correlation between two values.
4. Adjust the average by the correlation.

If we will check the common practices for agile planning articulated by Mike Cohn [8], we'll find the reflection of the Kahneman's proposal:

1. Pick the average velocity.
2. Identify the team's availability.
3. Find the ratio between team's availability in a 'regular' sprint and the upcoming one.
4. Adjust the velocity by ration as baselining for planning.

If a team manages to achieve low volatility around average velocity, that approach will also support another agile principle that insists on a sustainable working pace (Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely) [1].

As follows, suggesting an agile team to use the systematic approach to agile planning based on the common practices instead of a 'gut feeling forecast' can help to reduce the impact of the optimistic bias and as a result improve team's predictability and stability of working pace. That, in general, leads to higher trust from the management side what may result in a better employee engagement and productivity. Since the proposed approach should be used as a baseline for planning only, it'll not influence team's empowering in a negative way and will serve as introduction to the deeper discussion about actual plan which may have deviations from baseline if team accepts that.

***References*:**

1. Principles behind the Agile Manifesto. Retrieved June 4, 2023. https://agilemanifesto.org/principles.html

2. Ken Schwaber & Jeff Sutherland. The Scrum Guide. 2020.

3. Jim Highsmith. Agile Software Development Ecosystems. Indianapolis, 2002.

4. Roman Pichler. Agile Product Management with Scrum. 2010.

5. Daniel Kahneman. Thinking Fast and Slow. New York, 2011.

6. Kent Beck and Martin Fowler. Extreme Programming Planning. 2000.

7. Mike Cohn. Agile Estimating and Planning. 2006.

8. Mike Cohn. Three Approaches to Estimating the Impact of Holidays and Time Off on Velocity. Retrieved June 4, 2023. https://www.mountaingoatsoftware.com/blog/three-approaches-to-estimating-impact-of-holidays-and-time-off-on-velocity

УПРАВЛІННЯ ПЕРСОНАЛОМ

Бобылев А. В.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ОПЕРАЦИОННЫЙ МЕНЕДЖМЕНТ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ

Целью данной научной статьи является исследование роли операционного менеджмента в торговой компании для повышения эффективности.

В данной статье рассматриваются преимущества операционного менеджмента в торговых компаниях, в том числе совершенствование управления цепочками поставок, снижение затрат и повышение удовлетворенности клиентов. В статье также исследуются проблемы внедрения операционного менеджмента в торговых компаниях и предлагаются стратегии преодоления этих проблем.

Операционный менеджмент играет решающую роль в успехе торговых компаний. Операционный менеджмент включает в себя процессы планирования, организации и контроля ресурсов для достижения бизнес-целей. Операционный менеджмент в торговых компаниях включает в себя управление цепочкой поставок, запасами, логистикой и обслуживанием клиентов. Целью данной научной статьи является изучение роли операционного менеджмента в торговых компаниях и того, как его можно использовать в качестве инструмента повышения эффективности.

Преимущества операционного менеджмента в торговых компаниях

Улучшение управления цепочками поставок. Операционный менеджмент может улучшить управление цепочками поставок в торговых компаниях за счет оптимизации процессов, снижения уровня запасов и повышения прозрачности. Это может привести к экономии средств, сокращению сроков доставки и повышению удовлетворенности клиентов.

Сокращение затрат: Операционный менеджмент также может снизить затраты в торговых компаниях за счет оптимизации процессов и сокращения потерь. Это может привести к экономии средств, которую можно передать клиентам или использовать для повышения прибыльности.

Повышение удовлетворенности клиентов: операционный менеджмент может повысить удовлетворенность клиентов, гарантируя, что продукты будут доставлены вовремя, в хорошем состоянии и по правильной цене. Это может привести к повышению лояльности клиентов и повторным сделкам.

Проблемы внедрения операционного управления в торговых компаниях

Сопротивление изменениям. Одной из самых больших проблем при внедрении операционного менеджмента в торговых компаниях является сопротивление изменениям. Сотрудники могут сопротивляться изменениям в процессах или процедурах, особенно если они работают в компании долгое время.

Недостаток ресурсов. Еще одной проблемой является нехватка ресурсов для эффективного внедрения операционного менеджмента. Сюда входят затраты на обучение сотрудников, инвестиции в технологии и найм экспертов для управления процессами.

Проблемы координации. Торговые компании часто имеют сложные цепочки поставок, включающие множество поставщиков, дистрибьюторов и поставщиков логистических услуг. Это может привести к проблемам координации, с которыми может быть сложно эффективно справиться.

Стратегии преодоления трудностей внедрения операционного менеджмента в торговых компаниях

Коммуникация: Эффективная коммуникация необходима для преодоления сопротивления изменениям. Торговые компании должны сообщать своим сотрудникам о преимуществах операционного менеджмента и предоставлять им надлежащее обучение и поддержку для участия в этом процессе.

Распределение ресурсов: торговые компании должны выделять достаточные ресурсы для эффективного осуществления операционного менеджмента. Это включает в себя инвестиции в технологии, найм экспертов и обучение сотрудников.

Сотрудничество: торговые компании должны сотрудничать со своими поставщиками, дистрибьюторами и поставщиками логистических услуг, чтобы обеспечить эффективное управление цепочкой поставок. Для этого требуется четкая коммуникация, общие цели и регулярный мониторинг эффективности.

Операционный менеджмент является важнейшим инструментом торговых компаний для повышения эффективности и достижения бизнес-целей. Несмотря на трудности внедрения операционного менеджмента, торговые компании могут решить эти проблемы, сообщая о преимуществах, выделяя достаточные ресурсы и сотрудничая с партнерами по цепочке поставок. Инвестируя в операционный менеджмент, торговые компании могут улучшить управление цепочками поставок, снизить затраты и повысить удовлетворенность клиентов, что приведет к повышению конкурентоспособности и прибыльности.

Список использованных источников:

1. Chopra, S., & Meindl, P. (2016). Supply chain management: Strategy, planning, and operation. Pearson.

2. Chase, R. B., Jacobs, F. R., & Aquilano, N. J. (2018). Operations management for competitive advantage. McGraw-Hill.

3. Heizer, J., & Render, B. (2016). Operations management: Sustainability and supply chain management. Pearson.

4. Krajewski, L. J., & Ritzman, L. P. (2018). Operations management: Processes and supply chains. Pearson.

5. Lambert, D. M., & Cooper, M. C. (2014). Issues in supply chain management. Industrial marketing management, 23(1), 3-13.

6. *Lee, H. L. (2018). The triple-A supply chain. Harvard business review, 82(10), 102-112.*

Ковальчук Д. А.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ЕФЕКТИВНЕ УПРАВЛІННЯ ТАЛАНТАМИ У СУЧАСНІЙ ОРГАНІЗАЦІЇ

Управління талантами є ключовим елементом успіху сучасних організацій. В епоху постійних змін і гострої конкуренції, компанії все більше розуміють важливість залучення, розвитку та утримання найкращих працівників. Ефективне управління цими працівниками відіграє вирішальну роль у забезпеченні конкурентної переваги та стійкого розвитку організаційного потенціалу.

Сучасні організації розуміють, що таланти - це не просто працівники, а люди з унікальними здібностями, знаннями та навичками, які можуть принести значний внесок у розвиток бізнесу та розширення його потенціалу. Стратегічне планування кадрів стає необхідністю для ідентифікації, розвитку та розміщення цих цінних ресурсів у правильних місцях.

Одним з ключових аспектів ефективного управління талантами є процес рекрутингу та залучення цих працівників. Компанії повинні розробити стратегії, які дозволять їм залучати найкращі кадри на ринку праці. Інноваційні методи рекрутингу, такі як використання соціальних мереж та технологій, можуть допомогти привернути талановитих працівників із різних галузей.

Процес розвитку та утримання талантів також вимагає особливої уваги. Компанії повинні забезпечити неперервний розвиток своїх працівників, надавати їм можливості для професійного зростання та залучення до менторських програм. Крім того, створення гнучких систем компенсації та преміювання може стимулювати мотивацію людей і зберігати їх в компанії на довгостроковій основі.

Лідерство грає важливу роль у розвитку талантів. Керівники повинні бути свідомі своєї ролі у сприянні розвитку та мотивації працівників у своїй команді. Вони повинні давати поради, підтримувати, та створювати сприятливу корпоративну культуру, що сприяє розкриттю потенціалу кожного співробітника.

Розробка імплементації стратегії управління талантами для досягнення цілей організації

Це важливий етап для досягнення цілей організації. Стратегія визначає найефективніші способи виявлення, розвитку та утримання талантів, які забезпечать успішність і стійкість організації в довгостроковій перспективі.

Першим кроком у розробці стратегії є ретельний аналіз потреб організації та визначення цілей, які вона хоче досягти. Це можуть бути такі цілі, як забезпечення стабільного росту, збільшення конкурентоспроможності або створення інноваційного середовища. Наступним етапом є ідентифікація ключових компетенцій та навичок, необхідних для досягнення цих цілей.

Після аналізу організаційних потреб і ключових компетенцій важливо розробити план дій для виявлення та найму талантів. Це можуть бути заходи, які спрямовані на пошук талановитих кандидатів, використання соціальних мереж або залучення зовнішніх ресурсів для залучення нових талантів до організації.

Далі слід розробити програму розвитку та навчання для існуючих талантів, забезпечити їхню професійну та особистісну зрілість. Це може включати тренінги, менторські програми, можливості для отримання нових знань та навичок.

Нарешті, організація повинна розробити механізми збереження талантів, такі як гнучкі системи компенсації та преміювання, програми розвитку кар'єри та можливості для особистого зростання.

Розробка імплементації стратегії управління талантами є комплексним процесом, який вимагає уваги до деталей та глибокого розуміння потреб організації. Цей підхід дозволяє побудувати сильну команду талантів, яка сприятиме досягненню цілей організації та стане основою її успіху.

Впровадження сучасних підходів до оцінки та розподілу потенціалу співробітників

Впровадження сучасних підходів до оцінки та розподілу потенціалу співробітників є важливим елементом ефективного управління персоналом. Традиційні методи оцінки, такі як річні огляди та числові рейтинги, вже не відповідають сучасним вимогам організаційного середовища.

Сьогодні компанії все більше переходять до більш комплексних та індивідуалізованих підходів оцінки та розподілу потенціалу. Вони використовують методи, які засновані на виявленні навичок, здібностей та потенціалу співробітника, а не лише на його попередніх досягненнях. Наприклад, 360-градусний зворотній зв'язок, оцінка компетенцій, асесмент-центри та індивідуальні розмови.

Одним з ключових елементів сучасних підходів є здатність виявляти потенціал у співробітників та прогнозувати їхні можливості розвитку. Це може бути досягнуто за допомогою аналізу здібностей, оцінки особистісних характеристик та індивідуальних планів розвитку.

Крім того, впровадження сучасних підходів передбачає більш гнучкий та справедливий розподіл потенціалу. Замість традиційних систем ранжування і "декілька переможців", компанії все більше спрямовуються на командну співпрацю, розвиток всіх співробітників та створення рівних можливостей для розвитку.

Впровадження сучасних підходів до оцінки та розподілу потенціалу співробітників дозволяє організаціям залучати та розвивати найкращі таланти, сприяючи досягненню організаційних цілей та стимулюючи рост і продуктивність всієї команди.

Висновки і можливі шляхи застосування досліджень

Впровадження сучасних підходів до оцінки та розподілу потенціалу співробітників та розробки імплементації стратегії управління талантами є критично важливими аспектами успішного управління персоналом. Дослідження в цих областях надають цінні інсайти та рекомендації для організацій, які прагнуть досягти високої ефективності та стабільного розвитку.

Можливі шляхи застосування досліджень включають:

- Впровадження інноваційних методів оцінки та розподілу потенціалу співробітників, таких як 360-градусний зворотній зв'язок і оцінка компетенцій. Це дозволить компаніям отримати більш об'єктивну та повну картину професійних здібностей та потенціалу своїх співробітників.
- Розробка і впровадження індивідуальних планів розвитку для співробітників, що ґрунтуються на їхньому потенціалі та цілях організації. Це сприятиме підвищенню мотивації та залученості співробітників, а також сприятиме їхньому особистому та професійному зростанню.
- Створення системи постійного моніторингу та оцінки результатів реалізації стратегії управління талантами. Це дозволить організації вносити корективи та адаптувати стратегію для досягнення найкращих результатів.
- Підтримка культури інновацій та навчання в організації, що сприятиме створенню сприятливого середовища для розвитку талантів і просування новаторських ідей.

Застосування досліджень у цих напрямках дозволить організаціям залучати, розвивати та утримувати талановитих співробітників, що забезпечить їхню конкурентоспроможність і досягнення стратегічних цілей компанії.

Козырев С. С.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ПОЛИТИКА ОТНОШЕНИЙ РАБОТОДАТЕЛЕЙ И РАБОТНИКОВ НА ПРЕДПРИЯТИЯХ, В УЧРЕЖДЕНИЯХ, ОРГАНИЗАЦИЯХ

Работники и работодатели являются важнейшими субъектами рыночной экономики. Их отношения между собой построены таким образом, что с одной стороны они в силу экономических причин не могут существовать друг без друга, а с другой – им в то же время слишком сложно существовать между собой. Существование в одиночку вообще теряет для них свой смысл, поскольку цель работодателя состоит в осуществлении своей хозяйственной деятельности, направленной на выпуск определенной продукции, оказании услуг, то есть на работу предприятия для чего, собственно говоря, и было создано последнее. Понятно, что эта хозяйственная деятельность может быть проведена только с участием конкретных людей, потому что наличие производственных помещений, оборудования и всего прочего ничего не значит для работодателя без конкретных исполнителей. Учитывая это обстоятельство, работодатель вынужден использовать способность наемных работников к труду, чтобы обеспечить свое существование. С другой стороны, каждый человек имеет право на труд и может реализовать его в разных формах: предпринимательской деятельности, само занятости и т.д. Но в данном случае следует уточнить, что не все граждане способны заниматься предпринимательской деятельностью в силу личностной способности, таланта, ответственности, деловитости и других качеств. Большинство граждан реализует свое право на труд путем заключения именно трудового договора на предприятиях, в учреждениях, организациях независимо от форм собственности или работая по трудовому договору у работодателя – физического лица. Это не значит, что работа по трудовому договору на предприятии менее ответственна, не является творческой, но она по своему содержанию абсолютна другая, потому что несамостоятельна и заключается в подчинении работника, при исполнении своих трудовых обязанностей, правилам внутреннего распорядка работодателя. Учитывая изложенное, считаю, что отношения между работниками и работодателями должны быть толерантными. На толерантные отношения работодателей и работников ориентированы отдельные международно-правовые документы. Так, в п.п. 1. п. 2 Рекомендаций по связям между администрацией и работниками на предприятии, утвержденных Генеральной Конференции Международной Организации Труда № 129 от 28 июня 1967 г. (далее Рекомендация № 129)

указано, что предприниматели и их организации, а также работники и их организации должны в своих общих интересах признать важность атмосферы взаимопонимания и доверия на предприятии, которая благоприятна как для эффективной деятельности предприятия, так и для работников. Создание такой атмосферы должно облегчаться путем быстрого распространения и обмена более полной и объективной информацией из разных аспектов жизни предприятия и социальных условий работников (п.п. 2 п. 2). С целью создания такой атмосферы администрация должна после консультации с представителями работников принять соответствующие меры по применению эффективной политики связей с работниками и их представителями (п.п. 3 п. 2). Далее подчеркивается, что эффективная политика связей должна обеспечивать такое положение, чтобы до принятия администрацией решения по важным вопросам об этом давалась информация и между заинтересованными сторонами проходили консультации, поскольку передача такой информации не наносит ущерба ни одной из сторон (п. 3). Отмечено также, что методы связей никак не должны нарушать свободу объединения; они никак не должны наносить ущерб свободно избранным представителям работников или их организациям или ограничивать функции органов, представляющих работников в соответствии с национальным законодательством (п.4). Представляет интерес вопросы элементов политики связей на предприятии. Любая политика связей должна быть приспособлена к типу данного предприятия с учетом его размера, состава и рабочей силы. Внимание обращается на то, что для достижения своей цели любая система связей на предприятии должна обеспечивать действительную и регулярную двустороннюю связь: между представителями администрации (руководитель предприятия, начальник цеха, мастер и т.д.) и работниками; и между руководителем предприятия, начальником отдела кадров или любым другим представителем высшего руководящего состава и представителями профсоюзов или другими лицами, на которых в соответствии с законодательством или коллективных договоров возложена задача представлять интересы работников на предприятии (п. 9). К средствам связи Рекомендация №129 предлагает отнести: совещания по обмену мнениями и информацией; сообщения, предназначенные для определенных групп работников (как, например, бюллетени мастеров и справочники по вопросам политики в области кадров); средства, целью которых дать работникам возможность вносить предложения и высказывать свое мнение по вопросам, касающимся деятельности предприятия (п. 13). Как видим, международная практика предлагает целый ряд способов и форму взаимоотношений работодателей и работников, направленных именно на развитие общих интересов, атмосферу взаимопонимания и доверия на предприятии. В Рекомендации МОТ по рассмотрению жалоб на предприятиях с целью их решения № 130 от 29 июня 1967 г. (далее Рекомендация № 130) также обращено внимание на то, что для осуществления здоровой политики в

области кадров и решения социальных вопросов, касающихся работников на предприятии, администрация должна до принятия решений сотрудничать с представителями работников. Хотя этот международный нормативно правовой документ посвящен порядку рассмотрения жалоб работников, хочу обратить особое внимание на термин «здоровая политика в области кадров». Что понимается под этим термином?

1. На мой взгляд, здоровая политика в области кадров – это толерантные отношения между работниками и администрацией предприятия, учреждения, организации. Это отношения, когда наемные работники хорошо осознают свое предназначение на предприятии, понимают цель и направление своей деятельности, а также для какой цели они находятся на работе и т.д. Важное значение для понимания «здоровой политики в области кадров», на мой взгляд, имеет кадровая политика, существующая на предприятии. Кадровую политику раскрывают через совокупность правил и норм, целей и представлений, определяющих направление и содержание работы с персоналом. Из-за кадровой политики осуществляется реализация целей и задач управления персоналом, поэтому ее считают ядром системы управления персоналом. Кадровая политика формируется руководством предприятия, реализуется кадровой службой в процессе выполнения ее работниками своих функций и поэтому ее целью, по моему мнению, является: соблюдение работниками своих прав и обязанностей, установленных Конституцией Украины, трудовым законодательством Украины, правилами внутреннего трудового распорядка предприятия; подчиненность всей работы с кадрами задачей бесперебойного и качественного обеспечения основной хозяйственной деятельности необходимым количеством работников, имеющих определенный уровень квалификационной подготовки; рациональное использование кадрового потенциала; формирование и поддержка работоспособных, дружных трудовых коллективов; разработка принципов организации трудового процесса, развитие внутрипроизводственной демократии; разработка критериев и методики подбора, отбора, обучения и расстановки квалифицированных кадров; подготовка и повышение квалификации работников и т.д.

2. Проявлением здоровой политики в области кадров в Украине считаю Закон Украины «О социальном диалоге в Украине» от 23 декабря 2010 г. Согласно ст. 1 социальный диалог - процесс определения и сближения позиций, достижение общих договоренностей и принятие согласованных решений сторонами социального диалога, представляющих интересы работников, работодателей и органов исполнительной власти, и органов местного самоуправления, по вопросам формирования и реализации государственной социальной и экономической политики, регулирования трудовых, социальных, экономических отношений. Формами социального

диалога являются: обмен информацией, консультации, согласительные процедуры, коллективные переговоры по заключению коллективных договоров и соглашений (ст.8). Как видим, законодатель, предлагая эти формы, направляет работников и представителей работодателей на сотрудничество между собой по всем вопросам, возникающим на предприятии с тем, чтобы эти отношения были толерантными, понятными, прозрачными, доступными.

3. Одним из примеров здоровой политики в области кадров в вопросах трудовой дисциплины, на мой взгляд, является распространенная в последнее время «положительная» дисциплинарная политика (ж-л Менеджер по персоналу, 2011, № 1). В чем ее сущность? Предлагается поощрять работников за более хорошее поведение, чем взыскивать за плохое. Специалисты считают, что сначала нужно выяснить, чего хотят руководители от своих подчиненных: страха и ненависти или трудового энтузиазма в сочетании с четкой исполнительной дисциплиной? И чтобы работники не допускали нарушений трудовой дисциплины, предложены следующие меры: установить понятные и разумные правила, помогающие правильно организовать рабочий процесс и получать хорошие результаты; четко сконструировать правила поведения, должностные инструкции, стандарты обслуживания и регламенты работы; добиться соблюдения правил самими сотрудниками, набраться терпения: люди не механизмы, для перевоспитания нужно время.

4. В конце следует отметить, что здоровая политика в области кадров является неотъемлемым фактором взаимоотношений между работниками и работодателями. И здесь нужно понимать, что от того, как эти субъекты рыночной экономики построят отношения между собой, будет зависеть их существование в дальнейшем. Считаю, что здоровая политика в области кадров будет влиять на повышение производительности труда и моральное настроение трудового коллектива, будет способствовать хорошему нравственно-психологическому климату среди работающих, обеспечит комфортную обстановку трудящимся при выполнении ими задач, поставленных работодателем.

Список использованных источников:

1. Рекомендаций по связям между администрацией и работниками на предприятии, утвержденных Генеральной Конференцией Международной Организации Труда № 129 от 28 июня 1967 г.; ЗУ« О социальном диалоге в Украине» от 23 декабря 2010 г.; ж-л Менеджер по персоналу, 2011, № 1.

Разінков І. П.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

СУЩНОСТЬ, СТРУКТУРА И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ВОЕННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Стремление укрепить свою военную безопасность остается основой военной политики стран мирового сообщества. Основное содержание военной политики в этой сфере в рамках реализации соответствующих мероприятий включает: формирование и реализацию единой государственной политики в области военной безопасности; поддержание внутриполитической стабильности; защита конституционного строя, целостности и неприкосновенности национальной территории; развитие и укрепление дружественных отношений с соседними и другими государствами; создание и поддержание системы обороны страны на необходимом уровне; повышать боеспособность Вооруженных Сил, других войск, соединений и воинских частей и поддерживать в случае необходимости их готовность к согласованным действиям; защита важных объектов в различных областях и т. д. Вся эта деятельность направлена на поддержание и укрепление военной безопасности страны.

Военная безопасность - неотъемлемая, важнейшая составляющая национальной безопасности, определяющая состояние обороноспособности страны и ее способность обеспечивать защиту национальных интересов с помощью вооруженных сил [1, с. 93].

Военная безопасность характеризует способность государства предотвратить развязывание войны, участие в войне и, в случае войны, минимизировать ущерб и разрушительные последствия для национальной безопасности страны.

Для обеспечения военной безопасности страны необходимо иметь достаточный военный потенциал в непосредственной близости от государственной границы для самозащиты в случае кризиса. Необходимый уровень военной безопасности достигается благодаря решительным и согласованным усилиям государственных институтов при наличии всей совокупности структурных составляющих, как чисто военных, так и политико-дипломатических, экономических, идеологических и других.

Политико-дипломатическая составляющая военной безопасности отвечает за:

- высокий уровень (международной) системы коллективной безопасности;
- интеграция государства в систему военно-политических союзов;

- приемлемый баланс военно-политических сил в мире;
- гарантированное выполнение международных договоров и соглашений, в которых участвует та или иная страна;
- совершенствование международного режима контроля над вооружениями и нераспространения оружия массового уничтожения и средств его доставки.

Экономическая составляющая военной безопасности включает [5, с. 33]:

- финансовые возможности, обеспечивающие обороноспособность страны;
- количественные и качественные характеристики вооруженных сил и других войск;
- военно-промышленный комплекс, снабжающий армию, флот и другие войска всем необходимым, создает мобилизационный резерв вооружения и военной техники.
- научно-технический потенциал, позволяющий создавать новые виды вооружения и военной техники;
- мобилизационные возможности промышленности, обеспечивающие снабжение вооруженных сил и других войск требуемым количеством вооружения и военной техники в случае необходимости.

Военная составляющая включает военную организацию государства, созданную для обеспечения военной безопасности на основе военной силы.

Военная составляющая предполагает наличие определенных количественных и качественных показателей, среди которых [5, с. 3. 4]:

- обеспечение системами управления и обеспечения Вооруженных Сил, других войск, соединений и воинских формирований;
- уровень подготовки войск и вооруженных сил, от которого зависит их эффективность и боеготовность;
- техническое оснащение Бундесвера и других войск (военная техника, боеприпасы, военная техника);
- наличие запасов вооружения и военной техники в арсеналах, базах и складах;
- состояние военной инфраструктуры (стационарных объектов), предназначенных для подготовки войск (сил), стратегического и оперативного развертывания и боевых действий.

Морально-психологическая составляющая, тесно связанная с воинской составляющей, включает [5, с.36]:

- духовные возможности населения страны, которые определяются уровнем морально-психологической подготовки населения;
- общественный статус военнослужащих, представляющий собой совокупность их прав и обязанностей, положения и авторитета в обществе и государстве;

- морально-психологическое состояние основных категорий личного состава Вооруженных Сил и других войск.

Военная безопасность подразделяется на три уровня: глобальный, региональный и национальный.

К задачам военной политики относятся: определение возможности, необходимости и пределов применения военной силы для обеспечения военной безопасности; оценка качественных и количественных характеристик необходимых и достаточных вооруженных сил; определять пути и средства применения военной силы для обеспечения военной безопасности и, в случае необходимости, применения силы против вероятного противника.

Военная политика стран обычно ставит задачу создания системы обеспечения военной безопасности, которая позволит оценить внешние и внутренние военные угрозы безопасности и определить соотношение военных и невоенных средств обеспечения военной безопасности. Особое место в обеспечении военной безопасности отводится созданию, укреплению и совершенствованию военной организации государства, а также поддержанию военной мощи государства на уровне, обеспечивающем современное раскрытие, эффективное сдерживание и отражение агрессии.

Важное место должны занимать создание мобилизационной базы и обеспечение готовности органов государственной власти, хозяйства, транспорта и связи к решению задач обеспечения военной безопасности, определение задач и приоритетных направлений военно-экономического обеспечения военной безопасности. . Направления развития военной инфраструктуры предназначены для поддержания готовности вооруженных сил и других войск в мирное время и обеспечения выполнения задач в военное время, а также задач вооруженных сил и других войск по подавлению и отражению агрессии против стран, выявлять и нейтрализовывать антиконституционные акты, угрожающие территориальной целостности и государственному суверенитету страны, а также методы ведения вооруженной борьбы.

Основными задачами военной политики по обеспечению военной безопасности страны являются:

- определяют возможности, необходимость и пределы применения военной силы для обеспечения военной безопасности;

- оценка качественных и количественных характеристик необходимой и достаточной военной силы, определение способов применения военной силы для обеспечения военной безопасности и, в случае необходимости, применения военной силы против вероятного противника;

- обоснование и разработка военно-политических решений;

- разработка конкретных планов функционирования и развития военной системы государства;

- регулирование военно-политических отношений с другими государствами, коалициями, блоками;

- организация информационного обеспечения боевых решений, планов и операций;

- руководство военным строительством в целом, в частности строительством вооруженных сил, связанным с созданием военного потенциала страны;

- осуществлять военно-политические действия различных видов и масштабов на территории государства и на международном уровне, обеспечивая координацию действий с союзными войсками;

- решительное сопротивление противнику в случае возникновения конфликта, затрагивающего национальные интересы государства.

Концепция национальной безопасности государства определяет основные направления внешнеполитических действий по обеспечению его военной безопасности. Среди них следующие:

- проводить активную внешнюю политику;

- укрепить ключевые механизмы многостороннего управления глобальными политическими и экономическими процессами, прежде всего под эгидой Совета Безопасности ООН;

- полноправное участие государства в глобальных и региональных экономических и политических структурах;

- помощь в разрешении конфликтов, в том числе миротворческая деятельность под эгидой ООН и других международных организаций;

- добиваться прогресса в области контроля над ядерными вооружениями, поддержания стратегической стабильности в мире на основе соблюдения государствами международных обязательств в этой области;

- выполнение взаимных обязательств по сокращению и ликвидации оружия массового поражения.

Список использованных источников:

1. Алёшин А. А. 70 лет НАТО: Прежняя стратегия, новые разногласия. Год планеты: экономика, политика, безопасность. Ежегодник. М.: Идея-Пресс, 2020. С. 91-99.

2. Ананьева Е.В. Брекзит: предыстория и причины. Международная жизнь. 2018. № 2. С. 22-35.

3. Антюшин С.С. Военная безопасность как фактор стабильности общества (социально-философская концепция). М.: ВУ, 2004. 86 с.

4. Бабынина Л.О. Великобритания и ЕС: перспективы сотрудничества. Современная Европа. 2021. № 4. С. 57-67.

5. Бельков, О.А. Духовные основы и факторы национальной безопасности. Безопасность России 2011. Экспертно-аналитическое обозрение. М.: Критерий, 2010. 343 с.

6. Борис Джонсон достиг с ЕС нового соглашения о брексите. Чем оно отличается от старого? URL: https://www.bbc.com/russian/news-50068000

7. Великобритания: эпоха реформ / под ред. А. А. Громыко. М. : Весь Мир, 2017. 536 с.

Ретізник А. В.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

ПРОБЛЕМИ В УПРАВЛІННІ ПЕРСОНАЛОМ ПІДПРИЄМСТВА В УМОВАХ КРИЗОВОЇ СИТУАЦІЇ

Антикризовий розвиток не означає повну відсутність криз, але передбачає наявність криз, які стають стимулом для успішного розвитку, з урахуванням інтересів людини [1]. Лише людина може визначати мету та інтереси. Саме люди є основою для виявлення криз і їх управління.

Ефективність управління персоналом в умовах кризи залежить від якісного виконання функцій, що охоплюють різні напрями діяльності, реалізація яких сприяє досягненню цілей і завдань управління персоналом в умовах кризи. Антикризове управління персоналом, як специфічна галузь менеджменту персоналу, досягає своєї ефективності завдяки загальним функціям управління персоналом: плануванню, мотивації, організації та контролю. Проте, ці управлінські функції потребують вдосконалення, щоб ефективно впроваджувати конкретні антикризові заходи, залежно від етапу розвитку кризи (передкризовий стан, шок, відступ, адаптація, оволодіння ситуацією) та цілей антикризового управління персоналом (запобігання кризових процесів у персональному складі або ліквідація та мінімізація наслідків). Проблеми, пов'язані з управлінням персоналом, зазвичай виникають через законсервований стан системи, тобто кризи персоналу не виникають спонтанно, а є наслідком системних кризових явищ у різних сферах розвитку підприємства, невідповідності результатів діяльності персоналу новим змінюваним умовам, що виникають у будь-якій з систем підприємства. Тому важливо визначити основні фактори, що можуть призвести до кризи управління персоналом. Причинами кризи персоналу можуть бути внутрішні та зовнішні фактори. До внутрішніх факторів варто віднести:

- в системі управління можуть виникати проблеми, такі як відсутність чіткої стратегії розвитку, недостатня якість функцій контролю, неузгодженість між рівнями та ланками управління, обмежена самостійність підрозділів та неефективна кадрова політика;
- організаційна криза на підприємстві може бути виявлена через такі ознаки: несумісність розвитку окремих підсистем в організації з змінами в зовнішньому середовищі, що призводить до конфліктів внутрішньої організації; виникнення кризи на циклічних етапах; застарілі підходи, форми та методи управління підприємством; незбалансованість структури персоналу; неприсутність або помилки у визначенні пріоритетів, цілей та

стратегії розвитку підприємства (відомі як стратегічні організаційні конфлікти).;

У той же час, виникнення криз персоналу нерозривно пов'язане з екстернальним середовищем, що означає, що зовнішні чинники мають суттєвий вплив на стан персоналу на конкретному підприємстві.

Зокрема, зовнішніми причинами криз персоналу є:

- фактори загальноекономічного характеру (економічні показники розвитку країни, інфляційний рівень, рівень прожиткового мінімуму, рівень безробіття);
- ринкові та інші групи факторів.

Дослідження даної проблеми на підприємствах дозволяє виділити ряд найбільш часто зустрічаються проблем у системі управління персоналом [2, с. 114-115]:

- Низька продуктивність праці;
- Висока плинність кадрів.
- Дефіцит кваліфікованого персоналу.
- Звільнення співробітників із компанії.
- Відсутність чіткого та раціонального розподілу функцій між працівниками, дублювання робіт.
- Надмірна чисельність персоналу, невідповідність його кваліфікаційної структури потребам підприємства.
- Відсутність мотивації персоналу.
- Відсутність ініціативи працівників.
- Надмірна жорсткість та ієрархічність організаційних структур.
- Монополізація інформації, повноважень та відповідальності в межах керівництва підприємства.
- Відсутність загальних для всього персоналу традицій та норм поведінки.
- Низька трудова дисципліна.
- Напружена емоційна атмосфера в колективі, пов’язана з критичною кількістю демотивуючих факторів на підприємстві та високою кількістю конфліктних ситуацій.

Недоліки існуючих елементів системи управління персоналом на підприємстві є головними причинами всіх зазначених проблем.

Деякими основними ознаками кризи персоналу на підприємстві є зменшення кількості робочих годин, часті конфлікти, надлишковий персонал, зниження продуктивності праці, збільшення плинності кадрів, недотримання вказівок керівництва та погіршення дисципліни. Відповідно до причин, що призводять до кризи персоналу, можна виділити кілька типів криз: криза ефективності праці, кадровий дефіцит, криза компетентності, криза мотивації, криза корпоративної культури та соціально-трудових відносин.

Криза ефективності персоналу є найбільш небезпечним видом кризи, оскільки її наявність сприяє розвитку організаційної кризи. Криза компетентності характеризується проблемами в ініціативності, навчанні та здобутті нових навичок персоналом підприємства. Кадровий голод відображається в недостатній кількості персоналу на будь-якому рівні управління, що призводить до зниження трудового потенціалу та продуктивності праці.

Список використаних джерел:

1. Василенко В. О. Антикризове управління підприємством : навч. посіб. К. : ентр навч. л-ри. 2005. 504 с.

2. Гуріна О. В., Кишковська О. Л., Скрипник К. М. Моделі і методи управління персоналом в умовах кризи. Ефективна економіка. 2019. № 12. DOI: 10.32702/2307-2105-2019.12.11.

Рильцов Є. Р.

Студент, Akademie HUSPOL s.r.o.
м. Куновіце, Чеська Республіка

УПРАВЛІННЯ КОМАНДОЮ ПРОДАЖІВ У СФЕРІ ОНЛАЙН РЕКЛАМИ: АНАЛІЗ ТА ОПТИМІЗАЦІЯ

У сучасних умовах економічної кризи в Україні, підприємства виявляють особливу потребу в ефективному управлінні маркетинговою діяльністю. Один з найбільш обіцяючих антикризових заходів, якими компанії можуть скористатися, є застосування комплексу маркетингових комунікацій, зокрема реклами. Різні види рекламних носіїв мають свою вартість та спрямованість на вплив на цільову аудиторію з метою вирішення комунікативних завдань. Розумне комбінування цих носіїв, з переходом від дорогих до більш економічних, дозволяє компаніям оперативно реагувати на ринкову ситуацію та перемагати в умовах конкуренції.

У сучасному цифровому світі, де онлайн реклама стала необхідним інструментом для просування продуктів і послуг, ефективне управління командою продажів є ключовим фактором успіху для підприємств. Команда продажів відіграє важливу роль у генерації доходу і розширенні клієнтської бази.

Команда продажів складається з групи осіб, які спеціалізуються на продажу продуктів та послуг компанії потенційним клієнтам. Вони відповідають за досягнення бізнес-цілей організації шляхом ефективного продажу продуктів, послуг або підписок. Не існує двох абсолютно однакових команд продажів. Розмір, цілі та корпоративна культура кожної команди визначаються специфічними потребами конкретної організації.

Команда продажів відіграє вирішальну роль у маркетингу продуктів і послуг компанії. Вони співпрацюють для укладання угод, збільшення доходів та побудови довгострокових відносин з клієнтами, з метою стимулювання повторних покупок і підтримки лояльності до бренду.

Управління командою продажів у сфері онлайн реклами має на меті забезпечити ефективне функціонування і досягнення поставлених цілей. Роль менеджера команди полягає в організації та керуванні процесом продажів, координації роботи команди та забезпеченні її успіху. Основні завдання управління командою продажів надано в таблиці 1.

Таблиця 1

Основні завдання управління командою продажів

№	Завдання	Опис
1	Формування ефективної команди	Рекрутинг та підбір кваліфікованих фахівців є першим кроком до успішної команди

		продажів. Важливо знаходити талановитих спеціалістів, які мають необхідні навички і відповідають цінностям організації.
2	Навчання та розвиток	Постійне навчання та розвиток команди допомагають вдосконалювати їхні навички і знання в сфері онлайн реклами. Менеджер повинен забезпечити доступ до навчальних ресурсів та тренінгів, щоб команда мала актуальні знання та навички.
3	Створення мотиваційної системи	Мотивація є важливим елементом успішної команди продажів. Менеджер повинен розробити мотиваційну систему, яка включає в себе винагороди, похвали та можливості кар'єрного росту. Це стимулює продуктивність команди та підтримує високий рівень мотивації.
4	Ефективне комунікування	Комунікація є ключовим фактором для успішного управління командою продажів. Менеджер повинен забезпечити відкриту та ефективну комунікацію всередині команди, злагодженість та зрозумілість усіх інструкцій та вказівок.

Отже, успішне управління командою продажів у сфері онлайн реклами вимагає системного підходу та впровадження ефективних стратегій. Враховуючи ці аспекти та забезпечуючи аналіз, оптимізацію та розвиток команди, управління командою продажів у сфері онлайн реклами може досягти високої продуктивності та успіху. Послідовне виконання завдань, які були визначені у таблиці 1, сприятиме зміцненню командного духу, підвищенню ефективності роботи та досягненню поставлених цілей.

Аналіз результатів є важливим етапом управління командою продажів. Це допомагає виявити ефективність рекламних кампаній, ідентифікувати сильні та слабкі сторони команди, а також виявити можливі проблеми та виклики. Для проведення аналізу необхідно зібрати та проаналізувати дані про продажі, конверсію, витрати на рекламу, вплив маркетингових каналів та інші показники. Це дозволить виявити успішні стратегії та ті, що потребують оптимізації. В сфері онлайн реклами доступні різноманітні інструменти аналітики, які допомагають відстежувати та аналізувати результати рекламних кампаній. Наприклад, за допомогою системи веб-аналітики можна відстежувати трафік, конверсію та поведінку відвідувачів на сайті. Це надає цінну інформацію про ефективність рекламних кампаній та дозволяє виявити області для оптимізації.

Оптимізація рекламних кампаній є необхідною для досягнення максимальної ефективності та результативності. Це включає в себе налаштування та вдосконалення рекламних стратегій, використання цільових аудиторій, підбір оптимальних каналів реклами, тестування та аналіз результаті виконання. Оптимізація рекламних кампаній базується на аналізі даних, зокрема результатів попередніх кампаній, клієнтських поведінкових моделей, конкурентного середовища та трендів у сфері реклами.

Одним з ключових аспектів оптимізації є впровадження А/Б тестування. Цей підхід дозволяє порівняти дві або більше версії рекламної кампанії з метою визначення найефективнішої. Шляхом тестування різних елементів, таких як заголовки, зображення, способи виклику до дії та цільові аудиторії, можна знайти оптимальні комбінації, які найкраще привертають увагу та залучають клієнтів.

Крім того, ефективність управління командою продажів можна покращити за допомогою впровадження системи керування відносинами з клієнтами (CRM). Ця система дозволяє збирати, аналізувати та використовувати дані про клієнтів для більш ефективного спілкування та персоналізації рекламних пропозицій. CRM також допомагає відстежувати клієнтські запити та пропозиції, покращує комунікацію в команді та замовниками, а також забезпечує збереження даних для подальшого аналізу та стратегічного планування.

Необхідно також забезпечити постійний моніторинг та оновлення ринкових трендів та інновацій у сфері онлайн реклами. Це включає в себе стеження за змінами в популярних платформах реклами, впровадження нових технологій та інструментів, а також аналіз конкурентного середовища. Світ онлайн реклами постійно змінюється, тому важливо бути в курсі останніх тенденцій і адаптуватись до нових можливостей.

Крім аналізу та оптимізації рекламних кампаній, успішне управління командою продажів також передбачає зосередження на розвитку та навичках команди. Важливо забезпечити належне навчання та підтримку членів команди, щоб вони були експертами в своїй галузі та могли ефективно працювати з клієнтами. Також потрібно створити мотивуючу робочу атмосферу, де співробітники почуваються задоволеними та залученими до досягнення спільних цілей.

Управління командою продажів у сфері онлайн реклами також потребує ефективного комунікаційного процесу. Регулярні зустрічі, обмін досвідом та звітність допомагають забезпечити прозорість та співпрацю всередині команди. Крім того, важливо встановити чіткі цілі та показники ефективності, які дозволять оцінювати досягнення команди та індивідуальних співробітників.

Управління командою продажів у сфері онлайн реклами вимагає систематичного підходу, використання стратегій та інструментів аналізу, оптимізації та ефективного управління. Ключовими елементами успішного

управління командою продажів є створення мотиваційної системи, ефективна комунікація, аналіз та оптимізація результатів.

Менеджер повинен визначити стратегічні цілі, розробити стратегії та тактики для досягнення цих цілей. Аналіз результатів команди допомагає виявити сильні та слабкі сторони, а також проблеми, з якими стикається команда. Застосування інструментів аналітики дозволяє відстежувати ефективність рекламних кампаній та вносити необхідні зміни для оптимізації.

Успішне управління командою продажів також передбачає впровадження стратегій управління, визначення ключових показників продажів, контроль та звітність, навчання та розвиток команди, заохочення та мотивацію, а також ефективну комунікацію та співпрацю всередині команди.

Урахування цих факторів допоможе менеджеру команди продажів у сфері онлайн реклами досягти високих результатів, покращити продуктивність команди та забезпечити успішні продажі. Необхідно постійно аналізувати, оптимізувати та адаптувати стратегії управління, оскільки сфера онлайн реклами постійно змінюється та розвивається.

Список використаних джерел:

1. Діброва Т. Г. Маркетингова політика комунікацій: стратегії, вітчизняна практика: навчальний посібник. Київ: Видавничий дім «Професіонал», 2009. 320 с.

2. Діброва Т. Г. Рекламний менеджмент: теорія і практика: підручник / Т. Г. Діброва, С. О. Солнцев, К. В. Бажеріна. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. – 300 с.

3. Команда продажів: способи мотивації та розвитку вашої команди продажів URL: https://businessyield.com/uk/business-strategies/sales-team/(дата звернення: 23.06.2023).

4. Система мотивації відділу продажів для підвищення ефективності URL: https://business.diia.gov.ua/cases/hr/sistema-motivacii-viddilu-prodaziv-dla-pidvisenna-efektivnosti (дата звернення: 23.06.2023).

Рильцов Р. Є.

Студент, Akademie HUSPOL s.r.o.,
м. Куновіце, Чеська Республіка

СТРАТЕГІЇ УПРАВЛІННЯ ПЕРСОНАЛОМ ТА ЇХ ВНЕСОК В УСПІХ ВІДДІЛУ ПРОДАЖІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В сучасному конкурентному світі успіх підприємства в багатьох випадках залежить від ефективності його відділу продажів. Особливо це стосується компаній, які спеціалізуються на продажу програмного забезпечення. Успіх в цій сфері вимагає не лише якісних продуктів, але й висококваліфікованого та мотивованого персоналу. Саме тому важливо розробити ефективні стратегії управління персоналом, які сприятимуть підвищенню продуктивності та досягненню успіху відділу продажів програмного забезпечення.

За визначенням В.Г. Щербака, стратегія управління персоналом виступає як пріоритетний напрямок дій, який має якісні і кількісні параметри і спрямований на досягнення довгострокових цілей у зовнішньому і внутрішньому середовищі підприємства. Ця стратегія необхідна для формування високопрофесійного, відповідального та згуртованого колективу, з урахуванням стратегічних цілей розвитку підприємства і його ресурсних можливостей [7, с. 49].

Розробка стратегії управління персоналом - це процес систематичного і обдуманого планування, що передбачає реалізацію стратегічних рішень. Мистецтво розробки стратегії управління персоналом полягає в здатності перетворити загальні підходи до управління персоналом на конкретні дії, спрямовані на досягнення високої ефективності використання трудового потенціалу персоналу [5, с. 29].

Розробка стратегії управління персоналом постає з потреби в динамічному розвитку і передбачає поетапне визначення мети, критеріїв та показників ефективності, обмежень, що впливають на функціонування системи управління персоналом, таких як фінансові, матеріальні та соціальні фактори, організаційна структура служби управління персоналом та взаємозв'язки системи підприємства з зовнішнім середовищем.

Основою розробки стратегії управління персоналом на підприємстві є визначення мети управління персоналом, яка полягає в досягненні оптимального складу персоналу з точки зору якісних та кількісних параметрів [1].

Формування стратегії управління персоналом може здійснюватися двома способами: "зверху-вниз" і "знизу-вверх". У випадку застосування стратегії "зверху-вниз", керівництво визначає загальну стратегію управління

персоналом, на основі якої розробляються плани для кожного підрозділу окремо. За стратегією "знизу-вверх" кожен підрозділ розробляє власну стратегію та плани заходів, які потім інтегруються в загальний план підприємства. Важливо також враховувати життєвий цикл підприємства та встановлювати пріоритети в роботі з персоналом на різних рівнях управління, щоб побудувати ефективну кадрову стратегію [3].

Однією з ключових стратегій управління персоналом є рекрутинг та підбір кваліфікованих кадрів. Відповідно до потреб компанії, необхідно знайти талановитих фахівців, які мають не лише необхідні технічні навички, але й відповідають цінностям та корпоративної культурі організації. Ретельний відбір кандидатів забезпечує формування сильної команди, готової до викликів та досягнення високих результатів.

Після формування команди необхідно надати співробітникам необхідні навички та знання для ефективної роботи відділу продажів. Навчання та розвиток персоналу є ще однією важливою стратегією управління персоналом. Це можуть бути тренінги, семінари, онлайн-курси або інші форми навчання, спрямовані на підвищення навичок у продажах, взаємодії з клієнтами, управління відносинами та використання продажових інструментів. Це дозволяє співробітникам вдосконалювати свої вміння, підвищувати ефективність та досягати поставлених цілей.

Однак, не менш важливою є мотивація персоналу. Стратегії мотивації сприяють створенню стимулів для співробітників до досягнення високих результатів. Це можуть бути фінансові стимули, премії, бонуси, але також важливо враховувати інші аспекти, такі як можливість професійного зростання, розвитку кар'єри, визнання досягнень та створення комфортних умов роботи. Мотивований персонал більш схильний до активних продажів, більш залучений до своєї роботи та сприяє підвищенню продуктивності відділу продажів [4].

Крім того, стратегії комунікації є ключовим елементом управління персоналом відділу продажів програмного забезпечення. Ефективна комунікація між керівництвом та співробітниками, а також між співробітниками самого відділу, забезпечує взаєморозуміння, обмін ідеями та інформацією, вирішення проблем та швидке реагування на зміни. Регулярні наради, звіти, відкритий діалог сприяють побудові ефективної комунікаційної системи, що сприяє зміцненню командного духу та співпраці між співробітниками [2].

Створення сприятливої робочої атмосфери та забезпечення необхідних ресурсів також є важливою стратегією управління персоналом, що внесе значний внесок у успіх відділу продажів програмного забезпечення. Сприяти здоровій робочій атмосфері, встановленню робочих процесів та процедур, які спрощують роботу співробітників, та забезпеченню необхідного обладнання та інфраструктури допомагає зберегти високу мотивацію співробітників та підтримувати їх ефективність.

Окрім цього, ефективне управління персоналом передбачає також визначення та оцінку результатів роботи співробітників. Система зворотного зв'язку, встановлення цілей та об'єктивних критеріїв оцінки допомагають відстежувати прогрес та виявляти можливість для вдосконалення. Регулярні огляди роботи, фідбек та надання рекомендацій сприяють розвитку співробітників та підтримці їхнього професійного зростання [6].

Нарешті, стратегії управління персоналом повинні бути гнучкими та адаптованими до змінних умов та вимог ринку програмного забезпечення. Врахування нових технологій, трендів у сфері продажів, а також зміни потреб клієнтів є ключовими факторами успіху. Управління персоналом має бути готове до змін, швидко адаптуватись та впроваджувати інновації, що дозволить відділу продажів програмного забезпечення бути конкурентоспроможним та досягати високих результатів у постійно змінному середовищі.

Стратегії управління персоналом грають вирішальну роль у досягненні успіху відділу продажів програмного забезпечення. Рекрутинг та підбір кваліфікованих кадрів, навчання та розвиток персоналу, мотивація співробітників, ефективна комунікація, створення сприятливої робочої атмосфери, оцінка результатів роботи та гнучкість в управлінні - це лише кілька стратегій, які можуть бути застосовані для підвищення ефективності відділу продажів програмного забезпечення.

Зрозуміло, що кожна компанія має свої особливості та контекст, тому вибір конкретних стратегій управління персоналом повинен враховувати індивідуальні потреби та цілі підприємства. Проте, загальний підхід до ефективного управління персоналом може бути корисним для будь-якої компанії, що має відділ продажів програмного забезпечення.

Управління персоналом вимагає системного підходу та постійного вдосконалення. Використання стратегій управління персоналом допоможе створити сильну команду, забезпечити розвиток та мотивацію співробітників, поліпшити комунікацію та досягти успіху відділу продажів програмного забезпечення.

Отже, важливо постійно оцінювати потреби та вимоги відділу продажів, впроваджувати стратегії управління персоналом, адаптувати їх до змін у сфері програмного забезпечення та ринкових умов. Лише таким шляхом компанії будуть мати можливість досягати успіху, витримуючи випробування конкуренції та реалізуючи свій потенціал на повну силу.

Список використаних джерел:

1. Балабанова Л.В. Стратегічне управління персоналом підприємства в умовах ринкової економіки: монографія /Л.В. Балабанова, О.В. Стельмашенко. — Донецьк: [Дон НУЕТ], 2010. – 238 с.

2. Делія О. Ефективна комунікація в управлінні персоналом / О. Делія // Соціально-економічні проблеми і держава. – 2018. – Вип. 1 (6). – С. 36-40.

3. Козенков Д.Є. Стратегічне управління персоналом промислового підприємства: монографія / Д.Є. Козенков, А.В. Крамаренко, М.К. Вишневська, Т.В. Альошина // – Дніпро: Поліграфцентр «Формат», 2022. – 116 с.

4. Колот А. М. Мотивація персоналу: підручник / А. М. Колот, С.О. Цимбалюк // –К.: КНЕУ, 2016. 397 с.

5. Крушельницька О.В. Управління персоналом / О. В. Крушельницька, Д. П. Мельничук. – К.: Кондор, 2016. – 453 с

6. Савченко В.А. Управління розвитком персоналу підприємства / В. А. Савченко. – К.: КНЕУ, 2016. – 388 с.

7. Щербак В.Г. Управління персоналом підприємства / В. Г. Щербак. – Харків: Вид-во «ІНЖЕК», 2017. – 482 с.

Салиенко А. А.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ЛОЯЛЬНОСТЬ ПЕРСОНАЛА IT КОМПАНИЙ

В современных условиях определение факторов лояльности персонала IT компаний играет решающую роль для их дальнейшего развития и перспективности в будущем. Ключевой задачей HR-менеджера IT компании является создание неизменного, стабильного состава компетентных и высококвалифицированных работников, которые полностью идентифицируют себя с компанией, имеют профессиональную мотивацию на достижение общих корпоративных целей и способны отстаивать, защищать интересы своей компании. Увольнение специалистов или их переход в другую IT компанию, может повлечь за собой материальные убытки и потерю статуса компании на рынке труда. Все это требует сосредоточения и усилий компании для сохранения внутреннего кадрового ресурса и потенциала посредством построения правильной стратегии лояльности персонала. Таким образом, IT компания, имеющая целью существовать долгосрочно и выживать среди конкурентов, должна заботиться о состоянии лояльности персонала. Так как лояльность персонала – это не что иное, как залог устойчивого развития компании и уменьшение рисков, связанных с персоналом.

Изучением феномена лояльности персонала занимаются как зарубежные, так и отечественные ученые. Теоретические основы изучения феномена лояльности персонала отражены в трудах таких зарубежных ученых, как: М. Армстронга, Н. Аллена, Г. Беккера, Р. Бейрона, Дж. Гринберга, Дж. Мейера, П. Морроу, Л. Портера, Д. П. Шульца, С. Е. Шульц и других. Отечественными учеными, в контексте своей проблематики, изучаются различные аспекты лояльности персонала: сущность понятия «лояльность персонала» (Д. С. Батарчук, А. Г. Иванова, Н. Е. Иванова, К. В. Харский, Н. Ю. Челенкова); типы лояльности персонала (И. Грабская, А. В. Соловейчик, Ю. Н Харланова); организационная лояльность (С. С. Баранская, В. И. Доминяк, В. В. Смирнова); факторы, влияющие на уровень лояльности персонала (С. Горностаев, О. Н. Демушина, Н. В. Кузнецова, Е. А. Петрова, О. В. Сардак, А. А. Чумакова, А. И. Якушева) и другие.

Для определения уровня лояльности персонала используют такие методики: «Организационной лояльности» Дж. Майер и Н. Аллен [3]; опросник организационной лояльности Л. Портера «Organizational Commitment Questionnaire» (OCQ) [1]; методику оценки лояльности К. В. Харського «Лист наблюдения проявления лояльности» [4] и другие.

В научном дискурсе сегодня существует большое количество подходов к изучению лояльности персонала. Наиболее распространенным подходом к рассмотрению лояльности персонала является подход с точки зрения безопасности организации. Данный подход предполагает, что сотрудники изначально нелояльны к своей компании, поэтому лояльность персонала определяется как «поведение сотрудника, который не наносит ущерб своей организации» [5, с. 278].

Следующий подход – поведенческий. Одним из представителей этого подхода был Говард Беккер. Согласно этому подходу, лояльность персонала – это «готовность сотрудника продолжать работу в компании, желание сохранять принадлежность к компании» [2, с. 24].

Представители установочного подхода выдвигают концепцию установочной лояльности, которая включает в себя эмоциональную составляющую, а именно речь идет об эмоциональном отношении сотрудника к компании. Лояльность проявляется как эмоциональная реакция, включающая заботу и беспокойство за компанию и коллег, чувство присоединения, доверия. Представитель этого подхода Лиман Портер считает, что лояльный сотрудник, это сотрудник который действует в интересах компании, имеет желание продолжать работать в данной компании, принимает ценности компании [2, с. 24].

Таким образом, ознакомившись со всеми подходами к определению понятия лояльности персонала, можем сделать следующий вывод. Лояльность персонала – это такие сотрудники компании, которые разделяют ее цели и ценности, имеют желание строить свою карьеру именно в этой компании, в которой работают, идентифицируют себя с компанией и определяют себя как члена единственной большой семьи. На формирование высокого уровня лояльности персонала оказывают влияние организационные факторы (наличие системы вознаграждений, стиль управления, условия труда, интересное содержание работы) и личностные факторы (возможность самореализации, возраст и опыт работы, карьерный рост).

По результатам опроса сотрудников мировых компаний исследователи сделали вывод, что компании с высоко лояльным персоналом за три года принесли акционерам 112% прибыли; компании, имеющие средний уровень лояльности – 90%; компании, имеющие минимальный уровень лояльности персонала – всего 76%. Таким образом, исследователи подтвердили гипотезу, что «лояльные сотрудники» в 90% случаев готовы рекомендовать свою компанию другим, как достойное место работы, а в 55% опрошенных способны отклонить предложение работы от других работодателей [6]. Основываясь на результатах эмпирического исследования, можем сделать вывод, что лояльность персонала в IT компаний – это самое главное направление кадрового менеджмента.

Список использованных источников:

1. *Диагностическая методика «Опросник организационной лояльности» (OCQ) Л. Портера. URL: https://dominyak.com/methods/ocq.php (дата обращения: 04.03.2023).*

2. *Иванова Н. Е. Лояльность персонала как феномен. Научный вестник ЮИМ. 2019. № 2. С. 23–28.*

3. *Методика «Шкала организационной лояльности» Дж. Мейєр, Н. Аллен. URL: https://sites.google.com/site/test300m/ocs93 (дата обращения: 04.03.2023).*

4. *Методика оценки лояльности К. В. Харського. URL: https://hr-portal.ru/tool/metodika-ocenki-loyalnosti (дата обращения: 04.03.2023).*

5. *Челенкова Н. Ю. Лояльность сотрудников как способ повышения эффективности управления персоналом организации. Международный научный журнал «Инновационная наука». 2015. № 11. С. 277–281.*

6. *WorkUSA 2000: employee commitment and the bottom line: study of employee attitudes and opinions. Bethesda, MD : Watson Wyatt Worldwide, 12 p.*

Соколов Д. С.

Студент, Akademie HUSPOL s.r.o.
г. Куновице, Чешская Республика

ТЕХНОЛОГИИ КРОССКУЛЬТУРНОГО МЕНЕДЖМЕНТА МЕЖДУНАРОДНЫХ КОРПОРАЦИЙ

Каждому предприятию свойственна кросскультура, оказывающая влияние на его деятельность. В наше время, особенно когда происходит интенсивный переход к рыночной экономике, развитие научно -технического прогресса, потребность в понимании сущности и значение корпоративной культуры является приоритетным фактором развития предприятия. Прежде чем бездумно перенимать опыт ситуативно успешного зарубежного предприятия, следует упомянуть, что необходимо, в первую очередь, уважать себя и свою культуру.

Эффективное развитие культуры на предприятии возможно при условии налаживания процесса ее формирования. Поэтому процесс формирования культуры приводит как последовательность определения ценностей культуры, формирование поведения работников, осуществление эффективной деятельности предприятия и обеспечение интересов всех участников деятельности предприятия.

Учитывая необходимость постоянного усовершенствования культуры, целесообразно процесс формирования культуры предприятия, постоянно совершенствовать и поддерживать, что позволит менеджерам оценить влияние культуры на показатели деятельности организации и сделать выводы о значительном влиянии данной категории на деятельность, что в свою очередь докажет необходимость применения норм культуры.

В условиях усиления конкуренции и повышения эффективности ведения предпринимательской деятельности наблюдается рост интереса менеджеров к культуре и основных факторов, способных оказывать влияние на нее. Необходимость исследования данных факторов можно обосновать, определив влияние культуры на систему управления предприятием. Так, используя модель «7S», консалтингового предприятия General Electrics – МакКинси, можно отметить, что культура находится в неразрывной связи с основными элементами менеджмента в организации и оказывает влияние на них. И, учитывая, это можно утверждать, что уровень культуры зависит от составляющих системы управления.

Данная модель показывает, что кросскультура оказывает значимое влияние на систему управления и одновременно зависит от нее. Каждый элемент культуры динамично изменяется и развивается под влиянием многих факторов, способных обеспечить достаточно высокий уровень

кросскультуры. Следовательно, возникает необходимость исследовать влияние различных факторов на кросскультуру и на основе исследований уточнить классификацию факторов влияния на кросскультуру.

Соблюдение основных ценностей культуры руководителями высшего уровня управления является примером для руководителей управленческого уровня, и так вплоть до сотрудников. То есть культура должна проявляться не только в отделах кадров и работы с персоналом, но и на всех уровнях управления. Практика хозяйствования и зарубежный опыт свидетельствуют о том, что основные ценности должны передаваться в нисходящем порядке.

То есть руководители институционального уровня определяют основную цель функционирования предприятия. При этом в основе берутся именно ценности культуры (личные ценности руководителей и ценности предприятия). Они же определяют инструменты, посредством которых происходит формирование, развитие и направление кросскультуры менеджерам управленческого и технического уровня. А те, в свою очередь, всем остальным работникам. Так происходит развитие кросскультуры, то есть реализуются главные ценности, правила и нормы, обеспечивающие порядок в деятельности служащих.

Бесспорным аргументом роли руководства в развитии культуры является то, что только руководители имеют достаточные полномочия для создания и развития корпоративной культуры. Руководители показывают нормы корпоративной культуры, которых они ожидают от подчиненных. Однако одновременно с этим руководители должны прислушиваться к подчиненным, ценить, воплощать в практику их идеи, поскольку они являются основой корпоративной культуры. Руководители должны постоянно демонстрировать культуру, потому что это делает ее понятной для окружающих. Принятие решений обязательно должно производиться с учетом норм корпоративной культуры. Руководство всегда должно помнить о кодексе корпоративного поведения.

Руководители должны учитывать возможности своих подчиненных, поскольку часты случаи, когда задачи, которые ставит руководитель, недостижимы для подчиненных. Во избежание таких ситуаций менеджерам необходимо развивать кросскультуру.

Руководители не только формируют культуру, но постоянно совершенствуют, развивают ее и поддерживают ее жизнедеятельность. Примеры следования нормам корпоративной культуры со стороны руководителей обязывают работников соблюдать установленный порядок. На предприятии обязательно должны быть руководители, жестко контролирующие соблюдение корпоративного поведения. Ведь в случае их отсутствия может возникнуть ситуация, когда культура угаснет. Руководители, четко формирующие корпоративную культуру, в первую очередь должны сосредоточить внимание на совершенствовании своих

профессиональных навыков, влияющих на корпоративную культуру. Они должны прежде всего:

- уметь разделять личные цели и цели предприятия;
- четко формировать миссию и целые предприятия;
- постоянно заниматься самосовершенствованием и саморазвитием;
- эффективно осуществлять управление коллективом работников;
- рационально использовать власть;
- умело разрешать конфликтные ситуации.

Бесспорно, эти рекомендации базовые. Каждый руководитель должен сам выбирать, что развивать и совершенствовать в первую очередь, и это зависит от типа корпоративной культуры, поскольку корпоративная культура другая для каждого предприятия. Для поддержки корпоративной культуры на высоком уровне менеджеры должны развивать свои профессиональные, деловые, административные, организационные, моральные и социальные качества. Они должны умело делегировать полномочия, мотивировать работников и наряду с этим обеспечивать осуществление эффективного контроля. Именно менеджеры формируют корпоративную культуру. Поэтому при оценке фактора управленческого воздействия необходимо учитывать их квалификацию, профессиональные навыки; соотношение между их количеством и количеством работников; их текучесть за определенный период. Это позволит устранить неэффективные старые правила поведения, поскольку увольнения таких руководителей, которые придерживаются старых правил поведения и не желают внедрять, новые будут примером для работников.

Список использованных источников:

1. Алексєєва Т. І., Гончарук К. О. Міжнародні відносини між країнами Люблінського трикутника – новий формат співпраці крізь призму історичного минулого. Держава та регіони. Сер. Економіка та підприємництво. 2021. № 2. С. 11-14.

2. Баннікова К., Михайльова К. Потенціал організаційної культури в управлінні людськими ресурсами міжнародних компаній : монографія. Харків : Вид-во НУА, 2019. 231 с.

3. Глінковська Б., Чеботарьов Є., Чеботарьов В. Кроскультурні підприємницькі комунікації : навчальнометодичний посібник. Старобільськ, 2018. 120 с.

CONTENT

GREETINGS

Mgr. Pavel Polián 3

Ігор Копотун 4

КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНЕ-ВИКОНАВЧЕ ПРАВО; КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ 5

Mgr. Pavel Polián 5

THE CHARACTERISTIC OF EXEMPTION FROM CRIMINAL LIABILITY FOR CORRUPTION CRIMES 5

Копотун І. М. 10

ОСОБЛИВОСТІ НАДЗВИЧАЙНИХ ПОДІЙ КРИМІНАЛЬНОГО ХАРАКТЕРУ У КРИМІНАЛЬНО-ВИКОНАВЧИХ УСТАНОВАХ 10

Агаркова О. І. 14

ТАКТИКА ОГЛЯДУ МІСЦЯ ПОДІЇ ПІД ЧАС РОЗСЛІДУВАННЯ НЕЗАКОННОЇ ПОРУБКИ АБО НЕЗАКОННОГО ПЕРЕВЕЗЕННЯ, ЗБЕРІГАННЯ, ЗБУТУ ЛІСУ В УКРАЇНІ 14

Акімов М. О. 18

ЧИ ВДОСКОНАЛЕНА КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КАТУВАННЯ: АБО ДЕЯКІ ПРОБЛЕМИ ЗАКОНУ УКРАЇНИ ВІД 01 ГРУДНЯ 2022 РОКУ № 2812-IX 18

Рудик М. М. 22

МЕХАНІЗМ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ КРИМІНОЛОГІЧНОЇ ПОЛІТИКИ У СФЕРІ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ ТА ЕКСПЛУАТАЦІЇ АВТОМОБІЛЬНОГО ТРАНСПОРТУ 22

Моісеєв М. Г. 26

ЗАГАЛЬНІ АСПЕКТИ ОСОБИ ЗЛОЧИНЦЯ ПРИ НЕЗАКОННОМУ ВТРУЧАННІ В РОБОТУ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ І УСТАНОВАХ СИСТЕМИ ПРАВОСУДДЯ 26

ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА; ІСТОРІЯ ПОЛІТИЧНИХ І ПРАВОВИХ УЧЕНЬ; ДЕРЖАВНЕ УПРАВЛІННЯ; ПОЛІТОЛОГІЯ; ФІЛОСОФІЯ ПРАВА 30

Дорошенко Т. В. 30

ВПЛИВ ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ НА СУЧАСНІ КОНФЛІКТИ 30

Лясота А. Є 34

ІНСТИТУЦІЙНІ ВИКЛИКИ ТРАНСФОРМАЦІЇ ПОЛІТИЧНОЇ СИСТЕМИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ 34

КОНСТИТУЦІЙНЕ ПРАВО; МУНІЦИПАЛЬНЕ ПРАВО; ЦИВІЛЬНЕ ПРАВО І ЦИВІЛЬНИЙ ПРОЦЕС; СІМЕЙНЕ ПРАВО; МІЖНАРОДНЕ ПРИВАТНЕ ПРАВО 39

Рижук І. В. 39

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНДИВІДУАЛЬНОЇ КОНСТИТУЦІЙНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ НАРОДНИХ ДЕПУТАТІВ 39

ЗЕМЕЛЬНЕ ПРАВО; АГРАРНЕ ПРАВО; ЕКОЛОГІЧНЕ ПРАВО; ПРИРОДОРЕСУРСНЕ ПРАВО 44

Бєлєвцев Ю. В. 44

ЗЕМЕЛЬНЕ ПРАВО В СУЧАСНІЙ УКРАЇНІ 44

МІЖНАРОДНЕ ПРАВО 46

Рудецька П. А. 46

ДЕЯКІ ПИТАННЯ ЩОДО ДОМАШНЬОГО НАСИЛЬСТВА: ДОСВІД ЗАРУБІЖНИХ КРАЇН В НАЦІОНАЛЬНЕ ПОЛЕ УКРАЇНИ 46

Shevchenko - Ledyan Cristina 49

CURRENT ENVIRONMENTAL LAW IN THE EUROPEAN UNION: THE LEGAL ASPECT 49

Shevchenko - Ledyan Cristina 52

STUDY OF THE LEGAL MEANS OF IMPLEMENTING ENVIRONMENTAL POLICY IN SPAIN 52

НАЦІОНАЛЬНА БЕЗПЕКА; ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА; ДЕРЖАВНА БЕЗПЕКА; ЕКОНОМІЧНА БЕЗПЕКА 55

Абрамов А. В. 55

РОЗВИТОК КВАНТОВИХ ОБЧИСЛЕНЬ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ 55

Биндич В. В. **58**
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ КЛАСИФІКАЦІЇ ДАНИХ В ХМАРНИХ СХОВИЩАХ **58**
Воробьев И. О. **61**
ВЛИЯНИЕ КИБЕРАТАК НА БЕЗОПАСНОСТЬ ГОСУДАРСТВА И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ КИБЕРВОЙНЕ **61**
Гаврилюк В. С. **65**
ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ **65**
Грішко Д. Ю. **69**
ІНСТРУМЕНТИ ТА ВИМІРЮВАННЯ ДОТРИМАННЯ ВИМОГ GDPR ДЛЯ МАЛИХ ТЕХНОЛОГІЧНИХ КОМПАНІЙ **69**
Кучерук А. С. **73**
РОЛЬ LEAN-МЕНЕДЖМЕНТУ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ДЕРЖАВНОЇ ІНФОРМАЦІЇ **73**
Мацько В. А. **76**
КІБЕРБЕЗПЕКА ТА КІБЕРРИЗИКИ RFID СИСТЕМ **76**
Медвідь І. А. **80**
ІНФОРМАЦІЙНА БЕЗПЕКА ПРИ РОБОТІ З НЕРЕГЛАМЕНТОВАНИМИ ЗАПИТАМИ ДО БАЗИ ДАНИХ **80**
Науменко П. С. **85**
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ **85**
Нікітін Д. О. **91**
СУЧАСНА КІБЕРБЕЗПЕКА **91**
Романюк О. П. **94**
ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА **94**
Dmytro Barsukov **96**
LEVERAGING LARGE LANGUAGE MODELS (LLMS) FOR THREAT INTELLIGENCE: ENHANCING CYBER THREAT DETECTION AND ANALYSIS **96**
Kostiantyn Chapistrak **100**
6 STEPS TO SECURE SMALL BUSINESS NETWORKS **100**
Maksym Kozachenko **104**
THE TRANSFORMATIVE IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBERSECURITY **104**

Viktor Moskvych **106**
SECURITY WITH CLOUD SERVICES **106**
Oleksii Nechytailo **110**
A GENERAL APPROACH TO THE STEGANALYSIS METHODS USAGE 110
Maksym Proniaiev **112**
INFORMATION AND CYBER SECURITY IN RELATION TO MODERN NATIONAL SECURITY **112**
Maksym Protsenko **115**
INCORPORATING PRIVACY BY DESIGN: ENHANCING DATA PROTECTION IN TECHNOLOGY SOLUTIONS **115**
Mykola Radahuz **118**
USAGE OF CELLULAR AUTOMATA IN CYBER SECURITY **118**
Ihor Roid **122**
INCIDENT MANAGEMENT IN SCOPE OF ENTERPRISE INFORMATION SECUTIRY **122**
Yaroslav Veselovskyi **127**
POST-QUANTUM CRYPTOGRAPHY, LATTICE-BASED **127**

ПСИХОЛОГІЯ; ПЕДАГОГІКА (в т. ч. ФІЛОЛОГІЯ) **130**
Шутяк І. А. **130**
НЕВЕРБАЛЬНІ ЗАСОБИ СПІЛКУВАННЯ ТА ЇХ КЛАСИФІКАЦІЯ **130**

ЕКОНОМІКА **133**
Білодід В. В. **133**
СУЧАСНІ НАПРЯМКИ РОЗВИТКУ ПРОЦЕСУ УПРАВЛІННЯ ЛАНЦЮЖКІВ ПОСТАВОК ТА ЛОГІСТИЧНИХ ОПЕРАЦІЙ У ВИРОБНИЦТВІ **133**
Плющ А. В. **140**
ЛОГИСТИЧЕСКИЕ КОНЦЕПЦИИ УПРАВЛЕНИЯ ЗАПАСАМИ ПРЕДПРИЯТИЙ УКРАИНЫ В ВОЕННОЕ ВРЕМЯ **140**
Ромнов А. И. **144**
ОБЗОР ТЕХНОЛОГИИ БЛОКЧЕЙН И ЕЕ ПОТЕНЦИАЛЬНОЕ ИСПОЛЬЗОВАНИЕ В ЛОГИСТИКЕ И ТРАНСПОРТЕ **144**
Aleksandr Denysiuk **146**
PRINCIPLES OF BANK MANAGEMENT IN WARTIME (ON THE EXAMPLE OF UKRAINE) **146**

Eduard Dushynskyi **149**
DEVELOPMENT AND APPLICATION OF ALTERNATIVE ENERGY SYSTEMS **149**
Yevhenii Tyrsyna **151**
PARTICULARITY OF USING THE PERSONAL MANAGEMENT SYSTEM IN A TRADING ENTERPRISE **151**
Artem Zghurskyi **155**
TODAY'S CHALLENGES OF SCALING UP A FAST-GROWING START-UP **155**

ФІЛОСОФІЯ **160**
Кононенко Т. В. **160**
КУЛЬТУРА В КОНТЕКСТІ ОБҐРУНТУВАННЯ РОСІЙСЬКОЇ ВОЄННОЇ АГРЕСІЇ **160**

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ПРИКЛАДНА ІНФОРМАТИКА **164**
Абаровський С. С. **164**
ПРОБЛЕМИ ВІДДАЛЕНОГО УПРАВЛІННЯ ІТ У МУЛЬТИКУЛЬТУРНИХ ТА МУЛЬТИЗОНАЛЬНИХ ВІРТУАЛЬНИХ КОМАНДАХ **164**
Веретюк О. М. **169**
Веретюк С. М. **169**
НОВІ ТЕНДЕНЦІЇ В РОЗГОРТАННІ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ: 5G, LPWAN ТА ХМАРНІ СЕРВІСИ **169**
Іванов М. О. **172**
ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МІКРОСЕРВІСНОЇ ТА МОНОЛІТНОЇ АРХІТЕКРУТИ ПРОЕКТІВ **172**
Курочка С. В. **176**
АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ПРОМИСЛОВОГО ПРОТОКОЛУ ЗВ'ЯЗКУ MODBUS В СИСТЕМІ РОЗУМНОГО БУДИНКУ В ПОРІВНЯННІ З ПОШИРЕНИМИ ПРОТОКОЛАМИ **176**
Трофименко О. В. **180**
АНАЛІЗ ПЕРЕВАГ І ОБМЕЖЕНЬ ВПРОВАДЖЕННЯ ШІ В УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ **180**
Roman Kryvenko **182**
ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING **182**

Yurii Maliuha **187**
MAIN CONCERNS DURING THE MIGRATION THE INFRASTRUCTURE OF THE EDUCATIONAL INSTITUTIONS TO CLOUD COMPUTING **187**
Mykhailo Morozov **192**
TRANSFORMING OPERATIONAL MANAGEMENT: HARNESSING THE POWER OF ARTIFICIAL INTELLIGENCE **192**
Pavlo Semehen **195**
CREATING A PRODUCT FULLY REMOTELY FROM SCRATCH **195**
Artur Stepashkin **199**
THE USE OF ARTIFICIAL INTELLIGENCE IN PRE-PRODUCTION **199**
Kyrylo Zinovyev **202**
ETHICAL AND SOCIETAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE **202**

МЕНЕДЖМЕНТ ТА МАРКЕТИНГ **206**
Абраменко Р. А. **206**
ПРАВОВАЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ **206**
Андрійчук Я. Р. **209**
ОРГАНІЗАЦІЯ ОПЕРАЦІЙНОЇ ДІЯЛЬНОСТІ БІЗНЕС-ОРГАНІЗАЦІЇ **209**
Басін А. О. **217**
АНАЛІЗ І ПОРІВНЯННЯ СУЧАСНИХ СЕРВІСІВ УПРАВЛІННЯ ІТ ПРОЄКТАМИ **217**
Белов М. С. **220**
ВЛИЯНИЕ ИНТЕРНЕТА И СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ НА ПОТРЕБИТЕЛЬСКОЕ ПОВЕДЕНИЕ В СОВРЕМЕННОМ ОБЩЕСТВЕ **220**
Богомаз А. С. **224**
ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНИХ ІНСТРУМЕНТІВ ПОБУДОВИ ОСОБИСТОГО БРЕНДУ **224**
Бурлака Ю. В. **228**
СТВОРЕНННЯ ТА РОЗВИТОК RESEARCH&DEVELOPMENT КОМАНДИ В РАМКАХ МАРКЕТПЛЕЙСУ PROM.UA **228**

Гремляцкий А. В. **232**
УЛУЧШЕНИЕ ЗАПАСА ФИНАНСОВОЙ ПРОЧНОСТИ КОМПАНИИ С ПОМОЩЬЮ АНАЛИЗА ТОЧКИ БЕЗУБЫТОЧНОСТИ **232**
Гуменюк Р. С. **236**
ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА МАШТАБОВАНИХ ФРЕЙМВОРКІВ ОРГАНІЗАЦІЇ РОБОЧИХ ПРОЦЕСІВ **236**
Димов В. В. **238**
АДАПТИВНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ МАЛОГО БИЗНЕСА **238**
Завгородный А. В. **241**
СРЕДСТВА ПРИВЛЕЧЕНИЯ И МОТИВАЦИИ СОТРУДНИКОВ В СОВРЕМЕННЫХ IT КОМПАНИЯХ ВО ВРЕМЯ ВЫНУЖДЕННОЙ УДАЛЕННОЙ РАБОТЫ **241**
Золотаренко А. О. **244**
ЗНАЧЕННЯ ТА ВАЖЛИВІСТЬ ПОБУДОВИ ЕКОНОМІЧНОЇ МОДЕЛІ РОЗВИТКУ КОМПАНІЇ **244**
Кирилко І. В. **249**
УПРАВЛІННЯ ПІДПРИЄМСТВОМ НА ЗАСАДАХ МАРКЕТИНГУ **249**
Коваленко В. В. **253**
РОЛЬ ИННОВАЦИОННЫХ МЕТОДОВ АНАЛИЗА В ПОВЫШЕНИИ КОНКУРЕНТОСПОСОБНОСТИ IT-КОМПАНИЙ **253**
Ковтуненко С. В. **256**
ПРЕДУПРЕЖДЕНИЕ ЭМОЦИОНАЛЬНОГО ВЫГОРАНИЯ В УПРАВЛЕНИИ МОТИВАЦИЕЙ ПЕРСОНАЛА **256**
Лупаненко А. Ю. **262**
МОДЕЛИРОВАНИЕ И СИМУЛЯЦИИ В ОПЕРАЦИОННОМ МЕНЕДЖМЕНТЕ **262**
Луцків Т. Р. **265**
ВИБІР МАРКЕТИНГОВИХ КОНТАКТІВ З ЦІЛЬОВОЮ АУДИТОРІЄЮ В ПОБУДОВІ ЕФЕКТИВНИХ РЕКЛАМНИХ КАМПАНІЙ **265**
Онишко В. О. **268**
ВСЕОСЯЖНА РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНОМУ МАРКЕТИНГУ ТА УПРАВЛІННІ **268**
Павлив Е. В. **270**
ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ БИЗНЕС-ПРОЦЕССАМИ **270**

Петрунь А. **273**
СУЩНОСТЬ И ЗНАЧЕНИЕ ИННОВАЦИЙ КАК ОСНОВЫ КОНКУРЕНТНОГО РАЗВИТИЯ ПРЕДПРИЯТИЯ **273**
Сердюк М. А. **275**
PR ОСНОВНОЙ КОМПОНЕНТ МАРКЕТИНГОВЫХ КОММУНИКАЦИЙ: ФУНКЦИИ, ЗАДАЧИ **275**
Топчій О. Д. **278**
ПЕРЕВАГИ ВПРОВАДЖЕННЯ ІНТЕРНЕТ-МАРКЕТИНГУ ТА ЙОГО ІНСТРУМЕНТАРІЙ ДЛЯ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА НА РИНКУ НЕРУХОМОСТІ **278**
Чорний С. С. **281**
ЛИДЕРСЬКІ ТА ПРОФЕСІЙНІ ЯКОСТІ ОПЕРАЦІЙНОГО МЕНЕДЖЕРА **281**
Ievgenii Doroshenko **284**
OVERCOMING COMMON MARKETING CHALLENGES IN THE IT INDUSTRY **284**
Stanislav Fedorenko **288**
THE IMPORTANCE OF ENGAGEMENT MODEL AND WORKFORCE STRATEGY FOR BUILDING A DELIVERY TEAM IN IT OUTSOURCING **288**
Vitalii Ivanov **293**
THE ROLE OF TECH LEAD IN MODERN REMOTE AGILE DEVELOPMENT TEAMS: FINDING THE RIGHT PLACE AND ACHIEVING BALANCE **293**
Artem Kozlov **297**
COMPETITION AS A METHOD OF CONFLICT RESOLUTION **297**
Sergii Levchenko **299**
HUMAN-ORIENTED COMPANY STRUCTURES IN THE ERA OF GLOBALIZATION **299**
Anton Voronko **303**
COMMON PRACTICES FOR AGILE PLANNING AS OVERCOMING OF THE OPTIMISTIC BIAS **303**

УПРАВЛІННЯ ПЕРСОНАЛОМ **305**
Бобылев А. В. **305**
ОПЕРАЦИОННЫЙ МЕНЕДЖМЕНТ КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ **305**

Ковальчук Д. А. 308
ЕФЕКТИВНЕ УПРАВЛІННЯ ТАЛАНТАМИ У СУЧАСНІЙ ОРГАНІЗАЦІЇ 308
Козырев С. С. 311
ПОЛИТИКА ОТНОШЕНИЙ РАБОТОДАТЕЛЕЙ И РАБОТНИКОВ НА ПРЕДПРИЯТИЯХ, В УЧРЕЖДЕНИЯХ, ОРГАНИЗАЦИЯХ 311
Разінков І. П. 315
СУЩНОСТЬ, СТРУКТУРА И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ВОЕННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА 315
Ретізник А. В. 319
ПРОБЛЕМИ В УПРАВЛІННІ ПЕРСОНАЛОМ ПІДПРИЄМСТВА В УМОВАХ КРИЗОВОЇ СИТУАЦІЇ 319
Рильцов Є. Р. 322
УПРАВЛІННЯ КОМАНДОЮ ПРОДАЖІВ У СФЕРІ ОНЛАЙН РЕКЛАМИ: АНАЛІЗ ТА ОПТИМІЗАЦІЯ 322
Рильцов Р. Є. 326
СТРАТЕГІЇ УПРАВЛІННЯ ПЕРСОНАЛОМ ТА ЇХ ВНЕСОК В УСПІХ ВІДДІЛУ ПРОДАЖІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 326
Салиенко А. А. 330
ЛОЯЛЬНОСТЬ ПЕРСОНАЛА IT КОМПАНИЙ 330
Соколов Д. С. 333
ТЕХНОЛОГИИ КРОССКУЛЬТУРНОГО МЕНЕДЖМЕНТА МЕЖДУНАРОДНЫХ КОРПОРАЦИЙ 333

Scientific publication

SCIENTIFIC PROGRESS: INNOVATIONS AND ACHIEVEMENTS

COLLECTION OF ABSTRACTS
International scientific-practical conference
(Kunovice, Czech Republic, June 29-30, 2023)

НАУКОВИЙ ПРОГРЕС: ІННОВАЦІЇ ТА ДОСЯГНЕННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ
Міжнародна науково-практична конференція
(Куновіце, Чеська Республіка, 29-30 червня 2023 року)

Under the editorship of I. Kopotun, S. Petkov, P. Polián

Signed for printing 04.07.2023
Press: Tiskárna Grafema, s.r.o., Hranice, Česká republika

Дизайн обкладинки *Тетяна Кандиба*
Технічний керівник *Юрій Кандиба*

Підп. до друку 04.07.2023. Формат 60x90/8
Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 5263 від 20.12.2016.

Виготовлювач «ФОП Кандиба Т. П.»
Вул. Незалежності, 16, м. Бровари, 07400
Тел.: 067 231-02-86