Akademie HUSPOL

SCIENTIFIC ACHIEVEMENTS OF MODERN SOCIETY

COLLECTION OF ABSTRACTS

International scientific-practical conference
(Kunovice, Czech Republic, March 17-18, 2023)

НАУКОВІ ДОСЯГНЕННЯ СУЧАСНОГО СУСПІЛЬСТВА

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

Міжнародна науково-практична конференція
(Куновіце, Чеська Республіка, 17-18 березня 2023 року)

Akademie HUSPOL

Kunovice, 2023

Akademie HUSPOL

SCIENTIFIC ACHIEVEMENTS OF MODERN SOCIETY

COLLECTION OF ABSTRACTS
International scientific-practical conference
(Kunovice, Czech Republic, March 17-18, 2023)

НАУКОВІ ДОСЯГНЕННЯ СУЧАСНОГО СУСПІЛЬСТВА

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ
Міжнародна науково-практична конференція
(Куновіце, Чеська Республіка, 17-18 березня 2023 року)

Kunovice 2023

Recommended for publication
by the Academic Council at
Akademie HUSPOL
March 30, 2023 (Protocol № 18)

Scientific achievements of modern society: collection of abstracts of International scientific-practical conference, Kunovice, Czech Republic, March 17-18, 2023. Kunovice : Akademie HUSPOL, 2023. 342 p.

Наукові досягнення сучасного суспільства: зб. матеріалів Міжнар. наук.-практ. конф., м. Куновіце, Чеська Республіка 17-18 березня 2023 р. Куновіце : Академія ГУСПОЛ, 2023. 342 с.

ISBN 978-80-7314-404-3

The collection of abstracts contains the reports of participants of the International scientific-practical conference "Scientific achievements of modern society", which was held by the Akademie HUSPOL (Czech Republic) together with the State Tax University (Ukraine) with the assistance of the NGO "European Institute for Further Education" on March 17-18, 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 "Vědecké výsledky moderní společnosti", kterou pořádala Akademie HUSPOL (Česká republika) společně se Státní daňovou univerzitou (Ukrajina) za asistence nevládní organizace „Evropský institut postgraduálního vzdělávání“ 17-18.3.2023. 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 «Наукові досягнення сучасного суспільства», яка була проведена Академією ГУСПОЛ (Чеська Республіка) спільно з Державним податковим університетом (Україна) за сприянням ГО «Європейський інститут післядипломної освіти» 17-18 березня 2023 року. Конференцію присвячено розв’язанню актуальних проблем в забезпеченні інноваційного розвитку та пошуку шляхів удосконалення правової практики України та Чехії.

ISBN 978-80-7314-404-3

©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 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

НАДЗВИЧАЙНІ ПОДІЇ 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.*

Рудик М. М.

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

ОСОБЛИВОСТІ ЗАПОБІГАННЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ У СФЕРІ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ ТА ЕКСПЛУАТАЦІЇ ТРАНСПОРТУ В УКРАЇНІ

Нині складно уявити життя без автомобільного транспорту, адже автомобілі стали не лише предметом розкоші, вони перетворилися на об'єктивну необхідність. Про це яскраво свідчить статистика. Наприклад, порівняно з 2000-ми роками кількість машин на автошляхах України зросла майже в чотири рази. Крім того, йдеться про суттєве збільшення швидкості сучасного автотранспорту і появі значної кількості недосвідчених водіїв. Усе вказане в сукупності призвело до істотного збільшення кількості ДТП в Україні, а отже, до зростання рівня смертності (особливо серед молоді віком від 20 до 35 років). Такі, масштабні наслідки ДТП, а також відсутність сталого прогресу в справі їх профілактики (спорадичні успіхи на цій ниві завжди є нестабільними та швидкоплинними) зумовлюють постановку питання про побудову державної стратегії безпеки дорожнього руху (БДР), котра ґрунтуватиметься на засадах науковості, обґрунтованості, послідовності, безперервності, соціальної спрямованості, економічної доцільності. Ця задача передбачає розробку широкого спектру правових, організаційних, інформаційних та інших заходів, спрямованих на радикальне зменшення кількості ДТП й рівня дорожнього травматизму в довгостроковій перспективі. Але найпершим кроком до окресленої мети повинно стати забезпечення плідного наукового підґрунтя. Як свідчить практика, без точних розрахунків, достовірних прогнозів, інноваційних методик і теоретичних напрацювань неможливо ні виробити ефективну систему дій, ані створити надійний механізм їхньої реалізації.

Сьогодні, коли питання розробки стратегії БДР нарешті почало переходити в практичну площину, постає нагальна необхідність узагальнення та систематизації знань, накопичених у цій сфері вітчизняною правовою наукою. Причому, з огляду на прискорену динаміку еволюції дорожньо-транспортного комплексу (протягом останніх десятиліть об'єктивні умови його роботи зазнали неабияких змін), найбільший інтерес

становлять дослідження нової доби – доби державної незалежності. Як показує бібліографічний аналіз, з початку 90-х рр. XX ст. і до наших днів основна увага правничого загалу (передовсім, учених, які переймаються питаннями дорожньої безпеки) прикута до проблем застосування державного примусу. З одного боку це пояснюється залишковим «відлунням» радянської правової доктрини, котра постулювала примус в якості першочергового інструмента впливу на волю та свідомість громадян. З іншого – обумовлюється надзвичайною гостротою проблематики БДР: катастрофічні масштаби дорожнього травматизму вимагають негайного поліпшення ситуації, а в умовах існуючої економічної нестабільності швидкий ефект здатні забезпечити тільки примусові заходи. Тож саме на їх розгляді роблять акцент більшість сучасних правників: Задояный М. Т., Розвадовський В. Й., Гізімчук С. В., Галімшина Г. В., Гуржій Т. О., Собакарь А. О., Лошицький М. В., Мілєнін О. Л., Салманова О. Ю., Стоцька М. М., Михайлов Р. І., Коллер Ю. С., Циба Є. В. Незважаючи на чималий внесок вчених України у дослідженні проблеми забезпечення БДР в цілому та правового статусу учасників дорожнього руху зокрема, здебільшого ці наукові доробки стосувались тільки адміністративної відповідальності учасників дорожнього руху як одного з елементів правового статусу, що тільки у своїй невід'ємній сукупності відображають цілісне та завершене поняття правового статусу учасників дорожнього руху.

Крім того, враховуючи всі зміни та доповнення в адміністративному законодавстві України, які відбулися в країні за останні роки, зокрема, зміни у правах та обов'язках учасників дорожнього руху з прийняттям Закону України «Про Національну поліцію» та ліквідацію з цього приводу міліції та державної автомобільної інспекції як її складового підрозділу; зміни у складах адміністративних правопорушень у сфері БДР, санкціях, що накладаються повноваженими на те органами за їх скоєння, порядку притягнення особи до адміністративної відповідальності тощо, свідчить про те, що більшість висновків та рекомендацій науковців, викладених у своїх дослідженнях, на жаль, на сьогодні вже втратили актуальність, а тому є необхідність у комплексному дослідженні правового статусу учасників дорожнього руху з урахуванням сьогодення та наданні з цього приводу пропозицій щодо його розвитку та перспектив функціонування щодо забезпечення БДР на території України в майбутньому.

Стосовно кримінальної відповідальності за порушення БДР слід відмітити дослідження таких науковців як Мисливий В. А., Бабанін С. В.,

Матвійчук Я. В., Федчун Н. О, Колб О. Г., Горшков Д. В., Бесчастна В. В., Звоненко О. О.

Процеси, пов’язані з дорожнім рухом, явища, що його супроводжують, та їх наслідки, зокрема, шкода, яку несе суспільство від ДТП, займають важливе місце в суспільному житті та потребують глибокого наукового дослідження.

Сибір І. В.

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

КРИМІНОЛОГІЧНІ РЕАЛІЇ ГУМАНІТАРНОЇ ДОПОМОГИ ТА БЛАГОДІЙНОСТІ В УКРАЇНІ

Із початком російської збройної агресії в Україні залежно від регіону склалася різна гуманітарна ситуація. Території, на яких велися бойові дії, перебували у стані гуманітарної катастрофи. Не краще становище складалося й складається і дотепер в деокупованих районах, адже окрім людських жертв, масштабних руйнувань забудов, знищеної інфраструктури, у громадах виникає і продовольча криза, не кажучи вже про відсутність життєвонеобхідних ліків.

Із метою порятунку населення України міжнародне співтовариство розпочало процес гуманітарної та благодійної підтримки. Самі ж громадяни України також активізувалися в цьому напрямі. Так, із початком війни в державі спостерігався справжній «бум» реєстрацій благодійних фондів і громадських організацій, загальна кількість яких наразі перевищує 15 тис. [1]. Наприклад, у квітні 2022 року у порівнянні із квітнем 2021 року було зафіксовано у 12 разів більше реєстрацій організацій, що спеціалізуються на благодійній діяльності, зокрема, із урахуванням можливості збору коштів [1].

Гуманітарна допомога, яка надається такими фондами / організаціями, це не лише продукти харчування, одяг, медикаменти, що надаються військовим та цивільному населенню України. Це й автомобілі (різної вартості), військова техніка, предмети побуту, побутова техніка, комп’ютерна техніка, медичне обладнання тощо. Окремим аспектом є надання грошової допомоги постраждалим, у тому числі й міжнародними організаціями, фондами тощо. Відповідно до Закону України «Про гуманітарну допомогу» (1999 р.) під гуманітарною допомогою

розуміється цільова адресна безоплатна допомога в грошовій або натуральній формі, у вигляді безповоротної фінансової допомоги або добровільних пожертвувань, або допомога у вигляді виконання робіт, надання послуг, що надається іноземними та вітчизняними донорами із гуманних мотивів отримувачам гуманітарної допомоги в Україні або за кордоном, які потребують її у зв’язку з соціальною незахищеністю, матеріальною незабезпеченістю, важким фінансовим становищем,

виникненням надзвичайного стану, зокрема внаслідок стихійного лиха, аварій, епідемій і епізоотій, екологічних, техногенних та інших катастроф, які створюють загрозу для життя і здоров'я населення, або тяжкою хворобою конкретних фізичних осіб, а також для підготовки до збройного захисту держави та її захисту у разі збройної агресії або збройного конфлікту [2].

Поряд із гуманітарною допомогою, значних обсягів наразі в Україні набула й благодійна діяльність, яка визначається у законодавстві України, як: добровільна особиста та/або майнова допомога для досягнення визначених цілей, що не передбачає одержання благодійником прибутку, а також сплати будь-якої винагороди або компенсації благодійнику від імені або за дорученням бенефіціара [3].

Проте висока мета – надання підтримки у скрутних умовах, – закладена у наданні гуманітарної допомоги та благодійній діяльності, не могла не бути не використана у протиправній діяльності. Це пояснюється низькими моральними якостями окремих громадян, які шукають легкої вдачі чи способу отримання доходу навіть у таких скрутних умовах, як війна. Майже з перших днів набули розповсюдження цілі схеми отримання для продажу та безпосередньо реалізацією гуманітарної допомоги, а також нецільового використання благодійних коштів, про що неодноразово повідомлялося в ЗМІ. У зв'язку з цим діяння, пов'язані із продажем товарів (предметів) гуманітарної допомоги або використанням благодійних пожертв, безоплатної допомоги чи укладання інших правочинів щодо розпорядження таким майном з метою отримання прибутку (в тому числі у значному розмірі) були криміналізовані шляхом доповнення чинного КК України статтею 2012 («Незаконне використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги») [4].

Необхідно зазначити, що вчиненню злочину, передбаченого статтею 2012 КК України (крім вчинення цього діяння у його «чистій» формі, коли товари купуються за заниженим «прайсом» саме для благодійних цілей, отримуються пожертви тощо) можуть передувати і правопорушення проти власності, що пов'язані з викраденням, заволодінням чи розкраданням гуманітарної допомоги [5, с. 41].

Однак із введенням до КК України статті 2012 у науці кримінального права та кримінології виникла точка зору, що ця зміна до кримінального законодавства – прояв надмірної (надлишкової) криміналізації, що пояснюється тим, що в переважній більшості випадків дії, заборонені чинною редакцією статті 2012 КК України, за її відсутності визнавались б розкраданнями і кваліфікувались б за однією з частин статті 191 КК як

привласнення, розтрата або заволодіння чужим майном шляхом зловживання службовою особою своїм службовим становищем [6, с. 99].

Відповідно до офіційної статистики Офісу Генерального прокурора України протягом 2022 року за статтею 2012 КК України було обліковано 3 проступки (за частиною 1) та 381 злочин (за частинами 2, 3). Порівнюючи ці статистичні дані із реаліями українського сьогодення, розголосом подібних випадків у ЗМІ та громадською думкою, можна зробити висновок, що такий показник в масштабах усієї країни є значно заниженим. Причинами латентності подібних діянь є, на нашу думку, в першу чергу, існування явища корупції.

Таким чином, кримінологічними реаліями гуманітарної допомоги та благодійності в Україні є той факт, що поряд із тими людьми, які покладають своє життя на підтримку Збройних Сил України, що мужньо боронять державу вже понад рік, допомогу тисячам українців, які страждають від російської агресії, існують і ті, чиї моральні властивості дозволяють «наживатися» на трагедії українського народу.

Список використаних джерел:

1. *Динаміка реєстрацій благодійних організацій під час війни: дослідження Vkursi та Zagoriy Foundation. URL : https://vkursi.pro/news/content/splesk-reiestratsiy-blahodiynykh-orhanizatsiy-doslidzhennia-vkursi-ta-zagoriy-foundation-234986 (дата звернення: 10.03.2023 р.).*
2. *Про гуманітарну допомогу : Закон України 22 жовтня 1999 р. № 1192-XIV. URL : https://zakon.rada.gov.ua/laws/show/1192-14#Text (дата звернення: 10.03.2023 р.).*
3. *Про благодійну діяльність та благодійні організації : Закон України від 5 липня 2012 р. № 5073-VI. URL : https://zakon.rada.gov.ua/laws/show/5073-17#Text (дата звернення: 10.03.2023 р.).*
4. *Кримінальний кодекс України : Закон України від 5 квітня 2001 року № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 10.03.2023 р.).*
5. *Васильєв А. А. До питання про криміналізацію розкрадання гуманітарної допомоги. Проблеми кваліфікації та розслідування кримінальних правопорушень в умовах воєнного стану : матеріали науково-теоретичної конференції (Київ, 26 травня 2022 р.). С. 39 – 42. URL : http://elar.naiau.kiev.ua/jspui/handle/123456789/21473.*
6. *Дудоров О. О., Мовчан Р. О. Кримінально-правова заборона щодо незаконного використання гуманітарної допомоги: сумнівна законодавча новела. Вісник ЛДУВС ім. Е.О. Дідоренка. 2022. Вип.2 (98). С. 99–115. DOI:10.33766/2524-0323.98.115-125.*
7. *Єдиний звіт про кримінальні правопорушення по державі за грудень 2022 року : стат. інформ. Ген. прокуратури України. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 10.03.2023 р.).*

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

Лясота А. Є.

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

СТАГНАЦІЯ ПОЛІТИЧНОЇ СИСТЕМИ В УМОВАХ ДЕМОКРАТИЧНОГО ТРАНЗИТУ

Глобальне громадянське суспільство стає більш відкритим, люди скрізь хочуть, щоб їхні голоси були почуті і до них прислухалися. Це прагнення до політичного самовираження ставить питання переходу від авторитарного правління до демократії знову на міжнародний порядок денний і робить своєчасним вивчення того, як відбувалися попередні демократичні переходи і яким чином прогнозування політичних криз може пом'якшити цей процес. Це особливо важливо, оскільки успішні попередні переходи зовсім не були неминучими, а в багатьох випадках були несподіваними, що, власне, і призвело до глибокої політичної, соціальної та економічної кризи в країні. Нові демократичні режими, як правило, проходили через тяжку політичну та супутню економічну кризу, яка виникала унаслідок деієрархізації політичної влади.

У процесі трансформації політичного режиму до демократичного можна виділити чотири широкі групи викликів: підготовка до переходу, ліквідація авторитарного режиму, передача влади та управління нею, а також стабілізація та інституціоналізація демократії, що зароджується. Ці виклики виникали не лінійно і не обов'язково в такому хронологічному порядку, але вони з'являлися в усіх випадках і, ймовірно, будуть присутні в майбутніх перехідних процесах. У випадку, якщо хоча б на одному з етапів виникнуть внутрішні протиріччя або вакуум влади – кризові явища стають неминучими.

Яскравим, в даному контексті, прикладом демократичного транзиту є латиноамериканський регіон, де цей процес не завжди був вдалим та безболісним для громадян. Так, запит на демократизацію у деяких режимів (Парагвай) призвів до військової диктатури. На противагу, авторитарний режим Чилі був вкрай нестабільним, він породжував соціальний запит на

демократизацію, що призводило до стагнації політичної системи та кризи, в результаті чого до влади приходив або авторитарний політик, або військова хунта.

Досвід демократизації країн Латинської Америки дозволив узагальнити та виокремити основні особливості функціонування політичної системи в умовах переходу від авторитаризму до демократії. По-перше, внутрішні сили, які прагнули покінчити з авторитарним режимом, як правило, повинні були досягти достатньо широкої підтримки, узгодженості, легітимності та інших ресурсів, щоб кинути виклик здатності режиму керувати, а також стати реальними претендентами на національну владу. У деяких випадках вони також повинні були стати життєздатними співрозмовниками для тих всередині авторитарного режиму, хто усвідомлював, що режим потребує партнера для полегшення можливої стратегії виходу. Іноді їм також доводилося здобувати довіру міжнародних суб'єктів, які хотіли підтримати перехідний процес. Досягнення цих цілей часто вимагало подолання глибоких розбіжностей щодо цілей, стратегій, тактики і лідерства серед тих, хто виступав проти авторитарного режиму. Звісно, переконати різні опозиційні групи вирішити свої основні розбіжності для того, щоб протистояти авторитарному режиму, як правило, було нелегко [1, с. 43].

По-друге, створення широкої коаліції, здатної повалити авторитарний режим і з твердою прихильністю до демократичних цінностей, часто вимагало наполегливої роботи над подоланням розбіжностей всередині опозиції, в той же час розуміючи і використовуючи розбіжності, явні або приховані, всередині самого режиму [4, с. 469].

По-третє, авторитарні уряди не відмовлялися від влади доти, доки хоча б один важливий сектор всередині режиму не усвідомлював, що це єдиний спосіб уникнути серйозних небажаних наслідків: серйозної втрати суспільної підтримки, громадянського насильства, розколу збройних сил, серйозних економічних збитків, міжнародного остракізму або загрози територіальній цілісності країни. Приниження від військової поразки, економічного колапсу або виборчої поразки іноді прискорювало відхід режиму. Але ці травми зазвичай призводили до демократичних перетворень лише тоді, коли окремі сегменти авторитарного уряду толерували або підтримували вимоги опозиції до демократії [4, с. 470].

Наприклад, у країнах колишнього СРСР демократичні перетворення породили глобальну кризу політичних систем, яка у подальшому вилилась і у економічну, соціальну кризу, яку більшості країн вдалось подолати лише наприкінці 90-х років двадцятого століття. Однак, стагнація політичної

системи в період переходу від авторитаризму до демократії в таких країнаї, як Азербайджан, Казахстан, Білорусь та ін., призвела до соціального запиту серед населення на «сильну руку» у владі та відновлення авторитарних режимів.

Здійснення успішного політичного транзиту вимагає подолання численних дилем та реалізації політичних потреб. Перша потреба - встановлення громадянського порядку і припиненню насильства, одночасно гарантія, що всі сили безпеки і розвідки, в тому числі ті, які були в центрі попередніх репресій, відтепер будуть діяти в рамках закону і підлягати контролю з боку нової цивільної влади. Вони також повинні були викликати довіру всередині країни і здобути міжнародну легітимність.

Друга - у багатьох випадках це передбачало розробка виборчих процедур, які б гарантували, що воля більшості виборців буде зафіксована і дотримана, а також запевнення ключових політичних меншин (часто пов'язаних з режимом, що йде) у тому, що вони будуть представлені і що їхні основні інтереси будуть захищені відповідно до принципу верховенства права. Третя потреба полягала в тому, щоб запевнити, що ті, хто прийде до влади, будуть добре підготовлені, технічно і політично, до виконання своїх нових обов'язків: шляхом отримання необхідної підготовки і навичок, залучення чиновників, які вже мають такі навички, і/або збереження деяких кадрів з попереднього режиму [2, с. 19].

З цілої низки питань - від макроекономічної політики до надання соціальних послуг і пошуку шляхів правосуддя перехідного періоду - урядування вимагало поглядів, компетенцій і досвіду, які дуже відрізнялися від опозиційних. У багатьох випадках це означало навчання на робочому місці. Уряди, що перейшли до влади від опозиції, повинні були збалансувати потребу в бюрократичному, технократичному, безпековому та судовому досвіді з метою обмежити вплив колишнього режиму. Вони повинні були переорієнтувати бюрократію, а також сили безпеки і поліції з контролю над суб'єктами на служіння громадянам. Вони повинні були переконати громадян, у свою чергу, прийняти і почати довіряти державі, яку багато хто зі зрозумілих причин відкидав як нелегітимну і ворожу.

Лідерам перехідного періоду доводилося балансувати між суперечливими імперативами реагування на порушення прав людини попереднім режимом та притягнення до відповідальності тих, хто вчинив грубі порушення, з одного боку, та збереженням лояльності силових структур (деякі з яких були причетні до цих порушень), з іншого боку. Водночас, вони повинні були переконати громадян, що ці сили можуть ефективно боротися зі злочинністю, насильством і, в деяких випадках, з

сепаратистськими та повстанськими рухами. Нова влада, як правило, успадкувала давні моделі корупції і безкарності, тому необхідно було створити або захистити автономію і повноваження незалежних судових органів і незалежних засобів масової інформації, які могли б притягати до відповідальності національних керівників та інших осіб, уникаючи при цьому створення центрів вето, які могли б блокувати всі ініціативи нового уряду. Виникала, також нагальна потреба досягти економічного зростання і розширення зайнятості, контролювати інфляцію, одночасно покращуючи забезпечення житлом, охорону здоров'я і освіту та збільшуючи державні видатки для задоволення довготривалих потреб бідних верств населення [3, с. 111].

В процесі реальних демократичних перетворень, політичні лідери часто стикалися з іншими гострими питаннями. З плином часу громадськість часто звинувачувала демократичних лідерів, а іноді й саму демократію, у тому, що вони не виправдали економічних або політичних очікувань. Суспільно-політичні рухи, які були об’єднані політичними лідерами у протистоянні з авторитарним режимом, часто набували фрагментарного характеру, створюючи проблеми для урядів. На жаль, організації громадянського суспільства, в тому числі правозахисні групи та жіночі рухи, які зробили важливий внесок в антиавторитарну опозицію, іноді атрофувалися або перейшли на крайні та деструктивні позиції після того, як багато з їхніх найталановитіших і прагматичних лідерів увійшли в урядову або партійну політику. За таких обставин зберегти активність і незалежність неурядових організацій було нелегко. Розбудова взаємовигідних відносин між новою владою та новими опозиційними силами (до складу яких іноді входили представники колишньої влади), а також з незалежними громадськими силами та організаціями громадянського суспільства супроводжувалася чисельними внутрішніми конфліктами. Це вимагало особливо делікатної і постійної уваги.

Отже, у багатьох випадках вище описані чинники призводили до стагнації політичної системи. Демократична культура в країнах не встигла сформуватись, кожен суб’єкт політичного життя намагався просувати свою позицію вирішення проблем, що призводило до системних розбіжностей. Неефективність економічних реформ та слабкість економіки перехідних режимів призводили до збіднiння населення, це викликало недовіру до влади та стрімке бажання громадян певним чином вплинути на ситуацію. Стагнація політичної системи в умовах переходу до демократичного режиму призводила до того, що демократизація зупинялась «на пів дороги». Системна криза приводила до влади нові авторитарні режими.

Список використаних джерел:

1. *Генон Р. Криза сучасного світу /Р. Генон/ К.: Пломінь. - 2022. - 212 с.*
2. *Маційовський Ю. Деякі аспекти вивчення феномену кризи у політичних дослідженнях/ Маційовський Ю.// Політичний менеджмент. 2008. № 6. С. 16–29.*
3. *Неклесса А. Керований хаос рух до нестандартної системі світових відносин / А. Неклесса// Світова економіка і міжнародні відносини. - 2002. - №9. – С. 109-113.*
4. *Bellucci, P., Costa Lobo, M. and Lewis-Beck, M.S. Economic crisis and elections: the European periphery / Electoral Studies. №7. 2012. P. 469–471.*

Стеньгач Н. О.

кандидат історичних наук, доцент, професор кафедри теорії та історії держави і права
Хмельницького університету управління та права імені Леоніда Юзькова
м. Хмельницький, Україна

ІДЕЯ ЗАХИСТУ ЗАГАЛЬНОСУСПІЛЬНОГО БЛАГА У ПОЛІТИКО-ПРАВОВІЙ КУЛЬТУРІ КОЗАЦЬКОЇ СТАРШИНИ ГЕТЬМАНЩИНИ (ДРУГА ПОЛОВИНА XVII – XVIII СТ.СТ.)

Козацька старшина як політична еліта у виконанні своєї суспільної функції правління практично одразу ж після утворення козацької держави наштовхнулася на потребу узгодження інтересів усіх соціальних верств, підпорядкування окремішнього, часткового інтересу загальносуспільному. Дана потреба викликала до життя відповідну норму: підпорядкування приватного інтересу суспільному благу.

На наявність даної норми у політико-культурному комплексі еліти України-Гетьманщини передусім вказує той факт, що саме загальносуспільним благом «посполитим добром», «загального добра радінням» як метою своєї діяльності виправдовували учасники політичного процесу усі свої дії, засуджуючи при цьому будь-яке користолюбство. Так, за інструкцією І.Виговського миргородський полковник Г.Лісницький у переговорах з послами від турецького султана та польського короля мав підкреслювати, що підданство царю керівництво держави вибрало: «для милості самої православної віри, не даючись для своїх прибутків схилятися до їх намов і для допомоги всіх» [1, с. 210].

Ця політична ідея отримала чітке вираження у зверненні І.Виговського до європейських володарів з приводу війни з Московією. Документ на самому початку містить запевнення, що розпочавши та провівши «війну з поляками’ «свої приватні справи ми (Військо Запорозьке) ставили осторонь заради слави Божої та загального добра». [2, с.142]

Цю ж орієнтацію, але у формі критики містить лист правобережного генерального писаря Л. Бускевича до полковника Р. Дмитрашка-Райчі від 3 березня 1669 р., де він засуджував «наших людей військових» за «непостійність», визначаючи їх соціальну функцію так: «про спільне добро переважно радіти, а не про примхи». [3, с. 302]. Так само пояснював мету своєї діяльності і сам правобережний гетьман. У жовтні 1675 р., шукаючи домовленості з І. Сірком про підданство Війську Запорозькому низовому,

П. Дорошенко писав: «Незабаром гармати і всілякі запаси послати пораджу, тому що я не собі і не дітям моїм збиваю, тільки на оборону і на красу і на славу всього війська». [3, с. 307]

Посилаючись саме на дану норму П. Орлик пояснював причину переходу І. Мазепи на бік Карла XII. У листі до С. Яворського колишній генеральний писар стверджував, що присягаючи на вірність змовницьким задумам, гетьман казав йому, що це він робить «не для приватної моєї користі, не для високих гонорів, не для більшого збагачення, а ні для інших яких-небудь примх, але для вас всіх, хто під владою і регіментом моїм перебуває, для жінок і дітей ваших, для загального добра матері моєї вітчизни бідної України, всього війська Запорозького і народу Малоросійського, і для зміцнення і розширення прав і вольностей військових».[4, с. 181]

Саме на службу суспільній справі вказували старшини Мазепі, коли той щиро чи притворно засумнівався у доцільності організовуваної змови. Старшини, бачачи його, як описував П. Орлик, у «боязні і непевності, часто йому в Білій Церкві нагадували, щоб і про свою, і про спільну всіх цілість промишляв». [5, с. 36]

Як бачимо, у політико-культурному комплексі старшин виробилося чітке протиставлення загальносуспільної справи приватним потребам. Турботу загальним благом вони підносили до рівня чесноти. Це ми читаємо, наприклад, і в щоденнику Генеральної Військової канцелярії за 2 квітня 1723 р.: «Писаний лист до посланих на Москву в інтересах Малоросії пп. Граб'янки... та Гамалія... похваляючи їм за те, що вони два з чуйності своєї до спільного добра, для справування доручених собі справ залишилися в Москві, а інші ні з чим звідтіля, з ними бувши, додому їдуть». [1, с. 24]

До загально-суспільного інтересу апелювали й учасники боротьби за владу. Найсерйознішими обвинуваченнями, які учасники цієї боротьби могли висунути один одному, були звинувачення у нехтуванні загальносуспільними інтересами, загальним благом і т. п. За це засуджували попередніх гетьманів, наприклад, представники оточення Д. Многогрішного, що вели переговори з московським урядом щодо змісту Глухівських статей. Вони, зокрема, стверджували, що «по смерті Б.Хмельницького, по ньому наступні гетьмани, для своєї честі і собі примноження маєтності Війська Запорозького обмежували вольності». [1, с. 116] Практично одночасно, 19 лютого 1669 р. подібна думка була висловлена й на Правобережжі. П. Дорошенко у листі до київського воєводи П. Шереметьєва критикував тих «закутних гетьманчиків», які «для своєї привати повстаючи, статейні речі псували». [3, с. 545]

На ідеї турботи про загальне благо будував за останнього гетьманування свою пропагандистську роботу і Ю.- Хмельницький. У листах від 3 липня та 8 серпня 1677 р. до канівців та чигиринців, він стверджував, що жоден з гетьманів неспроможний гарантувати Війську Запорозькому дотримання привілеїв та вольностей, якщо він «своїм недозрілим розумом і марнослав'ям піднісся в гордість, не бажаючи нікому доброго, лише собі самому» або ж «за користю погнався і за славою свого світу, тимчасово панівною». [3, с. 258]

В орієнтаціях на загальносуспільне благо як сенс діяльності представника еліти українські старшини піднялися до усвідомлення необхідності контролю за її окремими представниками. В умовах змагання між гетьманом та старшинським загалом це проявилося насамперед у потребі відділення гетьманського особистого скарбу від державного.

З максимально виразною розумінням проблеми співвідношення приватного та загальносуспільного у взаєминах гетьмана та держави розглянуто дане питання у Конституції П. Орлика. Стосовно генерального підскарбія там сказано, що він би «скарб військовий у своєму нагляді мав... і ті (прибутки - О.С.) на потребу публічну військову, а не на свою приватну, за відомом Гетьманським, вживав. Сам зась Ясновельможний Гетьман до скарбу військового і до надходжень, до нього належних, не має стосуватися і на свій персональний пожиток вживати, задовольняючись своїми оброками і приходами». [4, с. 34]

Ідею захисту загальносуспільного блага посередництвом строгого контролю одночасно гетьманом *і* генеральною старшиною за витрачанням грошей з військового скарбу пропонувала й анонімна записка про обмеження влади гетьмана: «А доглядали б того зі старанністю, щоб на приватні нічиї потреби якого скарбу не витрачувано». [5, с. 250]

Природно, що свою службу у сфері правління й управління елітарні прошарки пов'язували зі служінням загальному добру. Саме спрямованістю на це витлумачували сенс життя представників еліти після їх смерті, навіть якщо на цій ниві їх заслуги були відносно скромними. Це ми бачимо зафіксованим у листі-відповіді переяславського полковника Л. Полуботка від 12 червня 1685 р. Військовому генеральному писарю В. Кочубею про смерть гетьманового сина Семена Самойловича: «...Але надія тая, котра вітчизні нашій Україні багато вже чинила, а більшої ще обіцяла по ньому оборони, багато вже засвідчувала, а ще більше засвідчувати може праця його на добро посполите». [1, с. 253]

Погоджуючись з тим, що у часи Гетьманщини загально-суспільне не могло подаватися інакше як через окремий соціальний інтерес провідної

верстви, ми не можемо не звернути уваги і на те, що українська еліта, принаймні у військовому аспекті усвідомлювала наявність загально-суспільного інтересу як такого, що потребує узгодження інтересів окремих станів. Це фіксується в універсалі І. Мазепи від 11 вересня 1687 р., опублікованому з приводу відмови підданих київських монастирів вартувати на вежах та ставати до оборони на валах. Гетьман зобов'язував їх до цього використовуючи такий аргумент: «А відаємо і те добре, що у всій вселенній в місцевостях своїх мешкаючи люди спільної цілості своєї спільним коштом і спільною працею стережуть і боронять». [6, с. 300]

Прояв усвідомлення того, що інтереси окремих панівних верств старшинства можуть розвиватися всупереч загально-суспільним (але, врешті, заради них же самих, мусять бути підпорядковані загальносуспільним) чітко фіксується в універсалі І. Самойловича від 1 березня 1686 р. про запровадження оренд або відкупів. Необхідність утримувати компанійців «людей до війни завше готових» гетьман обґрунтовував потребою «оборони вітчизни нашої України і... захования цілості церков Божих і добра загального всього народу нашого християнського» та нагадуванням, «що війська згадані ми рейментар не для самих нас, але для всієї загальної утримуємо оборони», включаючи й тих людей, «які з шинків призиски собі мають». Таким опонентам гетьман пояснював, що існували два шляхи накопичення необхідних коштів. Або «мусили бисьмо побори і подимне з посполитих людей для тої потреби витягати... які певне людей би розігнали» (а це б неминуче завдало б збитків тим старшинам, які могли б насамперед реалізувати право на вільне шинкування) або «тії з шинків горілчаних зиски на посполиту всього нашого народу обертатися [мусять] потребу, аніж в самотний і приватний шинкарів пожиток приходити». [6, с. 267]

Таким чином, перед нами політичне рішення, яке слід визначити як соціально відповідальне, тобто як таке, що вимагає максимально можливого узгодження інтересів різних соціальних верств, так і суспільства в цілому. Таке ж рішення не може бути ні прийняте, ні реалізоване без чіткого усвідомлення як різниці, так і взаємозв'язку між окремими соціальними інтересами, включаючи й інтереси еліти, та загальносуспільними інтересами.

Проте, вважаємо, не варто й перебільшувати ролі такого усвідомлення у суспільно-політичному житті України-Гетьманщини, особливо з огляду на зростання числа т.зв. інтеграціоністів, які за корпоративними інтересами стану не помічали їх взаємозв'язку з загальносуспільними потребами. З іншого боку, ми не можемо нехтувати й тим фактом, що й під кінець існування України-Гетьманщини, серед представників шляхетського стану знаходилося ще доволі представників політичної елітарної традиції, щоб з

трибуни З'їзду старшин 1763 р. пролунали, звичайно, зі сподіванням на розуміння і підтримку, слова: «Заради любові до вітчизни, заради власної вашої і нащадків ваших честі і користі, об'єднайте всі сили розуму вашого, зміцніть їх патріотичним натхненням, і забувши усі пристрасті і партикулярні користі, подумайте про відновлення колишніх Вітчизни вашої порядків та добробуту». [5, с. 252] В цілому, до самого скасування інституції гетьманства, в українському суспільстві йшла природна боротьба окремішнього, часткового і загальносуспільного, а її наслідками було постійне відтворення політико-культурних орієнтацій на служіння загальному добру.

Список використаних джерел:

1. *Акты, относящиеся к истории Южной и Западной России, собранные и изданные Археографической комиссией. СПб., Т. 7 : 1657-1663, 1668-1669 / [ред. Н. И. Костомаров]. 1872. 398 с.*
2. *Акты, относящиеся к истории Южной и Западной России, собранные и изданные Археографической комиссией. - СПб., Т. 8 : 1668-1669, 1648-1657 / [ред. Н. И. Костомаров]. 1875. 400 с.*
3. *Акты, относящиеся к истории Южной и Западной России, собранные и изданные Археографической комиссией. СПб., Т. 12 : 1675-1676 / [ред. Н. И. Костомаров]. 1882. 874 с.*
4. *Чухліб Т. В. Пакти та конституції законів і вольностей Війська Запорозького 1710 // Енциклопедія історії України : у 10 т. / редкол.: В. А. Смолій (голова) та ін. ; Інститут історії України НАН України. К. : Наукова думка, 2011. Т. 8. 520 с.*
5. *Бантыш-Каменский Д. Н. Источники Малороссийской истории : [в 2 ч.] / собр. Д. Н. Бантышем-Каменским и изд. О. Бодянским. Москва : В Унив. Тип., 1858, Ч.1 :1649-1687. 339 с.*
6. *Окиншевич Л. Центральні установи України-гетьманщини XVII - XVIII вв. / Л. Окиншевич; Всеукраїнська академія наук. Київ: Друкарня Всеукраїнської академії наук, 1929. 425 с.*

Коруняк А. В.

аспірант кафедри публічного управління та адміністрування
Хмельницького університету управління та права
імені Леоніда Юзькова
м. Хмельницький, Україна

ВЗАЄМОДІЯ СТАРОСТ ТЕРИТОРІАЛЬНИХ ГРОМАД ТА ОРГАНІВ САМООРГАНІЗАЦІЇ НАСЕЛЕННЯ

Визначаючи перелік основних повноважень старост, необхідних їм для ефективного виконання своїх функцій, законодавець закцентував увагу на необхідності взаємодії старости з органами самоорганізації населення (далі – ОСН), як суб'єктами, що представляють інтереси місцевих мешканців.

ОСН є представницькі органи місцевого самоврядування, що створюються жителями, які на законних підставах проживають на території села, селища, міста або їх частин, для вирішення завдань, передбачених законом [3]. Таким чином, функціонування ОСН є одним із дієвих способів залучення громадян до вирішення актуальних проблем місцевого значення населених пунктів, у яких вони безпосередньо проживають. Саме право на створення ОСН є важливим підґрунтям для залучення населення до вирішення соціально-економічних, культурних та інших питань розвитку певної території. Враховуючи основне покликання старости представляти інтереси жилетів відповідного старостинського округу та сприяти у вирішенні вищезазначених питань, цілком логічною та доречною є можливість старости брати участь у діяльності інших суб'єктів, функції яких переплітаються з функціями самого старости.

Аналіз норм Закону України «Про органи самоорганізації населення» дозволяє зробити висновок, що такими органами є:

1) будинкові, вуличні, квартальні комітети;
2) комітети мікрорайонів;
3) комітети районів у містах;
4) сільські, селищні комітети [3].

Таким чином, ОСН умовно можна поділити на три групи:

1) ОСН населених пунктів;
2) ОСН районів у містах;
3) ОСН частини населеного пункту.

Форми співпраці старости з ОСН випливають зі змісту п. 12 ч. 5 ст. 54-1 Закону України «Про місцеве самоврядування в Україні», згідно з яким староста сприяє утворенню та діяльності ОСН, організації та проведенню загальних зборів, громадських слухань та інших форм безпосередньої участі громадян у вирішенні питань місцевого значення у відповідному старостинському окрузі [2]. Вважаємо положення зазначеної статті доцільними та обґрунтованими, виходячи з такого:

1) Законом передбачений відповідний порядок створення ОСН, що включає в себе:

- ініціювання створення ОСН;
- надання дозволу (відмови) на створення ОСН;
- обрання ОСН;
- затвердження Положення про орган самоорганізації населення;
- легалізація ОСН шляхом реєстрації або повідомлення про заснування [3].

Таким чином, вбачається, що процедура створення ОСН потребує наявності певних знань та навиків, які не завжди присутні у осіб, що ініціюють створення такого органу. У свою чергу, староста, як посадова особа місцевого самоврядування, в силу своєї передбачених законом повноважень, зобов'язаний орієнтуватися в юридичних, організаційних, фінансових тощо аспектах зазначеного процесу. Тому, на нашу думку, можливість старости сприяти утворенню ОСН підвищить ефективність цих процесів, призведе до більш швидкого та якісного забезпечення механізму їх утворення.

2) Законом також передбачені вимоги до діяльності ОСН, такі як: гласність, підзвітність, вимоги до форми роботи, прийняття рішень тощо [3]. Дотримуватися цих вимог ОСН буде простіше у взаємодії зі старостою, оскільки останній володіючи необхідними можливостями може ефективно сприяти у діяльності таких органів, зокрема у таких формах як: допомога у наданні необхідних приміщень для проведення засідань ОМС, допомога у опублікуванні необхідної інформації, консультації щодо форми та змісту прийнятих рішень тощо. Таким чином, допомога старости у роботі ОСН безумовно сприятиме підвищенню ефективності такої роботи.

Разом з тим, на нашу думку, було б доцільно закріпити на законодавчому рівні повноваження старости щодо здійснення моніторингу діяльністю ОСН старостинського округу, формами якого контролю можуть бути періодичне інформування про діяльність, звіт про використання фінансових ресурсів тощо.

Таким чином, ОСН є специфічними органами місцевого самоврядування, які обираються на строк повноважень відповідної ради та поєднують в собі ознаки органу публічної влади (наділенні певними повноваженнями для вирішення окремих питань місцевого значення) та громадської організації (здійснюють свою діяльність на громадських засадах), а їх взаємодія зі старостою безумовно допоможе у вирішенні більшого кола питань місцевого значення.

Список використаних джерел:

1. Децентралізація влади [Електронний ресурс]. — Режим доступу: http://decentralization.gov.ua.

2. Про місцеве самоврядування в Україні: Закон України від 21.05.1997 р. № 280/97-ВР. Верховна Рада України. Законодавство України. URL: http://zakon.rada.gov.ua/laws/show/ 280/97-вр.

3. Про органи самоорганізації населення: Закон України від 11.07.2001 р. № 2625-III. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua /laws/show/2625-14#n14

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

Кушнєров Є. О.

кандидат технічних наук,
докторант кафедри конституційного та адміністративного права
Запорізького національного університету

АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ РЕАЛІЗАЦІЇ ТА ЗАХИСТУ ПАТЕНТНИХ ПРАВ

Центральною особливістю правової та демократичної держави є належний рівень забезпечення реалізації та захисту прав та свобод людини і громадянина.

До елементів правової держави необхідно віднести створення механізму захисту патентних прав в Україні. Основою для ефективного здійснення патентних прав є вирішення проблематики функціонування адміністративно-правового механізму забезпечення реєстрації, реалізації та захисту права інтелектуальної власності в Україні.

До об’єктів права інтелектуальної власності відносяться патентні права особи, що можуть виникати на винахід, корисну модель чи промисловий зразок.

Згідно із положеннями Закону України від 15 грудня 1993 року № 3687-XII «Про охорону прав на винаходи і корисні моделі» під патентом варто розуміти патент (патент на винахід, деклараційний патент на винахід, деклараційний патент на корисну модель, патент (деклараційний патент) на секретний винахід, деклараційний патент на секретну корисну модель) – охоронний документ, що засвідчує пріоритет, авторство і право власності на винахід (корисну модель) [1].

В межах загальнотеоретичних наукових розробок під патентом розуміється певний адміністративний акт індивідуальної дії, що має правовстановлюючий зміст та характер, який виступає гарантією захисту об’єкта інтелектуальної власності.

Можна виділяти різні типи власності як об’єкт права інтелектуальної власності, це закріплено у відповідних положеннях чинних міжнародних нормативно-правових актів, зокрема, у положеннях Паризької Конвенції про

охорону промислової власності та Бернської Конвенції про охорону літературних творів та творів мистецтва [2; 3].

Необхідно підкреслити, що відповідно до міжнародного законодавства закріплюється розширений перелік патентів, що не співпадає із встановленим чинним законодавством України змістом патентних прав. Так, згідно із законодавством ЄС до патентів на винаходи відносяться такі види промислових патентів, як: патенти, що ввозяться, патенти на вдосконалення, додаткові патенти і свідоцтва й таке інше.

З метою захисту патентних прав в країнах ЄС функціонує система єдиних торговельних марок Співтовариства. Організаційний супровід використання системи єдиних торговельних марок ЄС забезпечується в межах діяльності спеціального органу публічної влади, яким є відомство з торговельних марок [4].

В межах розвитку законодавства країн ЄС з питань реалізації та захисту патентних прав було розроблено та прийнято ряд актів, зокрема, у квітні 2004 року Директиви 2004/48/ЄС, де запроваджено посилення боротьби з піратством, усунення проявів виготовлення контрафактної продукції [5].

На національному рівні адміністративно-правове забезпечення захисту та реалізації патентних прав відноситься до функціональних повноважень Українського інституту інтелектуальної власності (УІІВ). При цьому положення про зміст статутної діяльності УІІВ віднесено до переліку відомостей, що містять службову таємницю [6].

Процедура реєстрації патентних прав в Україні здійснюється відповідно до таких етапів. Першим етапом є здійснення патентно-інформаційного пошуку, що функціонально дозволяє вирішити задачі із дослідження рівня техніки та технічного оснащення реалізації патентної заявки. Патентно-інформаційний пошук здійснюється не лише на національному українському рівні, але і на рівні відповідних патентних відомств США, країн Євразії, а також в межах бази даних Всесвітньої організації інтелектуальної власності (ВОІВ).

В разі успішності патентно-інформаційного пошуку здійснюється оформлення та подача заявки, що нормативно регламентується відповідними розумними строками, обмеженими 15 робочими днями. На підставі здійснення формальної експертизи заявки на реєстрацію патентних прав, що повинно тривати до 4 місяців. За результатами формальної експертизи приймається рішення кваліфікаційної експертизи (експертизи по суті), що здійснюється на підставі клопотання про її проведення та оплати відповідного збору. Задачами здійснення кваліфікаційної експертизи є

проведення перевірки відповідності заявленого винаходу умовам патентоздатності (новизні, винахідницькому рівню, промисловій придатності).

Після успішного здійснення формальної та кваліфікаційної експертиз відбувається державна реєстрація та видача патенту, що вимагає сплати збору за реєстрацію та публікацію винаходу. Термін оплати складає 3 місяці від дати отримання відповідного рішення. Здійснення видачі патенту відбувається впродовж одного місяця після державної реєстрації винаходу.

Захист патентних прав відбувається не лише на рівні органів публічної влади, але і невідомчими організаціями, що функціонують в сфері реалізації патентного права: Всеукраїнська асоціація патентних повірених України; товариство винахідників і раціоналізаторів України; Українська асоціація власників товарних знаків, що опікується інтересами правовласників знаків.

Питання реалізації Угоди про Асоціацію України до країн ЄС вимагає імплементації положень стандартів актів європейського законодавства, що передбачено глави 9 «Інтелектуальна власність», що містить підрозділ 5 «Патенти» [7]. Отже, цілями укладеної Угоди про Асоціацію у сфері охорони прав інтелектуальної власності є забезпечення ефективності використання та комерціалізації об'єктів патентних прав на території України відповідно до стандартів країн ЄС.

Однією із ключових проблем нормативного регулювання використання патентних прав в Україні є створення інформаційних можливостей для взаємного обміну та обігу об'єктів права промислової власності, що розуміється як запровадження системи заходів із спрощення інформаційних потоків, соціально-ділового партнерства, укладення та реалізації ліцензійних договорів та договорів про здійснення науково-дослідних робіт.

Список використаних джерел:

1. Про охорону прав на винаходи і корисні моделі: Закон України від 15 грудня 1993 року № 3687-XII. URL.: https://zakon.rada.gov.ua/laws/show/3687-12#Text

2. Паризька конвенція про охорону промислової власності від 20 березня 1883 року. URL.: https://zakon.rada.gov.ua/laws/show/995_123#Text

3. Бернська конвенція про охорону літературних і художніх творів. Паризький Акт від 24 липня 1971 року, змінений 2 жовтня 1979 року. URL.: https://zakon.rada.gov.ua/laws/show/995_051#Text

4. Право Европейского Союза. Под ред. С. Ю. Кашкина. М.: Юрист, 2003. С. 697-721.

5. Капіца Ю. Напрямки адаптації законодавства України у сфері охорони інтелектуальної власності до законодавства Європейського Союзу. Право України. 2005. №1. С. 66—70.

6. Статут Державного підприємства «Український інститут інтелектуальної власності». URL.: https://ukrpatent.org/uk/articles/about

7. Угода про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL.: https://zakon.rada.gov.ua/laws/show/984_011#Text

Васечко В. О.

здобувач наукового ступеня доктора філософії кафедри конституційного права та прав людини Національної академії внутрішніх справ м. Київ, Україна

ПРАВОВІ ЗАСАДИ ОТРИМАННЯ ТИМЧАСОВОГО ЗАХИСТУ В ЧЕСЬКІЙ РЕСПУБЛІЦІ

На сьогодні Чеська Республіка є однією із європейських держав, що надали тимчасовий захист великій кількості вимушено переміщених осіб з України. За даними Управління Верховного комісара ООН у справах біженців станом на 28 лютого 2023 р. в усій Європі зареєстровано 8104606 вимушено переміщених осіб з України, з них 4881590 осіб, зареєстровані на умовах тимчасового захисту або аналогічних національних схемах захисту в Європі [1]. Варто наголосити, що зазначені дані можуть включати багаторазові реєстрації однієї особи в двох або більше країнах ЄС; реєстрації, які залишаються неповними з різних причин, а також реєстрації осіб, які переїхали далі, в тому числі за межі Європи. Після повномасштабного російського військового вторгнення найбільше переселенців прийняли Республіка Польща, Федеративна Республіка Німеччина та Чеська Республіка (*далі* – ЧС). За даними організації «Globsec» частка вимушено переміщених українців у загальній чисельності населення Чехії досягла приблизно 4,5 відсотка [2]. В Чеській Республіці станом на 26 лютого 2023 р. 493149 вимушено переміщених осіб з України отримали тимчасовий захист [1].

Директивою Ради ЄС 2001/55/ЄС від 20 липня 2001 року передбачені мінімальні стандарти для надання тимчасового захисту у випадку масового припливу переміщених осіб та заходи, що сприяють збалансованості зусиль між державами-членами щодо прийому таких осіб та вирішення наслідків щодо цього (*далі* – Директива…2001 р.) [3]. Заходи передбачені Директивою…2001 р. вперше були запроваджені рішенням Ради ЄС 04 березня 2022 року з метою підтримки населення України [4].

Тимчасовий захист в Чеській Республіці надається відповідно до Закону ЧС № 65/2022, що являє собою низку законів, які отримали назву «Lex Ukraine» [5]. Варто зазначити, що надання тимчасового захисту не означає автоматичне отримання статусу біженця. У свою чергу, особа, яка отримала тимчасовий захист, має право отримати статус біженця в порядку, встановленому законодавством держави її перебування.

Відповідно до § 2 Закону ЧС «Про деякі заходи у зв'язку з озброєним конфліктом на території України, викликаним вторгненням військ Російської Федерації» № 65/2022 від 17 березня 2022 року (*далі* – Закон 65/2022) тимчасовий захист означає дозвіл на перебування на території Чеської Республіки згідно з законом про тимчасовий захист іноземців з метою надання тимчасового захисту на території Чеської Республіки згідно з рішення Ради ЄС 04 березня 2022 р. [5].

Водночас варто наголосити, що в Чеській Республіці тимчасовий захист мають право отримати такі категорії осіб:

1. громадяни України, які проживали в Україні до 24 лютого 2022 р. та залишили країну через агресію з боку Росії;

2. громадяни третіх країн, особи без громадянства та іноземці, яким було надано будь-яку з форм міжнародного захисту в Україні, які проживали там до 24 лютого 2022 р., а потім залишили територію країни через агресію з боку Росії;

3. близькі родичі осіб, зазначених у п п. 1, 2 (чоловік/дружина, зареєстрований партнер, неодружена неповнолітня дитина та дорослий родич на утриманні родини), які проживали разом з ними в Україні до 24 лютого 2022 р., а потім разом з ними залишили країну;

4. особи без громадянства та власники посвідки на постійне проживання в Україні станом на 24 лютого 2022 р., які не можуть поїхати до країни походження через існування реальної загрози, відповідно до Закону ЧС «Про проживання іноземців» [6].

Процедура отримання тимчасового захисту громадянами України в Чехії регламентується Законом 65/2022, відповідно до якого особа, яка отримала тимчасовий захист, вважається власником візи для перебування понад 90 днів з метою продовження перебування на території Чеської Республіки відповідно до положень законодавства, що регламентує перебування іноземців на території Чеської Республіки [5].

Законодавством Чехії передбачено, що клопотання про отримання тимчасового захисту буде неприйнятним і матиме відмову у таких випадках, якщо воно подано:

1) не особисто заявником;

2) особою, не зазначеною в § 3 Закону 65/2022;

3) особою, яка звернулася за тимчасовим або міжнародним захистом в іншій державі-член Європейського Союзу;

4) особою, якій було надано тимчасовий або міжнародний захист в іншій державі-член Європейського Союзу;

5) особою, яка є громадянином ЄС або держави, пов'язаної міжнародним договором укладеним з Європейським Союзом (наприклад, Угода між ЄС і його державами-членами, з одного боку, та Швейцарською конфедерацією, з іншого, про вільне пересування людей), відповідно до якого вона має право на вільне пересування еквівалентне такому праву громадян Європейського Союзу, або держави, пов'язаної Угодою про Європейський економічний простір (додаток V і VIII до Угоди про Європейський економічний простір з внесеними до нього поправками) [5]. У випадку відмови у клопотанні, Міністерство внутрішніх справ ЧС повідомляє про причини відмови. При цьому законодавством заборонено судове оскарження такого рішення.

Надання тимчасового захисту зазначається в документі, за яким особа перетнула кордон України (як правило, це закордонний паспорт громадянина України) візовою наклейкою з терміном дії до 31 березня 2024 року. Рішення про надання тимчасового захисту приймається негайно. Але у випадках, якщо клопотання про отримання тимчасового захисту потребує з'ясування додаткових обставин, рішення приймається протягом 60 днів з дати подання заяви про отримання тимчасового захисту. Крім того, кожен іноземець, який перебуває на території ЧС, зобов'язаний протягом трьох робочих днів від дня прибуття зареєструватися у Службі поліції з питань іноземців. Цей же обов'язок мають виконувати громадяни України, які отримали тимчасовий захист, а також у випадку зміни їх адреси проживання.

Узагальнюючи, варто зазначити, що особи, які отримали тимчасовий захист в Чеській Республіці мають такі права:

1) свобода пересування та проживання в Чехії, що включає не тільки свободу пересування в межах держави, а й подорожі в межах країн Шенгенської зони;

2) право на працю;

3) право на соціальну допомогу;

4) право на медичну допомогу (отримувачі тимчасового захисту мають право повний безоплатний доступ до державної системи охорони здоров'я);

5) право на освіту;

6) возз'єднання родини, оскільки законодавством ЧС передбачено, що близькі родичі (чоловік/дружина, зареєстрований партнер, неодружена неповнолітня дитина та дорослий родич на утриманні, які спільно проживають) мають право подати клопотання про отримання тимчасового захисту;

7) на психологічну допомогу [6].

Таким чином, в Чеській Республіці на підставі Директиви…2001 р. розроблено національний механізм надання тимчасового захисту громадянам України у зв'язку з військовою агресією рф. Із метою допомоги в отриманні тимчасового захисту громадянам України, які вимушені залишити свою державу у зв'язку з війною, на території Чехії було створено та функціонують Регіональні (або Крайові) центри допомоги Україні (KACPU).

Список використаних джерел:

1. Situation Ukraine Refugee Situation. Operational data portal Ukraine refugee situation. URL: https://data.unhcr.org/en/situations/ukraine (дата звернення 04.03.2023)

2. Дзюба Дарина. Чехія прийняла найбільше переселенців з України за кількістю населення. Seznam Zprávy. URL: https://www.seznamzpravy.cz/clanek/ukrajinski-novyny-chekhiia-priiniala-naibilshe-pereselentsiv-z-ukrayini-za-kilkistiu-naselennia-225862 (дата звернення 04.03.2023)

3. Council Directive 2001/55/EC of 20 July 2001 on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between the Member States in receiving such persons and bearing the consequences: Директива Ради ЄС 2001/55/ЄС від 20 липня 2001 р. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0055 (дата звернення 04.03.2023)

4. Council Implementing Decision (EU) 2022/382 of 4 March 2022 establishing the existence of a mass influx of displaced persons from Ukraine within the meaning of Article 5 of Directive 2001/55/EC, and having the effect of introducing temporary protection: Рішення Ради (ЄС) 2022/382 від 04 березня 2022 р. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022D0382&from=EN (дата звернення 04.03.2023)

5. Zákon o některých opatřeních v souvislosti s ozbrojeným konfliktem na území Ukrajiny vyvolaným invazí vojsk Ruské federace: Zákon č. 65/2022 Sb od 17. března 2022. URL: https://www.zakonyprolidi.cz/cs/2022-65 (дата звернення 04.03.2023)

6. Чехія. Агентство Європейського Союзу з питань надання притулку (EUAA). 2022 р. URL: https://euaa.europa.eu/sites/default/files/2022-07/Booklet_Czechia_UK.pdf (дата звернення 05.03.2023)

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

Власюк Р. А.

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

ПІДВИЩЕННЯ ВИМОГ ДО ПРАЦІВНИКІВ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ В УМОВАХ ВІДДАЛЕНОЇ РОБОТИ

Інформаційна безпека для підприємства полягає у певних діях щодо вияву, усунення та нейтралізації негативних джерел, причин і умов впливу на інформацію. При цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб'єкта, в умовах якого можлива дія загроз. Досягається це системою заходів, спрямованих на попередження, вияв та ліквідацію інформаційних загроз. [1, с. 2].

Впровадження заходів та методів контролю якості інформаційної безпеки на підприємствах та організаціях стало звичним явищем останніх років. Керуючись відповідною законодавчою базою та загальноприйнятими Європейськими стандартами компанії намагаються ставити питання інформаційної безпеки на рівні з впровадженням нових технологічних процесів у виробництві.

Високий рівень залучення інформаційних технологій в управлінні компаніями, а також керуванням виробничими процесами вимагає прийняття чітких організаційно-технічних заходів щодо дотримання стандартів захисту інформації.

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб. Важливим є визначення етапів побудови політики інформаційної безпеки, а саме:

1. реєстрація всіх ресурсів, які мають бути захищені;
2. аналіз та створення переліку можливих загроз для кожного ресурсу;
3. оцінка ймовірності появи кожної загрози;

4. вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему [2].

Більшість організацій та підприємств успішно запроваджували організаційно-технічні заходи такі як:

1. Встановлення антивірусного захисту на вузлах розподілення доступу до мережі Інтернет, мережевих маршрутизаторах, серверах, кінцевих робочих станціях з регулярним скануванням та оновленням антивірусних баз.
2. Встановлення систем контролю доступу та ідентифікації.
3. Налаштуванням міжмережевих екранів та фільтрації вхідного та вихідного мережевого трафіку.
4. Криптографічний захист інформації та шифрування даних.
5. Захист мобільних пристроїв.
6. Запровадження спеціалізованих систем захисту серверного програмного забезпечення та систем управління базами даних.
7. Впровадженням комплексу перевірки цілісності встановленого програмного забезпечення та забезпечення резервного копіювання даних.
8. Встановленням апаратно-програмного комплексу захисту від зовнішніх кібер атак, а також виявлення інсайдерських порушень доступу до даних.

Вище перелічені заходи дають змогу підприємствам та організаціям в значній мірі знизити ризики витоку інформації, втрати даних та підвищити стабільність власних інформаційних систем.

Одним з найважливіших факторів успішності впровадження будь-якої системи інформаційної безпеки є тренінги та підвищення рівня кваліфікації працівників підприємства. Як показує практика, гарантоване виконання організаційних заходів інформаційної безпеки можливе в умовах перебування працівників на об'єктах підприємства, де є змога забезпечити контроль над виконанням вказаних мір. Незначна частка компаній погоджувалась на впровадження практики віддаленої роботи для працівників. Звісно, на виробництвах та підприємствах, де технологічний процес вимагає прямої присутності працівників питання віддаленої роботи неможливе. А от для представників невиробничої сфери, менеджменту та керівників практика віддаленої роботи має свою доцільність.

З настанням глобальної пандемії у 2020 році викликаної стрімким розповсюдженням вірусу COVID-19, питання переходу на віддалену роботу в умовах локдауна стало питанням виживання для багатьох компаній. Значною мірою було приділено увагу заходам інформаційної безпеки при організації режиму віддаленої роботи. Серед них варто відмітити:

1. Налаштування доступу до мережі організації через віртуальні приватні мережі (VPN).

2. Використання систем посиленої авторизації (2MFA).

3. Забезпечення працівників ноутбуками та персональними комп'ютерами з предустановленим сертифікованим програмним забезпеченням, програмами антивірусного захисту та використання для роботи користувача з обмеженими правами.

4. Обов'язковий криптографічний захист інформації при передачі та зберіганні на робочих станціях та ноутбуках.

5. Перенесення інформаційних ресурсів у “хмарні” сервіси (AWS, GCP, Azure) та використання їхніх рекомендованих систем захисту інформації та віддалених робочих місць.

Вказані заходи в значній мірі підвищують рівень інформаційної безпеки, проте вирішальним фактором залишається розуміння працівниками ступені серйозності в дотриманні поставлених вимог.

Технічні заходи не в змозі захистити від розповсюдження персональної чи секретної інформації у разі коли працівник дозволив перегляд таких даних у публічному місці. Використання публічних бездротових мереж у кафе, ресторанах чи коворкінгах ставить під загрозу передачу даних у зашифрованому форматі. Залишення не заблокованого ноутбука у публічному місці чи навіть удома може призвести до несанкціонованого доступу до захищених даних чи навіть їх втрати. Слабкий захист від злому домашніх мережевих маршрутизаторів є потенційною загрозою несанкціонованого доступу до мережевих ресурсів компанії.

Базуючись на проведеному аналізі, можна зробити висновки, що в умовах віддаленої роботи на працівника покладається відповідальність не лише у дотриманні політик інформаційної безпеки які діяли на підприємстві чи організації, але й у додаткових заходах, таких як: забезпечення захисту робочих станцій та ноутбуків, вибору відповідного місця роботи, відповідний захист домашньої комп'ютерної мережі та мережевих пристроїв, дотримання інформаційної гігієни у користуванні мережею Інтернет.

Звісно не кожен працівник здатен повною мірою самостійно забезпечити виконання вказаних додаткових заходів. Технічні спеціалісти компанії зобов'язані також проводити регулярні тренінги та забезпечити інструкціями працівників переведених у режим віддаленої роботи для підтримання належного рівня інформаційної безпеки.

Список використаних джерел:

1. Коваленко Ю. О., Забезпечення інформаційної безпеки на підприємстві, Економіка пром-сті. — 2010. — № 3. — С. 123-129. — Бібліогр.: 11 назв. — укр.

2. Легомінова С. В., Теоретичні засади інформаційної безпеки підприємства, журнал "Економіка. Менеджмент. Бізнес" № 3, 2015.

Воробьев И. О.

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

ОЦЕНКА СПОСОБНОСТИ ПЕРСОНАЛА ПРЕДПРИЯТИЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ К ПРОТИВОДЕЙСТВИЮ КИБЕРУГРОЗАМ

В современных условиях кибербезопасность является одной из важнейших составляющих функционирования любого предприятия, особенно если оно является частью критической инфраструктуры. Защита от киберугроз должна быть внесена в каждый этап жизненного цикла предприятия, включая оценку способности персонала к противодействию киберугрозам.

Оценка способности персонала к противодействию киберугрозам является важным элементом стратегии кибербезопасности предприятия. Это позволяет предприятию обеспечить высокий уровень защиты от киберугроз, учитывая человеческий фактор, который может быть слабым звеном в системе кибербезопасности.

Первым шагом в процессе оценки способности персонала является определение потенциальных угроз, которые могут возникнуть в сфере кибербезопасности. После этого необходимо провести анализ, который покажет, насколько компетентны сотрудники предприятия по предотвращению и выявлению киберугроз, а также их умение реагировать на эти угрозы.

Для проведения оценивания можно использовать различные методики, в частности проводить тестирование и симуляции ситуаций, касающихся кибербезопасности. Также можно проводить тренинги и учебные курсы, которые помогут сотрудникам повысить уровень своей компетентности в сфере кибербезопасности.

Кроме того, необходимо установить процедуры контроля и отслеживания результатов оценки, чтобы обеспечить постоянное совершенствование системы кибербезопасности предприятия. Это можно осуществлять через систему отчетности, которая позволит выявлять слабые места в кибербезопасности и принимать необходимые меры по их устранению.

Оценка способности персонала предприятий критической инфраструктуры к противодействию киберугрозам имеет большое значение для обеспечения надежности и безопасности функционирования предприятия. Применение системы оценки поможет повысить уровень компетентности персонала в сфере кибербезопасности, что позволит эффективно предотвращать и выявлять киберугрозы, а также своевременно реагировать на них.

Одним из важных этапов оценки является идентификация категорий персонала, которые занимаются предотвращением и выявлением киберугроз. Например, это могут быть инженеры по информационной безопасности, системные администраторы, специалисты по сетевой безопасности и другие.

Также важно обратить внимание на уровень подготовки персонала, занимающегося кибербезопасностью. Например, если у предприятия нет специалистов с соответствующим образованием, то необходимо провести обучение и курсы для повышения их уровня компетентности.

Кроме того, необходимо учитывать технические возможности и инфраструктуру, которая используется для защиты от киберугроз. Например, если предприятие использует устаревшие программные средства и оборудование, то возникает угроза подрыва кибербезопасности. Поэтому важно оценивать не только персонал, но и технические средства, которые используются для защиты от киберугроз.

Оценка способности персонала предприятий критической инфраструктуры к противодействию киберугрозам должна стать постоянным процессом в рамках предприятия. Обеспечение кибербезопасности является важной составляющей функционирования предприятия, поэтому необходимо постоянно повышать уровень компетентности персонала и использовать современные технологии и методики защиты от киберугроз.

Одним из примеров оценки способности персонала к противодействию киберугрозам может быть проведение тестирования на знание основных принципов информационной безопасности. Например, предприятие может провести тестирование для инженеров по информационной безопасности, которые занимаются предотвращением и выявлением киберугроз. В рамках тестирования могут быть предложены вопросы о защите от взлома паролей, использовании защиты от вирусов и других угроз.

Другой пример - проведение практических учений и тренингов по противодействию киберугрозам для персонала предприятия. Например, это может быть симуляция атаки с использованием различных методов атаки и защиты от них, что позволит проверить знания и навыки персонала.

Также важно проводить аудит безопасности внутренней сети и инфраструктуры предприятия с целью выявления возможных слабых мест и рисков. Например, можно использовать программные средства для сканирования сети и выявления возможных уязвимостей, а также анализировать журналы безопасности для выявления необычной активности.

Кроме того, важно проводить периодический обзор и анализ деятельности персонала предприятия с целью выявления возможных нарушений безопасности. Например, это может быть анализ доступа к системе и действий, которые были выполнены, а также выявление необычной активности или попыток выполнить неправомерные действия.

Все эти примеры могут помочь предприятиям критической инфраструктуры улучшить свою способность к противодействию киберугрозам. При этом необходимо учитывать тот факт, что киберугрозы постоянно меняются и эволюционируют, поэтому персонал предприятия должен быть готов к быстрому реагированию на новые угрозы и постоянное самообразование в этой области.

Оценка способности персонала к противодействию киберугрозам является важным элементом информационной безопасности предприятия, позволяющим обеспечить надлежащий уровень защиты от киберугроз. Правильно организованный процесс оценки поможет выявить возможные проблемы и риски и разработать план действий для улучшения безопасности.

В мире, где киберугрозы становятся все более сложными и распространенными, оценка способности персонала к противодействию киберугрозам является ключевым элементом информационной безопасности предприятий критической инфраструктуры. Для достижения успеха в этой области необходимо иметь высококвалифицированный персонал, готовый к постоянному самосовершенствованию и реагированию на новые вызовы.

Список использованных источников:

1. Агентство по кибербезопасности и инфраструктурной безопасности (CISA). (2021). Инструмент оценки кибербезопасности. Получено с сайта https://www.cisa.gov/cybersecurity-evaluation-tool.

2. Национальный институт стандартов и технологий (2020). Framework for Improving Critical Infrastructure Cybersecurity. Получено с сайта https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity.

3. Управление директора национальной разведки (ODNI). (2020). Cyber Threats to Critical Infrastructure: An Intelligence Perspective. Получено с сайта https://www.dni.gov/files/CTIIC/documents/CTIIC_2019_Report_Final.pdf.

4. Ponemon Institute. (2019). 2019 Cost of a Data Breach Report. Получено с сайта https://www.ibm.com/security/data-breach.

5. SANS Information Security White Papers (2021). Building a Cybersecurity Awareness and Training Program. Получено с сайта https://www.sans.org/white-papers/40106/.

6. United States Government Accountability Office (GAO). (2018). Cybersecurity Workforce: Agencies Need to Implement Strategies to Address Persistent Challenges. Получено с сайта https://www.gao.gov/assets/gao-19-128.pdf.

Грішко Д. Ю.

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

ЗВ'ЯЗОК ПРОБЛЕМ ЕТИКИ ТА КІБЕРБЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Розвиток Штучного Інтелекту (ШІ) привів до небачених раніше досягнень технології, але також викликає етичні питання. Кібербезпека, з іншого боку, відіграє важливу роль у захисті фізичних осіб та організацій від кібератак. Ця робота аналізує зв'язок між кібербезпекою та етикою ШІ, та як ці два напрями можуть доповнювати один одного.

Прогнозується, що до 2030 року в наших домівках та офісах буде приблизно 125 мільярдів розумних пристроїв [1]. Ці пристрої матимуть можливість відчувати, обробляти та приймати рішення без отримання дозволу від хмарних сервісів чи від людей. Оскільки ми дедалі більше покладаємося на ці пристрої, щоб вони брали на себе більш активну та відповідальну роль у нашому житті, важливо переконатися, що вони працюють безпечно та надійно, дотримуючись етичних стандартів. Це означає, що нам потрібно довіряти технологіям штучного інтелекту та машинного навчання, які їх приводять в дію, щоб вони не лише були етичними, але й працювали в безпечному та надійному режимі.

Етика ШІ. Для досягнення цієї мети різні країни, такі як США та ЄС [2], розпочали роботу над законами та регуляторними актами, спрямованими на регулювання впливу штучного інтелекту на кінцевих користувачів. Крім того, декілька технологічних компаній та організацій [3] співпрацюють для розробки етичних кодексів поведінки для штучного інтелекту, які базуються на ключових принципах конфіденційності, прозорості та справедливості. Європейська комісія “European Commission’s High Level Expert Group” визначила наступні базові права які технології не мають порушувати [4]:

- Повага до людської гідності.
- Свобода особистості.
- Повага до демократії, справедливості та верховенства права.
- Рівність, відсутність дискримінації та солідарність.

Та 4 основні принципи етики ШІ:

- Повага до автономії людини.
- Запобігання шкоди.

- Справедливість.
- Зрозумілість.

Отже можна прослідкувати, що питанням етики штучного інтелекту активно займаються та обговорюють структури різного походження, від корпорацій, держав до релігійних установ [3].

Кібербезпека програмного забезпечення ШІ. Для забезпечення етичного та безпечного ШІ не достатньо лише надійного програмування машин з наслідуванням правил кібербезпеки. Як у багатьох інших галузях, ШІ-програми та пристрої потребують сильної структури та підтримки ПЗ, щоб забезпечити безпечні та найбільш етичні рішення. Також потрібні фізичні заходи безпеки у разі виникнення проблем. Це особливо важливо в контексті Інтернету Речей (IoT) та обчислення на межі мережі, де ШІ стає все більш важливою складовою. За оцінками Deloitte [5], у 2020 році було продано більше 750 млн чіпів ШІ. Deloitte також передбачає, що до 2024 року продажі зростуть до понад 1,5 млрд чіпів. Потужність обробки ШІ значно збільшується, а чіпи стають ключовою складовою смартфонів, термостатів, відеокамер, дверних дзвінків та динаміків. З такої тенденції очевидно, що ступінь інтегрування розумних технологій у наше буде критично високим, тому питання підходів до розробки безпечних та етичних рішень виходить на новий рівень.

Щоб створити штучний інтелект, якому можна довіряти, важливо:

- Створювати системи, які можуть навчатись від людей та працювати з ними у зрозумілий та явний спосіб.
- Безпека та конфіденційність повинні бути враховані з самого початку створення будь-якої нової технології, а не додаватись пізніше.
- Максимальний рівень безпеки та захисту даних повинен бути вбудований як в апаратне, так і в програмне забезпечення, і його повинні враховувати на кожному етапі процесу розробки та ланцюжка постачання, від проектування до бізнес-моделей технології.

Ініціатива “The Charter of Trust” [6], що створена за участю великих корпорації, державних та наукових структур, пропонує принципи для наслідування щодо методології та перевірки, що ґрунтується на оцінці ризику. Такі принципи мають бути включенні у процес розробки.

Після визначення основних принципів, які керуватимуть розвитком штучного інтелекту, також потрібно знайти способи забезпечити, щоб етичні системи штучного інтелекту не були скомпрометовані. Машинне навчання може виявляти аномалії в даних, але, на жаль, його також можна використовувати зловмисниками для збільшення ефективності кібератак.

Тому забезпечення цілісності та безпеки систем штучного інтелекту є так само важливим, як і розробка їх з етичної точки зору.

Важливо акцентувати увагу на способах використання апаратного забезпечення безпеки як засобу запобігання та захисту від атак штучного інтелекту, що можуть витягувати конфіденційну інформацію з захищених систем. Це підвищить загальний рівень безпеки та конфіденційності даних в системі.

Сьогодні великим викликом є те, що екосистема штучного інтелекту є мозаїкою внесків різних розробників, але забезпечення консистентності та повної інтеграції є ключовими вимогами етичного ШІ. Наразі рівень відповідальності та довіри серед учасників розробки ШІ неоднаковий та нестабільний, а найменша вразливість в принципі "захист та конфіденційність за дизайном" може призвести до зруйнування всієї екосистеми при атаках зловмисників. Тому кожен учасник сфери ШІ має працювати над сумісними та оцінюваними заходами безпеки.

Потрібен час, щоб розробники ШІ змогли узгодити універсальний кодекс етики, і ще довше, щоб кінцеві користувачі переконались, що пристрої ШІ будуть діяти в інтересах людства. Перед тим, як ми зможемо працювати над створенням безпечних та надійних систем ШІ, потрібно стандартизувати положення щодо безпеки і захисту в усіх системах обчислень на всіх дотичних точках систем. Як виробники мікросхем та процесорів, так і їхні клієнти повинні надавати пріоритет сертифікації зв'язку, апаратному забезпеченню та взаємодії, працюючи разом, щоб створити безпечні та надійні системи ШІ для майбутнього.

Список використаних джерел:

1. *News Release | IHS Markit Online Newsroom. Overview | IHS Markit Online Newsroom. – [Електронний ресурс]. – Доступ: https://news.ihsmarkit.com/prviewer/release_only/slug/number-connected-iot-devices-will-surge-125-billion-2030-ihs-markit-says.*
2. *Murgia M., Shrikanth S. How governments are beginning to regulate AI. Financial Times. – [Електронний ресурс]. – Доступ: https://www.ft.com/content/025315e8-7e4d-11e9-81d2-f785092ab560.*
3. *Copestake B. J. AI ethics backed by Pope and tech giants in new plan. BBC News. – [Електронний ресурс]. – Доступ: https://www.bbc.com/news/technology-51673296.*
4. *EU: High level expert group on artificial intelligence. Ethics guidelines for trustworthy AI (2019). – [Електронний ресурс]. – Доступ: https://www.aepd.es/sites/default/fles/2019-12/ai-ethics-guidelines.pdf*
5. *Bringing AI to the device: Edge AI chips come into their own. Deloitte Insights. – [Електронний ресурс]. – Доступ: https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2020/ai-chips.html.*
6. *Charter of Trust. – [Електронний ресурс]. – Доступ: https://www.charteroftrust.com/.*

Малюга Ю. І.

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

КІБЕРВІЙНА ЯК СКЛАДОВА ГІБРИДНОЇ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ 2013-2022 РОКУ

Росія та Україна активно ведуть боротьбу на кіберфронті вже протягом десяти років. Так у 2013 році під час масових протестів, які згодом переросли у Революцію гідності, протистояння відбувались в соціальних мережах, де невідомі особи почали масово використовувати нетботи з метою засмічення інформаційного поля, введення людей в оману та поширення чуток. Крім засмічення українського інфопростору, атакам також піддався такий традиційний спосіб зв'язку як мобільний зв'язок. Використовуючи механізми автоматичних дзвінків, атаки скеровувались на телефони окремих активістів чи політиків, що впливало на ефективність їхньої комунікації та ускладнювало координації організаторів протесту. Початок збройної агресії Російської Федерації проти України знаменує й ескалацію конфлікту на кіберфронті. Підтвердженням цього є події 2014 року, коли Росія запустила масштабну DDoS-атаку на Дарницьку ТЕЦ. Згодом подібні атаки поширились на державно-військовий сектор України та галузь критичної інфраструктури і, якщо порівнювати з довоєнним періодом, їхня чисельність зросла на 196% [1]. Хоча такі атаки завдали серйозних політичних й економічних втрат (середній економічний збиток через недоступність сайту складає 22 000 американських доларів на хвилину, тоді як подібні атаки тривали близько години [2]), вони значно мобілізували українську владу й бізнес та призвели до залучення інвестицій у сферу кіберзахисту. Це у свою чергу відіграло ключову роль у наступній фазі війни, яка розпочалась із широкомасштабним вторгненням Росії в Україну 24 лютого 2022 року. В цій роботі я хочу зосередитись на аналізі кібервійни України і Росії в період з 2014 по 2022, розглянути засоби і техніки, які для цього використовувались, а також зупинитись на залучених хакерських групах та в кінці розглянути концепцію кіберстійкості, як дієвого засобу боротьби з кіберзагрозами на рівні держави.

Для кращого розуміння специфіки ведення кібервійни варто зрозуміти слабкості комп'ютерної мережі та принципи, за якими обирають жертву для атаки. Найбільш вразливими до атак є системи з єдиної точкою відмови, які

поширені серед АСДУ-систем (автоматизована система дистанційного управління). Такі системи використовуються у всіх галузях господарства, в тому числі і в галузях критичної інфраструктури, де потрібно забезпечувати операторський контроль за технологічними процесами в реальному часі. У багатьох складних системах отримання доступу до єдиних точок відмов може призвести до одномоментного краху всього процесу в системі. Складність для захисту подібних систем додає ще той факт, що нападник у кіберпротистоянні завжди має перевагу, так як йому потрібно докласти менших зусиль в порівнянні зі стороною, яка обороняється. Враховуючи, що не існує ідеальної системи захисту від подібних атак, стратегія кіберзахисту полягає в зосередженні на обороні частин, які є критичними для функціонування системи. Це дозволяє отримати достатньо ефективний захист, вартість якого не буде перевищувати вартості самої атаки. Наступною поширеною слабкістю є монокультурне програмне забезпечення. Використання єдиного програмного забезпечення є поширеним явищем, оскільки воно дозволяє значно спростити та оптимізувати процеси ведення бізнесу. Проте ціною такої оптимізації є потенційна схильність системи до проникнення. Саме цю слабкість використали розробники вірусу Petya, який в 2017 році зміг вразити низку українських компаній і відомств. Серед постраждалих були як і державні установи, національна пошта, метрополітен Києва, міжнародний аеропорт "Бориспіль", так і низка ЗМІ, банків та комерційних структур [3]. Згодом стало відомо, що дія вірусу поширюється лише на комп'ютери з системою Windows, так як злочинцям вдавалось сфальсифікувати електронний підпис Microsoft.

Проаналізувавши загальні слабкості комп’ютерної мережі, перейдемо до аналізу методів та інструментів, які використовувались для введення кібервійни як складової російсько-української війни в період з 2013 по 2022 рік. Найбільш поширеними та простими в реалізації є DdoS атаки (розподілена атака на відмову в обслуговуванні) та атаки спрямовані на зламування конкретного сайту. Для розподілених атак використовувались комп’ютери користувачів, які були заражені ботнетами, тоді як самі користувачі й не здогадувалася, що є залученими до атаки. Цей тип кібератак був застосований обома сторонами конфлікту: наприклад, у листопаді 2013 року проросійські хакери напали на українські новинні сайти, а в грудні 2013 року вже російські новинні сайти були атаковані. DDoS-атаки також використовувались як відволікаючий маневр. Поки жертва була сфокусована над усуненням наслідків атаки, опонент намагався встановити шкідливе програмне забезпечення для викрадення даних. Надалі

розглянемо два наймасштабніші випадки застосування програм такого типу. Першою з них є троянські програми групи BlackEnergy, які використовувались для атаки на енергетичну систему в північній частині Києва в 2015 році. Ця атака мала комплексний характер з такими складовими: попереднє зараження мереж за допомогою підроблених листів електронної пошти; захоплення управління АСДУ, що призвело до відключень підстанцій; знищення інформації на серверах та робочих станціях за допомогою функції KillDisk; атака на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів. Наступним прикладом є атаки за допомогою троянської програми X-Agent. Її основними цілями були пристрої українських військових, які використовувались для наведення артилерії. Ця атака демонструє, що кібершпіонаж використовується не лише з економічної чи політичної вигоди, але й для прямої підтримки фізичних бойових дій.

Надалі хотілося б зупинитись детальніше на дійових особах російсько-української кібервійни. Визначення винних у злочинах в кіберпросторі є надзвичайно складною задачею. Зазвичай використовується логіка «cui bono» - кому це вигідно - але завжди існує невизначеність щодо винних. До основних джерел, на основі яких будуються подібні висновки, відносять академічні журнали, провідні західні ЗМІ та фірми з кібербезпеки. Однак існує можливість того, що технічні докази, знайдені в кіберпросторі, можуть бути спеціально підготовлені однією стороною, щоб підставити іншу. У випадку війни в Україні, питання визначення винних є особливо складним через обсяг кібератак та те, що обидві сторони використовують проксі-сервери. Використання проксі-серверів дозволяє державам мати можливість заявити, що вони не мають ніякого стосунку до атак, які були проведені через ці сервери, адже вони можуть заперечити будь-яку причетність до цих груп, заявляючи, що вони діяли на власну відповідальність без будь-якої підтримки від держави. Для класифікації учасників цієї війни варто використовувати політичну орієнтацію, а не лише приналежність до однієї чи іншої країни. Наприклад, згідно з проведеними українськими дослідженнями, деякі проросійські хакерські групи здійснювали свої атаки з територій України, щоб обійти територіальні фільтри, які блокують Інтернет-протоколи (IP-адреси), що приходять з Росії. Спершу розглянемо проукраїнських учасників цього конфлікту та їхню роль у боротьбі з ворогом. До найбільш відомих учасників відносять організацію Інформаційних військ України та Кіберсотня. Діяльність обох цих організацій є цілком легальною, оскільки не передбачає злому сайтів опонента. Натомість учасники цих організацій працюють над очищенням

українського інфопростору від російської пропаганди та навчанням фірм і населення методами протистояння кібератакам. Також є інший тип учасників, такий як організація Null Selector, які спеціалізуються на проведенні розподілених атак на відмову в обслуговуванні (DdoS атаки) російських медіа. Із проросійської сторони залученими були хакерські групи APT28 та APT29, яких пов'язують із Головним розвідувальним управлінням Росії (ГРУ) та Федеральною службою безпеки Росії (ФСБ) відповідно. Окрім злочинів проти України, учасники цих груп брали участь у війні Росії проти Грузії в 2008 році та вторгненні у систему Демократичного Національного Комітету США в 2016 році. Також російське керівництво активно залучало у війну тролів для розповсюдження пропаганди та атак на українських активістів. Одна з таких ферм тролів була виявлена в Санкт-Петербурзі, де тролі були розміщені в секторах, відповідальних за різні медіа, та отримували квоти на коментарі та пости, які мали бути написані щодня.

Наостанок, варто розглянути стратегію кіберстійкості на рівні держави як дієвий засіб для протидії кіберзагрозам. Кожна країна та організація вирішують питання кібербезпеки по-різному через різні причини, проте всі згодні, що необхідний комплексний підхід для вирішення проблем та питань кібербезпеки. Враховуючи український контекст, як на мене, доцільно буде розглянути випадок імплементації такої стратегії в Малайзії, що також відноситься до країн, які розвиваються. У 2019 році в країні було створено Національне агентство з кібербезпеки (National Cyber Security Agency, NACSA) з метою координації та впровадження національних стратегій кібербезпеки, включаючи кіберстійкість. NACSA розробило Національну політику з кібербезпеки та Національну стратегію з кібербезпеки, які надають рамки для впровадження кіберстійкості на національному рівні. Для впровадження стратегії кіберстійкості Малайзія прийняла кілька кроків, таких як створення навчального центру Cyber Range для професіоналів кібербезпеки, запуск онлайн-платформи для звітування про кіберінциденти (Cyber999) та співпрацю з міжнародними партнерами для обміну інформацією та передачі кращих практик з кібербезпеки. Станом на 31 грудня 2021 року, завдяки платформі Cyber999 було виявлено більше 10 000 кіберзагроз [4]. Тож саме імплементація подібної комплексної стратегії кіберстійкості Україною на державному рівні є наступним логічним кроком для протистояння можливим кіберзагрозам у майбутньому.

Список використаних джерел:

1. Як Росія та Україна воюють на кіберфронті. Українська Правда. 2022. URL: https://www.epravda.com.ua/columns/2022/09/28/691925/

2. Baezner M. Cyber and Information warfare in the Ukrainian conflict. Center for Security Studies (CSS). Цюрих. 2018. 54 с.

3. Аросєв. Г. Кібератака вірусу Petya: що відомо. Deutsche Welle. 2017. URL: https://p.dw.com/p/2fXKk

4. Azwa N. Binti A. Aziz A. A Proposal in Having A Cyber Resilience Strategy for The Critical National Information Infrastructure Sectors in Malaysia. OIC-CERT Journal of Cyber Security. 2022. URL: https://www.oic-cert.org/en/journal/vol-4-issue-1.html#.Y_OGy3bMI2w

Мацько В. А.

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

КІБЕРБЕЗПЕКА ТА КІБЕРРИЗИКИ В АВТОНОМНИХ ТА НАПІВАВТОНОМНИХ АВТОМОБІЛЯХ

За оцінками експертів, до 2025 року на дорогах буде близько 8 мільйонів автономних або напівавтономних автомобілів.

Товариство автомобільних інженерів (SAE) визначає 6 ступенів автоматизації водіння в діапазоні від 0 (повністю ручний) до 5 (повністю автономний) [1].

- Рівень 0 (без автоматизації водіння)
- Рівень 1 (допомога водієві)
- Рівень 2 (часткова автоматизація водіння)
- Рівень 3 (умовна автоматизація водіння)
- Рівень 4 (високий рівень автоматизації водіння)
- Рівень 5 (повна автоматизація водіння)

Незважаючи на те, що майбутнє автономних автомобілів є інтригуючим і захоплюючим, масове виробництво не перевищить другого рівня протягом найближчих років. Не через технічну спроможність, а через недостатню безпеку.

Споживачі не приймуть автономні транспортні засоби, поки не переконаються, що вони будуть принаймні такими ж безпечними, як і комерційні літаки, поїзди чи автобуси. Цього результату вдасться досягти, але спершу автомобільний сектор повинен подолати кілька перешкод.

Громадськість, федеральні, державні та муніципальні органи влади, а також регуляторні органи та агенції зі стандартизації все більше усвідомлюють необхідність кібербезпеки. Один із прикладів: у 2016 році ФБР і NHTSA опублікували попередження для широкої громадськості та виробників автомобілів, транспортних компонентів і вторинних пристроїв, про «обізнаність щодо можливих вразливостей та загрози кібербезпеці, пов’язаних з транспортними технологіями в сучасних автомобілях». У січні 2016 року NHTSA також організувала відкритий круглий стіл, щоб заохотити різні зацікавлені сторони до обговорення питань кібербезпеки транспортних засобів. Були присутні представники 17 виробників автомобілів, 25 державних установ і 13 галузевих організацій.

Нещодавні рекомендації Європейської економічної комісії ООН (ЄЕК ООН) щодо «кібербезпеки та системи управління кібербезпекою» описують, як зацікавлені сторони можуть координувати свої зусилля в розробці структур для управління загрозами кібербезпеці автономних транспортних засобів. Метою рекомендацій є створення основи для кібербезпеки транспортних засобів у багатьох регіонах земної кулі.

Поступове збільшення обсягу обчислень у звичайних автомобілях у другій половині 20-го століття зробило їх сприйнятливими до кібератак, створивши основу для поточних занепокоєнь. Транспортні засоби швидко стають функціональними активами та універсальними платформами; вони не лише перевозять людей з одного місця в інше. Таким чином, внесок виробників оригінального обладнання (OEM) у вартість автомобіля змінюється на користь програмного забезпечення порівняно з апаратним забезпеченням.

Зростаюча надмірна залежність від програмного забезпечення та зовнішнього підключення, наприклад для оновлення програмного забезпечення та моніторингу технічного обслуговування, породжує нові проблеми кібербезпеки для автомобілів і AV-пристроїв, зокрема. На відміну від традиційних автомобілів, автономні транспортні засоби керуються програмним забезпеченням. Навіть за помірного, часткового рівня автоматизації, такого як автоматичне паркування, існують значні загрози кібербезпеці. Недостатня кібербезпека може дозволити ворожим особам взяти під контроль транспортний засіб або вивести його з ладу, наказати автономному транспортному засобу (AV) змінити своє положення або атакувати інфраструктуру, пов’язану з AV через мережі, такі як камери та світлофори.

Застосування штучного інтелекту та методів машинного навчання (ML) автономними автомобілями загострює проблеми кібербезпеки. Штучний інтелект використовується автономними автомобілями для опрацювання величезних обсягів даних, зібраних їхніми камерами та датчиками, для розпізнавання дорожних знаків та дорожньої розмітки, ідентифікації інших транспортних засобів у русі, планування маршруту тощо. Незважаючи на те, що ШІ використовується для підвищення безпеки, це створює додаткову небезпеку системних помилок, таких як неправильне сприйняття оточення. Деякі з цих неточностей можуть бути створені навмисно, наприклад, незначною зміною візуальних зображень вуличних знаків або використанням складних зображень, які призначені для того, щоб ввести в оману системи ML, таким чином ускладнюючи використання ними машинного бачення та створюючи небезпечні обставини.

Зменшення сприйнятливості штучного інтелекту до спуфінгу - неправдивого представлення за допомогою хибних зображень та інших махінацій - матиме вирішальне значення для захисту AV.

Проте оскільки штучний інтелект покладається на величезні обсяги даних, занепокоєння щодо конфіденційності і збереження даних можуть посилити недовіру до автономних транспортних засобів.

Багаторівневий підхід до кібербезпеки транспортних засобів зменшує ймовірність успішної кібератаки та пом'якшує можливі наслідки успішної атаки. Ретельна та методична стратегія створення багатошарових заходів кібербезпеки для автомобілів включає наступне:

- Визначення пріоритетів ідентифікації та захист важливих систем автомобіля залежно від ризику.
- Своєчасне виявлення та вирішення можливих подій пов'язаних з кібербезпекою автомобіля.
- Архітектура, процедури та заходи, які включають кібербезпеку та кібервідмовостійкість у свій дизайн, що дозволяє швидко відтворити інцидент.
- Методи ефективного обміну даними та інформацією в усьому секторі для прискорення впровадження найкращих галузевих практик.

У минулому було задокументовано кілька атак пов'язаних з автономними транспортними засобами. У 2010 році дослідники з Університету Каліфорнії в Сан-Дієго та Університету Вашингтона провели один із перших зломів автомобіля. Використовуючи бортову телематичну систему та зворотне проектування, вони змогли отримати повний контроль над автомобілем.

Тим не менш, дослідники співпрацювали з компанією і не розкрили весь масштаб уразливості. У наступні роки було проведено низку додаткових робіт, спрямованих на зворотне проектування блоків керування автомобілями. Однак усі ці спроби вимагали фізичної присутності зловмисника всередині цільового автомобіля. Як наслідок, ЗМІ приділяли мало уваги цим атакам через їхню малоймовірність [2].

Ситуація змінилася в 2015 році, коли двоє дослідників безпеки провели першу серйозну дистанційну атаку на немодифікований Jeep Cherokee 2014 року [3]. Дослідники виявили програмну помилку в інформаційно-розважальній системі автомобіля, яка дозволяла їм дистанційно підключатися до автомобіля через 4G LTE і надсилати сигнали CAN на ECU. Вони демонстрували різноманітні атаки, починаючи від дистанційного керування основними функціями автомобіля, такими як радіо, кондиціонер і

склоочисники, до керування більш важливими функціями, такими як гальма, трансмісія та навіть вимикання двигуна, коли автомобіль був на шосе.

Цей злом викликав масовий резонанс у ЗМІ, і виробник був змушений розробити оновлення для усунення вразливості. У 2016 році ті ж дослідники виявили ще одну вразливість, яка дозволяла дистанційно керувати системами прискорення, керма та круїз-контролю автомобіля.

У 2016 році було виявлено, що зловмисник з Австралії зміг дистанційно керувати Nissan Leaf в Англії. Ці напади змінили ландшафт автомобільних кібератак і підкреслили необхідність уваги до кібербезпеки в автомобілях.

З 2018 року набула популярності окрема категорія нападів, які здебільшого спрямовані проти систем ADAS і бортових датчиків. Дослідники ввели кілька значних візуальних змін до знаку "стоп" [4], через що система помилково сприйняла його за знак обмеження руху 45 миль на годину.

Кілька років тому дослідники змогли засліпити камеру Mobileye C2-270 і здійснити глушіння, підробку та ретрансляцію датчика Ibeo LUX3 LiDAR. Лабораторія безпеки Tencent Keen в 2019 році обдурила систему зміни смуги руху Tesla Model S, використовуючи яскраві наклейки на дорозі.

Дослідники змогли дистанційно виконати програмний код (RCE) через WiFi в інформаційно-розважальній системі Tesla Model 3 за допомогою дрона. Вони отримали змогу дистанційно отримувати доступ до дверей і багажника, а також регулювати налаштування сидінь, кермування та режими прискорення. Тим не менш, ця вада не дає доступу до управління кермом автомобіля.

Як висновок ми можемо сказати, що кібербезпека може мати значний вплив на успіх автономних транспортних засобів.

Інші зовнішні елементи, такі як розумні міста та участь регуляторів у ключових країнах, таких як Сполучені Штати, Європа та Китай, також відіграватимуть значну роль у цьому процесі.

Нарешті, важливо відзначити, що зараз розвивається спеціалізована індустрія кібербезпеки з індивідуальними рішеннями для автомобільної промисловості. Її здатність протистояти загрозам, що швидко розвиваються, безсумнівно, відіграватиме роль у визначенні успіху автономних автомобілів.

Список використаних джерел:

1. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. 2018.

2. *K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in IEEE symposium on security and privacy, 2010.*

3. *C. Valasek, and C. Miller, "Remote Exploitation of an Unaltered Passenger Vehicle," in Black Hat USA, 2015.*

4. *K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, "Robust physical-world attacks on deep learning visual classification," in Proc. of IEEE CVPR, 2018.*

Медвідь І. А.

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

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБ-ДОДАТКІВ

Світ надзвичайно залежить від Інтернету. Зараз веб-безпека є найбільшою проблемою в корпоративному світі. Він вважається основною структурою для всесвітнього суспільства даних. Веб-додатки схильні до атак на безпеку. Веб-безпека — це захист рівня веб-додатків від атак неавторизованих користувачів. Багато проблем, які виникають у веб-додатках, головним чином пов’язані з неправильним введенням, наданим клієнтом.

У цій статті обговорюються різні аспекти веб-безпеки та її слабкі сторони. У цьому документі також обговорюються основні елементи техніки веб-безпеки, такі як паролі, шифрування, автентифікація та цілісність. Анатомія атаки веб-додатків і методи атаки також розглядаються детально. У цій статті розглядається ряд методів боротьби з цим класом загроз і оцінюється, чому вони не виявилися більш успішними. У цьому документі пропонується кращий спосіб мінімізації веб-уразливостей такого типу. Він також забезпечує найкращі механізми безпеки для зазначених атак.

Веб-безпека є важливим аспектом веб-додатків. Сьогодні веб-безпека є справжньою проблемою, пов’язаною з Інтернетом. Він вважається основною структурою для всесвітнього суспільства даних. Веб-програми забезпечують кращий інтерфейс для клієнта через веб-сторінку. Сценарій веб-сторінки виконується у веб-браузері клієнта.

Веб-програми є основною базою атак, таких як міжсайтовий скриптинг, крадіжка сеансу cookie, атака на браузер, черв’яки, що саморозповсюджуються в електронній пошті та на веб-сайтах. Ці типи атак називаються «атаками ін’єкцій», які атакують за допомогою шкідливого коду. Атаки ін’єкцій займали найвищу позицію в списках уразливостей веб-додатків протягом значної частини попереднього десятиліття.

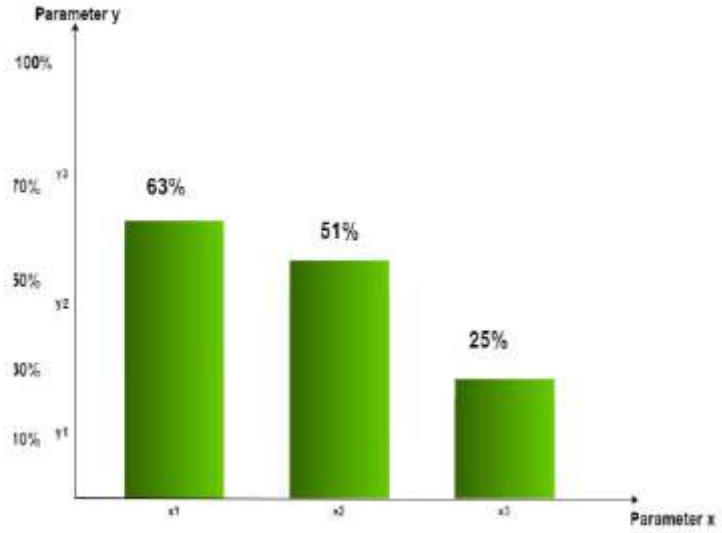


Рисунок 1. Відсоток веб-сайтів, що містять уразливості

Сьогодні існує дві найпоширеніші вразливості безпеки: впровадження SQL і міжсайтовий сценарій. Оцінка безпеки програми defencecenter, яка містила понад 250 програм електронної комерції, онлайн банківські та корпоративні сайти висунули заяву про те, що понад 85% веб-додатків уразливі до атак [2].

Основна проблема в дослідженнях веб-безпеки полягає в тому, щоб надати користувачеві безпечну та надійну платформу для спілкування з веб-програмою. Але деякі люди продовжують вести бізнес із незахищеним сайтом. Деякі організації чи компанії не хочуть розкривати інформацію про власні діри в безпеці. Отже, отримати достовірну інформацію про стан веб-безпеки сьогодні дуже складно [1], [3], [4], [8], [11].

Сьогодні існує дві поширені важливі вразливості системи безпеки: впровадження SQL і міжсайтовий сценарій. Ці типи вразливостей безпосередньо впливають на веб-сервери, сервери додатків і середовище веб-додатків. [3], [4], [5], [7].

У цьому документі OWASP досліджує ряд Таблиця 1: Причини атак [2] методів виявлення загроз і оцінки, чому вони не виявилися більш ефективними. У цьому документі пропонується кращий механізм для мінімізації такого типу веб-уразливостей. Зараз у веб-додатках існує багато ризиків конфіденційності. Сьогодні занадто багато сайтів зламано анонімними людьми. Вони орієнтуються на веб-сайт з різних причин.

Огляд літератури щодо різних вразливостей визначає, що двома поширеними вразливими місцями безпеки є впровадження SQL і XSS. Різні дослідники пропонують багато технологій і механізмів для запобігання атакам SQL і XSS. Під час нашого дослідження ми з'ясували, що атаки SQL-ін'єкцій і атаки XSS все ще можливі навіть після впровадження

механізму запобігання, наявного на ринку, і таким чином забезпечують превентивні дії. механізм, ми запропонували архітектуру, показану на малюнку 2. На цьому малюнку ми запропонували схему, за допомогою якої ми будемо атакувати будь-який веб-сайт за допомогою SQL-ін'єкції, незалежно від того, чи завадить цьому будь-який із доступних на даний момент механізмів.

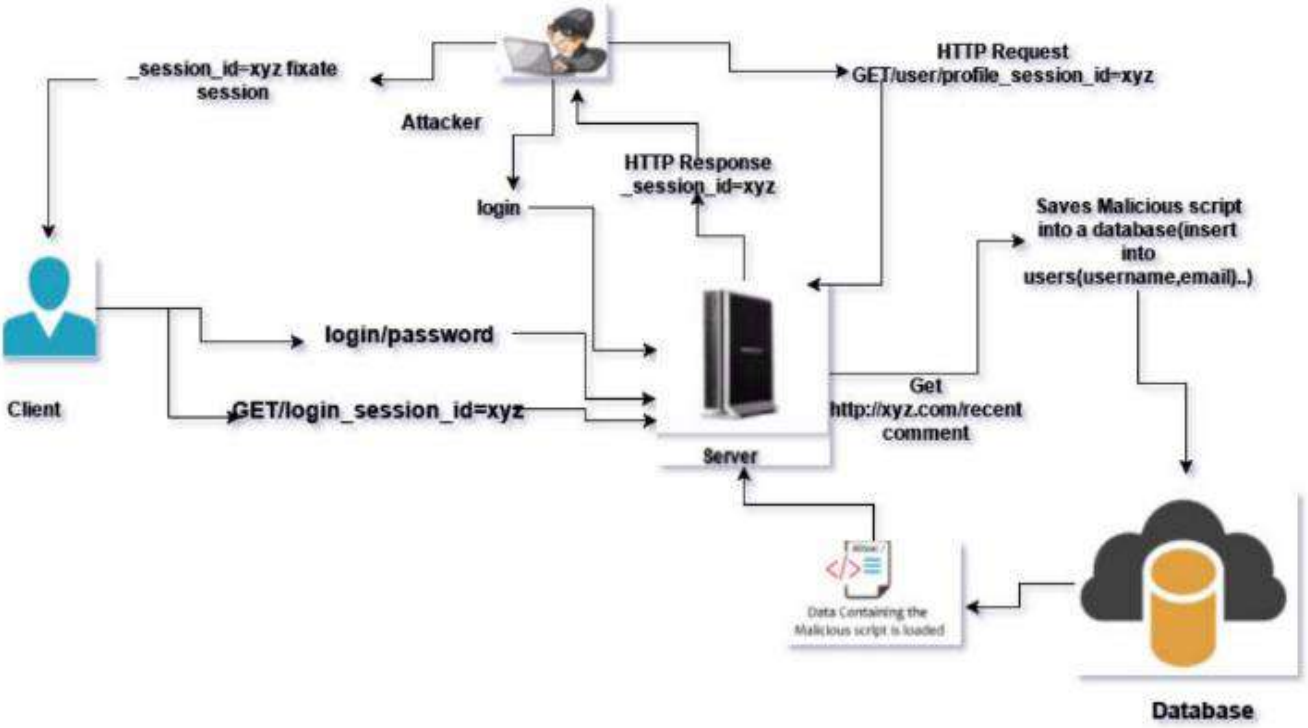


Рисунок 2. Веб-сайт у вразливості

У нашій архітектурі ми описуємо всі сеанси. Клієнт: клієнт веб-браузера фактично надсилає клієнтським запитам сторінки з серверів по всій мережі. У цій статті клієнт входить до системи звичайним чином, клієнт надсилає запит на сервер і отримує відповідь. Це відбувається лише у звичайній ситуації. Зловмисник: Зловмисник є неавторизованим користувачем. Зазвичай таким зловмисником є досвідчений програміст або інженер із достатніми технічними знаннями, щоб зрозуміти слабкі місця в системі безпеки. У цій статті зловмисник атакує веб-сайт за допомогою SQL-ін'єкції та XSS. Використання зловмисником SQL-ін'єкції та XSS описано нижче.

Зловмисні атаки роблять веб-додатки менш безпечними, оскільки зловмисник може пошкодити цілісність бази даних, застосовуючи зловмисні запити.

Вищезазначений запит є простим способом приборкати атаки додатків. Це можна сформувати шляхом застосування простих змін до коду сайту сервера. Зв'язування змінних — це ще один спосіб контролювати атаки SQL-ін'єкцій, і за допомогою зв'язування змінних ми можемо покращити продуктивність веб-додатків. Розробник має використовувати цей тип змінної в усіх операторах SQL, а також у мові Java, яка забезпечує кращий метод під назвою підготовлений оператор. Також підготовлений оператор використовує змінні прив'язки. Щоб захиститися від атак SQL-ін'єкцій, нам слід уникати передачі вхідних даних безпосередньо в SQL-запити. Замість цього користувач має використовувати параметризовані оператори або ретельно відфільтрований дезінфікований вхід. Щоб очистити наданий користувачем введений текст, він має бути прив'язаний до параметра, а введення має здійснюватися за допомогою методу фільтрації або очищення. Основна мета цього методу полягає в тому, що він додає зворотну косу риску ('\') проти всього шкідливого коду.

Зараз міжсайтові сценарії відбуваються через те, що розробники додають певну вразливість у код. Кожен розробник несе відповідальність за атаки, тому що розробник повинен розуміти, які атаки можливі на веб-програму. Ніколи не довіряйте введеним користувачами, оскільки користувач може вставляти будь-які типи символів і завжди використовувати метасимволи фільтрів, оскільки це зменшує атаки XSS. Розробники повинні конвертувати написане між будь-якими двома етапами, укладеними в «<» і «>». Прогалини XSS можуть пошкодити вашу програму, тому що зловмисники розкриють такі прогалини для громадськості, і часто кожен може бачити вашу особисту інформацію. Фільтрування не є належним рішенням для атак міжсайтових сценаріїв.

Ця дослідницька стаття містить повний огляд поточних результатів досліджень безпеки веб-додатків. Ми розглянули всі властивості розробки веб-додатків, зрозуміли важливі функції безпеки та властивості, які мають використовувати захищені веб-додатки, і розділили існуючі роботи на три основні класи. Ми також обговорили кілька питань, які ще потрібно розглянути. Щоб отримати доступ до кількох готових функцій у веб-додатках, застосовуються різні концепції та інструменти програмування, які створюють важливі аспекти безпеки наших додатків. Окрім цього, дослідники безпеки докладають необхідних зусиль, щоб розширити функції безпеки у веб-додатках за допомогою кількох інструментів і методів. Як правило, наша логіка та важливі коди знаходяться на стороні клієнта, тобто в нашому браузері, який розкриває концепції програміста. Таким чином для

зловмисників стає легко перехопити логіку та завдати повної шкоди серверному стану програми.

Список використаних джерел:

1. Tajpour, Atefeh, Maslin Masrom, Mohammad Zaman Heydari, and Suhaimi Ibrahim. «Оцінка інструментів виявлення та запобігання SQL-ін'єкцій» в комп'ютерних науках та інформаційних технологіях (ICCSIT), 2010, 3-я міжнародна конференція IEEE, том. 9, стор. 518-522. IEEE, 2010.

2. Алі С., Шахзад С. К. та Джавед Х. SQLIPA: механізм автентифікації проти впровадження SQL. Європейський журнал наукових досліджень, том. 38, № 4, 2009, стор. 604-611.

3. Садана, С. Дж. та Селам, Н. «Аналіз міжсайтових сценарних атак», Proc. Міжнародний журнал інженерних досліджень та застосувань (IJERA), вип. 1, № 4, pp 1764-1773, 2011.

4. Кумар, Р. «Пом'якшення вразливостей автентифікації у веб-додатках через вимоги безпеки», Інформаційні та комунікаційні технології (WICT), том. 60, pp 651–663, 2011.

5. Аванчіні, А. та Чеккато, М. «До тестування безпеки за допомогою аналізу забруднення та генетичних алгоритмів», семінар ICSE з розробки програмного забезпечення для безпечних систем, том. 5, pp. 65–71, 2010.

6. Шар, Л. С. Тан, Г. Б. К. і Бріанд, Л. К. «Вразливості ін'єкцій SQL для майнінгу та міжсайтового сценарію за допомогою аналізу гібридних програм», Proc. Міжн. конф. on Software Engineering (ICSE '13) IEEE Press, pp 642-651, 2013.

7. Li, Y. Wang, Z. and Guo, T. "Reflected XSS Vulnerability Analysis," International Research Journal of Computer Science and Information Systems (IRJCSIS), том. 2, pp 25-33, 2013.

8. Шар, Л. К. і Тан, Х. Б. К. «Автоматичне видалення вразливостей міжсайтових сценаріїв у веб-додатках», Інф. програмне забезпечення техн., вип. 54, pp 467–478, 2012.

9. Ян Хайся та Нань Чжихонг, «Схема тестування безпеки бази даних веб-додатків», 4-та Міжнародна конференція з комп'ютерних наук та освіти, 2009, IEEE, PP .953-955.

10. Meijunjin, «An Approach For Sql Injection Vulnerability Detection», 2009 Sixth International Conference on Information Technology: New Generations IEEE, PP 1411-1414.

11. Marashdih Abdalla Wasef, ZaabaZarulFitri Cross Site ScriptingDetection Approaches in Web Application, International Journal of Advanced Комп'ютерні науки та застосування, Том 7, № 10, стор 155-160, 2016

Мирченко І. Є.

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

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Бурхливий розвиток інформаційних технологій спричинив появу так званої комп'ютерної злочинності, яка в свою чергу може набувати масштабів кібертероризму. Поява кіберзлочинності та кібертероризму стала викликом сучасному світові, оскільки є загрозою для інформаційних технологій всього світу, зокрема України. Наразі всі ми є свідками діджиліталізації суспільства України (наприклад сервіси "Дія", "HELSI", "NovaPoshta" тощо), де всі процеси соціального, економічного, політичного, наукового, військового характеру переходять в режим он-лайн. Журналісти, політики та експерти розповсюджують сценарій, за яким кібертерористи можуть надійти в комп'ютери, що контролюють дамби або системи управління повітряним рухом, за допомогою електронних засобів, завдавши хаосу та загрожуючи не тільки мільйонам життів, але й самій національній безпеці. Фахівці вважають, що тероризм, який використовує останні досягнення в галузі високих технологій, не менш небезпечний, ніж ядерний чи бактеріологічний тероризм. Важливість та актуальність даної теми підтверджується і тим фактом, що дослідженням даної проблеми займаються всі передові організації, які відповідають за національну безпеку України [1, 2].

Таким чином, у зв'язку з наростаючим процесом глобалізації та формуванням інформаційного суспільства, кібертероризм став важливим фактором, який може загрожувати державній цілісності України та навіть дестабілізувати міжнародну обстановку. Сучасний кібертероризм має вплив не тільки на внутрішню політику України, але й на міжнародну безпеку. В контексті транснаціональної комп'ютерної злочинності та кібертероризму, запобігання кібератакам стає особливо важливою складовою національної безпеки, оскільки пов'язані ризики оцінюються як високі [1].

Дослідників кібертероризму ми зустрічаємо як на сторінках вітчизняної літератури, так і у працях зарубіжних науковців. Серед вітчизняних видається важливим згадати наступних: С. О. Гнатюк, В. П. Харченко, О. Г. Корченко, Є. В. Паціра, С. В. Казмірчук, В. Л. Бурячок, М. А. Погорецький, С. В. Мельник, Д. Б. Дубов, Р. М. Кравченко, та ін. До зарубіжних вчених, які дискують над цією темою можемо, вважати: В. А. Мазурова,

Ю. В. Гаврилова, М. М. Безрукова, В. Б. Вєхова, С. Гриняєва, Е. О. Роговського, Е. Конрі-Мюррея, Рональда Л-Діка та ін [1].

Метою дослідження є вивчення проблеми кібертероризму як загрози для інформаційної безпеки України; на основі досліджень та розробок проблеми визначити явище кібертероризму, виявити та охарактеризувати його вплив в Україні. Для досягнення поставленої мети нами використовувалися методи політологічного, історичного, порівняльного, статистичного аналізу, класифікації, систематизації, узагальнення, описи.

Кібертероризм – є широким поняттям та характеризує новий вид тероризму у глобалізованому та диджиталізованому суспільстві. Кібертероризм описується як будь-яка навмисна політично мотивована атака на інформаційні системи, програми та дані, що може призвести до насильства або загрожувати безпеці. Це може включати широкомасштабні атаки на комп'ютерні мережі, особливо ті, що підключені до Інтернету, з використанням різноманітних інструментів, таких як комп'ютерні віруси, хробаки, фішинг, шкідливе програмне забезпечення, апаратні методи, скрипти програмування. Все це може бути розглянуто як форма інтернет-тероризму. Знання про комп'ютерні системи та їх слабкі сторони стають все більш поширеними, попри те, що інструменти кібертерориста (комп'ютерні модеми, телефонні з'єднання) легко доступні. Існують три категорії хакерів: хакер, кіберпанк і шифропанк. Розширені атаки постійної загрози використовують складні та концентровані методи проникнення, щоб отримати доступ до мережі та вкрасти дані. Організації з високоцінною інформацією є типовими цілями атак APT. Комп'ютерні віруси, хробаки та шкідливі програми націлені на різні системи контролю IT та можуть бути використані для нападу на критично важливу інфраструктуру та військові системи. Атаки DoS намагаються перешкодити легальним користувачам отримати доступ до цільових комп'ютерних систем. Злом або отримання несанкціонованого доступу намагається викрасти критично важливі дані з установ, урядів і компаній. Програми-вимагачі утримують дані або інформаційні системи в заручниках, поки жертва не заплатить викуп. Фішингові атаки намагаються зібрати інформацію через електронну пошту цілей, використовуючи цю інформацію для доступу до систем або викрадення особистої інформації. Кібертероризм становить загрозу кібернетичній безпеці України, оскільки кібератаки можуть завдати шкоди на різних рівнях, включаючи локальний, державний та міжнародний. На даний момент законодавство України не містить норм, що стосуються кібертероризму, але законодавча робота в цьому напрямку проводиться. Проект Закону про внесення змін до Кримінального кодексу України

№ 2439а від 24.07.2015 запропоновує доповнення статті 258-6 ККУ, в якій кібертероризм визначається як умисна атака на комп'ютерні системи або мережі з метою створення небезпеки для людей або інших тяжких наслідків, що скоєна з політичних мотивів з метою порушення суспільної безпеки, залякування населення або провокації військового конфлікту [3, 5].

Аналізуючи найбільш відомі приклади кібератак за останні 25 років, можна зробити висновок, що в багатьох випадках об'єктами кібертероризму є системи функціонування та управління приватних та державних компаній в нафто-, газопереробних та металургійних галузях. Наприклад, 25 грудня 2015 року відома міжнародна компанія ESET виявила аварію на «Прикарпаттяобленерго», яка була наслідком зовнішньої хакерської атаки. За допомогою вірусу-трояна Black Energy було запущено спеціальну програму KillDisk, що призвело до збою комп'ютерних програм. Також, 27 червня 2017 року відбулась масова атака, в результаті якої близько 30 банків, система інфраструктури (80% підприємств, підпорядкованих Міністерству інфраструктури), Кабмін, мобільні оператори, ЗМІ та підприємства енергетичної сфери були уражені, що призвело до тимчасового припинення їх роботи. Вірус не відомого походження, що отримав назву «вірус Petya», атакував комп'ютерні системи сотень державних установ, підприємств та організацій близько 12 години дня [4].

Отже, для боротьби з кібертероризмом важливим є налагодження співпраці та координації між правоохоронними органами, спецслужбами та судовими інстанціями, спрямованих на розкриття та запобігання кібератак. Також необхідно покращення законодавства в Україні з метою більш ефективної боротьби з цим видом злочинності [2].

Список використаних джерел:

1. *Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/Nvkhdu_jur_2015_6%283%29__16*
2. *Алієв М.М., Куньо А.М. «Проблема кіберзлочинності та шляхи її подолання у сучасному інформаційному суспільстві» // XI Міжнародна науково-технічна конференція «АВІА-2013» 21-23 травня 2013 р. – К.: НАУ, 2013. – Т.6. – С. 36-47.*
3. *Про національну безпеку України: Закон України [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19.*
4. *Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/96/2016#n11.*
5. *Zanini, M. & Edwards, S. J. A. (2001). The Networking of terror in the information age. In J. Arquilla & D. Ronfelt (Eds), Networks and netwars, (pp.29-60). Santa Monica, CA: RAND Corporation.*

Науменко П. С.

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

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

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.

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 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?

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 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.*

Радагуз М. В.

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

ГЕЙМІФІКАЦІЯ ПРОЦЕСУ ПЕРЕВІРКИ КІБЕРБЕЗПЕКИ ПРОДУКТУ

Захист інформації є критично важливим для бізнесу в епоху цифрової трансформації. Процес перевірки безпеки продукту є важливим етапом в розробці будь-якого програмного забезпечення, щоб запобігти вразливостям та забезпечити високу надійність продукту. Однак, перевірка безпеки може бути складною та технічно вимогливою процедурою, яка вимагає від розробників великих зусиль та часу.

Одним зі способів полегшення процесу перевірки безпеки є гейміфікація. Гейміфікація полягає у використанні ігрових елементів та механік для залучення користувачів та стимулювання їхньої активності в конкретному контексті. Використання гейміфікації може допомогти розробникам привернути увагу до процесу перевірки безпеки та забезпечити більш ефективне та ефективне виконання завдань з безпеки.

Вивчення гейміфікації в контексті безпеки продукту є досить новим напрямом досліджень. Проте, за останні роки відбулось досить багато досліджень та публікацій на цю тему.

Наприклад, Гамбург (2019) провів дослідження використання гейміфікації у процесі перевірки безпеки продукту та прийшов до висновку, що гейміфікація може допомогти залучити користувачів до процесу перевірки безпеки та забезпечити більш ефективне та ефективне виконання завдань з безпеки.

Крім того, Левін та Шоу (2018) використали гейміфікацію для залучення користувачів до процесу

Зокрема, Бюркі та його колеги (2018) досліджували використання гейміфікації у процесі навчання кібербезпеки та зазначили, що гейміфікація може покращити мотивацію та підвищити зацікавленість користувачів у вивченні теми безпеки.

Також варто згадати роботу Дурдікулакара та його колег (2020), де автори використовували гейміфікацію для покращення свідомості користувачів про кібербезпеку. Результати дослідження показали, що гейміфікація може бути ефективним інструментом для залучення та навчання користувачів про безпеку в Інтернеті.

Дослідження, проведені Морсікою та її колегами (2018), показали, що гейміфікація може збільшити ефективність процесу перевірки безпеки за допомогою механізмів стимулювання користувачів до активної участі та вирішення проблем.

Загалом, дослідження підтверджують потенційну ефективність гейміфікації у процесі перевірки безпеки продукту та демонструють її можливості для поліпшення мотивації та ефективності користувачів у процесі роботи з кібербезпекою.

Види гейміфікації:

Зараз широко використовуються різноманітні підходи до гейміфікації процесу перевірки безпеки продукту. Деякі дослідження демонструють, що гейміфікація може бути ефективним способом залучення користувачів до більш активного вивчення тем безпеки та до більш відповідальної поведінки в Інтернеті [1].

Один з можливих підходів до гейміфікації полягає у використанні різноманітних ігрових завдань та квестів, які допоможуть залучити користувачів до процесу вивчення тем безпеки. Застосування ігрових елементів, таких як ігрові персонажі, виклики, підказки та інші, також можуть стимулювати більш активну участь користувачів у процесі безпеки [2].

Гейміфіковані системи нагородження можуть бути іншим ефективним способом залучення користувачів до більш активної участі у процесі безпеки. Використання різних типів нагород, таких як бали, зірки, медалі та інші, можуть стимулювати користувачів до дотримання певних правил безпеки та забезпечити позитивну мотивацію [2].

Одним з перспективних напрямків гейміфікації є використання гейміфікованих соціальних мереж. Застосування форумів, чатів, груп в соціальних мережах та інших інструментів може забезпечити спілкування та обмін думками користувачів про кібербезпеку [3].

Наша пропозиція:

Гейміфікація використовує ігрові елементи та механіки для залучення та мотивації користувачів. Текстові рольові ігри - це один з видів ігор, який базується на історії та нарративі. У нашому випадку, ми пропонуємо використовувати текстову рольову гру для гейміфікації процесу перевірки безпеки продукту. Це може зробити процес більш залученим та мотивуючим для учасників, що забезпечить кращі результати перевірки та більшу відповідальність у питаннях безпеки продукту.

Так, можна створити кампанію, яка складається з трьох квестів, що відповідають трьом етапам перевірки безпеки продукту: моделювання

загроз, перевірка коду та тестування безпеки. Кожен квест буде включати в себе відповідні завдання та виклики, які допоможуть учасникам краще зрозуміти, які загрози можуть існувати для продукту, як перевіряти код на наявність вразливостей та як проводити тестування безпеки для переконання, що продукт належним чином захищений. Цей підхід може зробити процес перевірки безпеки продукту більш цікавим та залученим для учасників, що забезпечить кращі результати та більшу відповідальність у питаннях безпеки.

Високорівневий дизайн гри-перевірки кібербезпеки:

Нехай, команда розробників представлана командою авантюристів, які мають захистити свої скарби - assets продукту - від сил зла, які хочуть їх захопити. Кожен авантюрист має свою расу та клас, і кожна комбінація раси та класу спеціалізується на певній сфері безпеки продукту.

На етапі моделювання загроз команда дізнається про можливі загрози, які загрожують їхнім скарбам. Використовуючи свої знання та досвід відповідно до свого класу та раси, авантюристи беруть участь в процесі брейнштормінгу і перелічують можливі загрози.

На етапі перевірки коду команда займається перевіркою коду продукту на наявність вразливостей та помилок, використовуючи свої спеціалізовані навички та знання відповідно до свого класу та раси.

На етапі тестування безпеки команда проводить практичні тести, щоб переконатися, що продукт захищений від можливих загроз, використовуючи свої спеціалізовані навички та знання відповідно до свого класу та раси.

Ця гра-кібербезпека заснована на текстовій рольовій грі, яка використовує команди Slack, де кожен гравець може виконувати свої завдання та отримувати бали за успішне виконання завдань, які можуть бути обміняні на різні види нагород.

У фінальному етапі гри команда розробників отримує повідомлення про прибуття ворогів, тобто сторонньої команди тестувальників на проникнення. Завдання команди розробників - захистити свої скарби, тобто assets продукту, від ворогів, тобто виявлених вразливостей. Якщо тестувальники знайшли критичні вразливості, команда розробників програла. В іншому випадку, коли вразливості не були виявлені або їх вдалося виправити до часу нападу, команда розробників перемагає. У разі перемоги, команда отримує винагороду у вигляді балів або медалей, які можуть бути використані для підвищення рівня своїх авантюристів та поліпшення їхньої екіпіровки.

Гейміфікація процесу перевірки безпеки продукту може бути ефективним інструментом для підвищення рівня безпеки продукту та

привернення уваги розробників до цього процесу. Використання текстової рольової гри, як механізму гейміфікації, може стимулювати розробників до активної участі у процесі перевірки безпеки продукту, сприяючи збільшенню ефективності і якості перевірки.

Застосування різних видів гейміфікації, таких як нагороди, таблиці лідерів та інші, може збільшити мотивацію розробників до дотримання правил безпеки та забезпечити їх позитивну мотивацію.

Для реалізації гейміфікованої системи перевірки безпеки продукту, можна використовувати текстового чат-бота, який надає розробникам можливість брати участь в рольовій грі. Така система може бути ефективною для залучення розробників до процесу перевірки безпеки продукту, що сприятиме поліпшенню безпеки та якості продукту.

Однак, перед запровадженням гейміфікованої системи перевірки безпеки, необхідно провести додаткові дослідження, щоб з'ясувати ефективність такої системи та її вплив на робочий процес розробників.

Далі можливо варто розглянути можливості використання інших інструментів гейміфікації, таких як віртуальна реальність, а також можливість поєднання гейміфікації з іншими методами забезпечення безпеки, такими як DevSecOps та Continuous Integration/Continuous Delivery (CI/CD).

Список використаних джерел:

1. Hamari, J., Sarsa, H., Koivisto, J. (2014). Does Gamification Work? -- A Literature Review of Empirical Studies on Gamification. Proceedings of the 47th Hawaii International Conference on System Sciences, 3025-3034. doi: 10.1109/HICSS.2014.377

2. Landers, R.N., Bauer, K.N. & Callan, R.C. (2017). Gamification of Compliance Training: Does It Really Work? Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 61(1), 1077-1081. doi: 10.1177/1541931213601485

3. Razmerita, L., Kirchner, K., & Sudzina, F. (2015). Gamification: A systematic review of design frameworks. Journal of Business Research, 69(8), 31-42. doi: 10.1016/j.jbusres.2015.02.025

Срибный Р. О.

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

БЕЗОПАСНОСТЬ САЙТА: АНАЛИЗ 10 ОСНОВНЫХ УГРОЗ И КАК ОТ НИХ ОБЕЗОПАСИТСЯ

Недостаточная защищенность веб-приложений чревата для собственников экономическими, репутационными и другими видами рисков. Взломанные сайты используются для распространения вирусов, кражи данных, публикации конфиденциальной информации и проникновения во внутренние сети предприятий [1].

OWASP Top 10 - это стандартный документ для разработчиков и специалистов по безопасности веб-приложений. Он представляет собой широкий консенсус в отношении наиболее серьезных угроз безопасности для веб-приложений. Компании должны принять этот документ и начать процесс обеспечения того, чтобы их веб-приложения минимизировали эти риски [5]. OWASP Top 10 для веб-угроз был актуализирован в 2021 году. OWASP важен для организаций, так как его рекомендации высоко ценятся проверяющими безопасность корпоративных систем аудиторами. Рекомендации проекта по защите приложений необходимо включить в жизненный цикл разработки ПО и использовать для формирования политик безопасности [4].

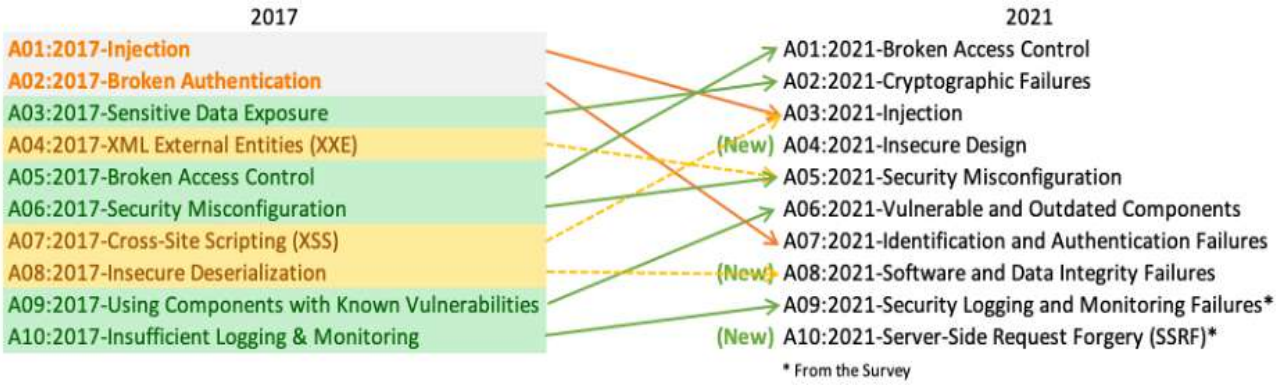


Рис.1. 10 главных угроз безопасности веб-приложений в 2017 и 2021гг [5].

С рисунка 1, видно, что появились три новые категории, четыре категории с измененными названиями и областью действия, а также некоторая консолидация в Топ-10 на 2021 год [5]. Для составления данного рейтинга, OWASP собирает информацию от более чем 40 известных

отраслевых компаний, которые занимаются обеспечением безопасности веб-приложений, а также проводят опрос среди специалистов из сферы информационной безопасности [2].

В последнем отчете OWASP перечислены 10 основных уязвимостей:

1. *Нарушенный контроль доступа (Broken Access control):* эта категория по сравнению с 2017 годом поднялась сразу на 4 позиции и заняла первое место. В среднем, 3,81% протестированных веб-приложений имело данный тип уязвимости [2]. Возникает, когда нарушен доступ к ресурсам: некоторые ограничения для аутентифицированных пользователей не работают или настроены неправильно, что позволяет получать, например, доступ к другим учётным записям. Злоумышленники при нарушенном контроле доступа получают возможность управления сеансом пользователя и могут также получить доступ к незащищенным логинам и паролям из активных сеансов [3]. Риск нарушения контроля доступа можно снизить: 1. развернув концепцию наименее привилегированного доступа, регулярно проверяя серверы и веб-сайты, применяя MFA и удаляя с серверов неактивных пользователей и ненужные службы; 2. защитить элементы управления доступом, используя токены авторизации при входе пользователей в веб-приложение и делая их недействительными после выхода из системы; 3. регистрация и отчеты об ошибках доступа, ограничение скорости для минимизации причиняемого автоматическими атаками ущерба [4]

2. *Сбои криптографии (Cryptographic Failures)* - перемещается на одну позицию вверх, ранее известную как раскрытие конфиденциальных данных, что было общим симптомом, а не основной причиной [5]. Эта уязвимость возникает в приложениях, в которых не защищены должным образом конфиденциальные данные (банковских карт, имена, пароли и т.д). Важно следить за шифрованием данных и избегать устаревших криптографических функций [3].

3. *Инъекции (Injections):* такие атаки происходят, когда ненадежные данные передаются интерпретатору кода через ввод формы или с помощью другого способа отправки информации в веб-приложение. Например, злоумышленник может ввести код на SQL в форму, которая ожидает имени пользователя. Если ввод данных не защищен должным образом, это приведет к выполнению кода – такие атаки известны как SQL-инъекции. Инъекционные атаки можно предотвратить путем проверки и/или очистки отправленных пользователем данных. Администратор базы данных может установить специальные элементы управления, чтобы минимизировать

объем информации, которую может раскрыть атака с использованием SQL-инъекций [4]. Межсайтовый скриптинг (XSS) теперь является частью этой категории в этом издании [5].

4. *Небезопасный дизайн (Insecure Design):* новая категория в 2021 году, посвящена рискам, связанным с ошибками проектирования и архитектуры приложения. Введение этой угрозы можно считать призывом к использованию моделирования угроз, безопасных шаблонов проектирования и эталонных архитектур. Одним из факторов, способствующих небезопасному проектированию, является отсутствие профилирования бизнес-рисков [3].

5. *Неправильная конфигурация (Security Misconfiguration):* с увеличением количества переходов на программное обеспечение с широкими возможностями настройки эта категория продвигается вверх. Прежняя категория для внешних объектов XML (XXE) теперь является частью этой категории [5]. Встречается в веб-приложениях, которые анализируют ввод XML, когда плохо сконфигурированные процессоры XML оценивают ссылки на внешние объекты в документах XML и отправляют конфиденциальные данные неавторизованному внешнему объекту (устройству хранения). По умолчанию большинство анализаторов XML уязвимы для этого вида атак [3]. Конфигурацию безопасности можно исправить, изменив настройки веб-сервера или CMS по умолчанию, удалив неиспользуемые функции кода и контролируя данные пользователей и видимость пользовательской информации. Разработчики должны удалить ненужную документацию, функции, структуры и образцы, сегментировать архитектуру приложений и автоматизировать проверку эффективности конфигураций и настроек веб-среды [4].

6. *Уязвимые и устаревшие компоненты (Vulnerable and Outdated Components).* Существует множество программных компонентов с открытым исходным кодом, а так же библиотек и фреймворков, доступных разработчикам. Если в приложении используется компонент, имеющий уже известную уязвимость, он становится слабым звеном, которое может повлиять на безопасность всей системы [3]. Этого можно избежать с помощью виртуального исправления, которое защищает устаревшие веб-сайты от эксплуатации уязвимостей с помощью брандмауэров, систем обнаружения вторжений (IDS) и WAF; или предотвратить, сохранив только реально необходимые компоненты и удалив все неиспользуемые или не обслуживаемые. Лучший метод - установка компонентов из надежных источников и постоянное их обновление [4].

7. *Ошибки идентификации и аутентификации (Identification and Authentication Failures):* эти ошибки также новая категория в списке. Проблемы с аутентификацией позволяют злоумышленнику использовать различные методы для получения контроля над любой учётной записью в системе или полного контроля над системой [3]. Ранее это была категория Broken Authentication, и она опустилась со второй позиции, и теперь включает уязвимости, которые больше связаны с ошибками идентификации [5]. Количество уязвимостей можно уменьшить путем внедрения многофакторной аутентификации, внедрения ограничений, делающих невозможности автоматизированные атаки грубой силы; внедрение процедур тестирования кода на безопасность; необходимо внедрить жесткую парольную политику и использовать безопасные диспетчеры сеансов [4].

8. *Нарушение целостности данных и программного обеспечения (Software and Data Integrity Failures):* новая категория на 2021 год, основное внимание уделяется предположениям, связанным с обновлениями программного обеспечения, критическими данными и конвейерами CI/CD без проверки целостности. Небезопасная десериализация из 2017 года теперь является частью этой более широкой категории [5]. Небезопасная десериализация позволяет злоумышленнику удалённо выполнять код в приложении, подделывать или удалять сериализованные объекты, проводить атаки путём внедрения, повторного воспроизведения [3]. Этого можно избежать, запретив сериализованные объекты и десериализацию данных, поступающих из ненадежных источников [4].

9. *Журнал безопасности и сбои мониторинга (Security Logging and Monitoring Failures):* время от атаки до обнаружения может занять до 200 дней и больше. Тем временем злоумышленники могут вмешиваться в работу серверов, повреждать базы данных и красть конфиденциальную информацию [3]. Важно вести журналы аудита, которые позволяют отслеживать любые подозрительные изменения, регистрировать аномальную активность и отслеживать несанкционированный доступ или компрометацию учетной записи [4].

10. *Подделка запросов со стороны сервера или же SSRF (Server-Side Request Forgery):* ошибки SSRF возникают, когда веб-приложение извлекает удаленный ресурс без проверки предоставленного пользователем URL-адреса. Это дает злоумышленнику возможность перенаправить созданный запрос в неожиданное место назначения, обходя защиту брандмауэром, VPN или другими средствами управления доступом к сети. Поскольку современные веб-приложения предоставляют конечным

пользователям разные функции, получение URL-адреса становится распространенным сценарием. Частота ошибок SSRF становится выше из-за распространения облачных сервисов и сложности архитектур [3].

Отметим, что список построен в виде рейтинга. Ранжирование основывается на частоте дефектов, серьезности уязвимостей и их потенциального воздействия. Это позволяет разработчикам и специалистам по безопасности понимать наиболее серьезные риски и минимизировать возможные последствия эксплуатации уязвимостей злоумышленниками.

Список использованных источников:

1. *Как защитить сайт от взлома: 10 главных угроз и как от них защитится. Режим доступа: https://webcase.com.ua/blog/bezopasnost-web-prilozhenij/#id13*

2. *Самые опасные уязвимости веб-приложений. Режим доступа: https://softline.by/about/news/samyie-opasnyie-ugrozyi-dlya-veb-prilozheniy*

3. *Что такое Топ-10 OWASP и какие уязвимости веб-приложений наиболее опасны? Режим доступа: https://rcngroup.ru/blog/chto-takoe-top-10-owasp-i-kakie-ujazvimosti-veb-prilozhenij-naibolee-opasny/*

4. *Что такое Топ-10 OWASP и какие уязвимости веб-приложений наиболее опасны? Режим доступа: https://proglib.io/p/chto-takoe-top-10-owasp-i-kakie-uyazvimosti-veb-prilozheniy-naibolee-opasny-2021-09-09*

5. *OWASP Top Ten. Режим доступа: https://owasp.org/www-project-top-ten/*

Ягнич І. М.

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

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЛЯ ВЕБ-САЙТІВ

У сучасну епоху цифрових технологій веб-сайти стали невід'ємною частиною повсякденного життя як для працівників компаній, так і для окремих людей. Веб-сайти забезпечують платформу для спілкування, обміну інформацією, електронної комерції та інших видів діяльності. Зі збільшенням кількості веб-сайтів зростає й загроза кібератак. Кібератаки можуть мати різні форми, включаючи зловмисне програмне забезпечення, фішинг, атаки на відмову в обслуговуванні та програми-вимагачі.

Кібератаки становлять зростаючу загрозу веб-сайтам, комп'ютерам, серверам і мережам у всьому світі. Ці атаки мають різні форми, можуть завдати значної фінансової та репутаційної шкоди, а також призвести до втрати конфіденційних даних.

Зловмисне програмне забезпечення – це тип шкідливого програмного забезпечення, яке може заражати веб-сайти та комп'ютери, викрадати дані та завдавати шкоди системам. Зловмисне програмне забезпечення може мати форму вірусів, хробаків, троянів, шпигунського програмного забезпечення та програм-вимагачів. Після встановлення в системі, зловмисне програмне забезпечення може взяти під контроль веб-сайт або комп'ютер і викрасти конфіденційні дані або завдати шкоди системам [1].

Фішинг – ще одна поширена кібератака, спрямована на веб-сайти та їх користувачів. Фішингові атаки використовують тактику соціальної інженерії, щоб обманом змусити користувачів розкрити свою особисту та фінансову інформацію. Ці атаки зазвичай включають надсилання електронних листів або повідомлень, які нібито надійшли з надійного джерела, наприклад, банку або веб-сайту електронної комерції, і просять користувачів натиснути посилання або ввести свої облікові дані.

Атаки типу «відмова в обслуговуванні» (DoS) – це ще один тип кібератак, який може вплинути на веб-сайти. Ці атаки перевантажують веб-сайт трафіком, роблячи його недоступним для користувачів. DoS-атаки можуть бути запущені кіберзловмисниками за допомогою ботнетів, які є мережами комп'ютерів, заражених шкідливим програмним забезпеченням.

Кібербезпека – це практика захисту веб-сайтів, комп'ютерів, серверів і мереж від несанкціонованого доступу, кіберзагроз і атак. Кібербезпека

передбачає впровадження заходів безпеки для запобігання кібератакам і реагування на атаки, які відбулися. Заходи кібербезпеки охоплюють апаратні та програмні технології, політики та процедури, а також навчання користувачів.

Веб-сайти особливо вразливі до кібератак, оскільки вони доступні для всіх, хто має підключення до Інтернету. Веб-сайти також зберігають багато конфіденційних даних, зокрема особисту та фінансову інформацію. Кіберзловмисники часто націлюються на веб-сайти, щоб отримати доступ до цих даних, які потім можуть використовувати для фінансової вигоди або крадіжки особистих даних [2].

Веб-сайти можуть впроваджувати різні заходи кібербезпеки, щоб захистити свої дані та користувачів. Одним із найважливіших кроків є встановлення сертифікатів SSL. Сертифікати SSL – це цифрові сертифікати, які забезпечують безпечне зашифроване з'єднання між веб-сайтом і його користувачами. Це захищає від витоку даних та інших форм кібератак.

Сертифікати SSL працюють шляхом шифрування даних, що передаються між веб-сайтом і його користувачами. Це означає, що будь-яка інформація, яку вводить користувач, як-от облікові дані для входу або дані кредитної картки, захищена від перехоплення кіберзловмисниками. Сертифікати SSL також забезпечують автентифікацію, гарантуючи, що користувачі підключаються до правильного веб-сайту, а не до шахрайського.

Щоб запровадити сертифікати SSL, власники веб-сайтів повинні придбати та встановити їх на своїх серверах. Багато провайдерів веб-хостингу пропонують сертифікати SSL як частину своїх послуг, а інші можуть вимагати від власників веб-сайтів придбати їх окремо. Після встановлення власники веб-сайтів повинні переконатися, що їхній веб-сайт налаштовано на використання HTTPS замість HTTP. HTTPS – це безпечна версія HTTP, яка вказує на те, що веб-сайт використовує шифрування SSL для захисту даних користувача [3].

Іншим важливим заходом кібербезпеки для веб-сайтів є використання надійних паролів. Слабкі паролі є легкою мішенню для кіберзловмисників, які можуть отримати доступ до конфіденційних даних й облікових записів користувачів. На веб-сайтах повинно бути забезпечено використання надійних унікальних паролів для всіх облікових записів користувачів й адміністративного доступу.

Регулярні оновлення програмного забезпечення також є важливим заходом кібербезпеки для веб-сайтів. Застаріле програмне забезпечення може надати зловмисникам легкий доступ до конфіденційних даних і облікових

записів користувачів. Регулярні оновлення програмного забезпечення допомагають забезпечити захист веб-сайту від останніх кіберзагроз.

DDoS-атаки є поширеною формою кібератак, метою яких є порушення трафіку веб-сайту. Веб-сайти можуть застосовувати заходи захисту від DDoS, щоб запобігти таким атакам [4]. Ці заходи включають обмеження кількості запитів із однієї IP-адреси, моніторинг мережевого трафіку на наявність аномалій і використання мереж доставки контенту (CDN) для розподілу трафіку.

Регулярне резервне копіювання даних – це важливий захід кібербезпеки, який також повинні впроваджувати веб-сайти. Резервне копіювання даних гарантує, що власники веб-сайтів можуть відновити свої дані у разі втрати даних, кібератаки чи іншого лиха. Резервні копії слід зберігати за межами сайту, щоб запобігти втраті даних у разі фізичного лиха, наприклад, пожежі.

Власники веб-сайтів повинні проводити регулярний моніторинг безпеки, щоб виявити будь-яку підозрілу активність на своїх веб-сайтах. Це включає моніторинг веб-трафіку, системних журналів і журналів доступу. Регулярний моніторинг безпеки допомагає виявити та усунути проблеми безпеки, перш ніж ними зможуть скористатися кіберзловмисники.

Контроль доступу є ще одним критично важливим заходом кібербезпеки для веб-сайтів. Власники веб-сайтів повинні дозволити доступ до конфіденційних даних і адміністративних функцій лише обраним користувачам. Це включає застосування надійних паролів, багатофакторну автентифікацію та обмеження доступу до певних IP-адрес.

Нарешті, веб-сайти повинні вибирати безпечних хостинг-провайдерів для захисту від кібератак. Провайдери безпечного хостингу використовують передові засоби безпеки, такі як брандмауери, системи виявлення та запобігання вторгненням, а також сканери зловмисного програмного забезпечення для захисту від кібератак.

Таким чином, кібербезпека є критично важливою для веб-сайтів. Кібератаки можуть спричинити фінансові втрати та втрату конфіденційних даних. Застосування заходів кібербезпеки, таких як сертифікати SSL, надійні паролі, регулярні оновлення програмного забезпечення, захист від DDoS, резервне копіювання даних, моніторинг безпеки, контроль доступу та безпечний хостинг, можуть допомогти захистити веб-сайти від кібератак. Власники веб-сайтів повинні активно впроваджувати заходи кібербезпеки, щоб забезпечити безпеку своїх даних і користувачів.

Список використаних джерел:

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. 2009. 608 с.

2. Золотар О. О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

4. Мєшков В. І., Віролайнен В. О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. 2015. URL: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf

5. Що таке пентест — тест на проникнення? 2020. URL: https://datami.ua/shho-take-pentest-test-na-proniknennya/

Dmytro Barsukov

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

COMPREHENSIVE SECURITY-AS-A-SERVICE (CSAAS) AS AN EFFECTIVE SOLUTION TO ADDRESS CYBERSECURITY CHALLENGES FACED BY SMALL AND MEDIUM-SIZED BUSINESSES (SMBS)

Small and medium-sized businesses (SMBs) play a crucial role in the global economy, accounting for a significant portion of employment and economic growth. However, despite their importance, SMBs often struggle with limited resources and budgets, which can leave them vulnerable to cyber attacks. The threat of cyber attacks is increasing, and SMBs are an attractive target for cyber criminals due to their relatively weaker cybersecurity defenses. SMBs face numerous cybersecurity challenges, including limited resources for cybersecurity, lack of expertise, and the complexity of cyber threats. Therefore, it is essential to address the cybersecurity problems faced by SMBs to protect their business operations and prevent the negative economic and social consequences of cyber attacks. In this article, we will explore the unique challenges that SMBs face in cybersecurity and the measures that can be taken to mitigate the risks of cyber attacks.

We investigated current state of specific for SMB cybersecurity problems and created list of top problems:

1. Limited resources: SMBs often have limited resources for cybersecurity, which can make it challenging to implement adequate security measures and keep up with evolving threats.
2. Lack of expertise: Many SMBs do not have in-house IT staff with cybersecurity expertise, which can make it difficult to address cybersecurity issues effectively.
3. Complexity of cyber threats: Cyber threats are becoming increasingly complex and sophisticated, and SMBs may struggle to keep up with the latest threats and defenses.
4. Lack of cybersecurity awareness: SMBs may not be aware of the cybersecurity risks they face or may not prioritize cybersecurity due to competing business demands.

5. Inadequate incident response plans: SMBs may not have adequate incident response plans in place to address cybersecurity incidents, which can lead to delays in responding to attacks and increased damage.

6. Dependence on third-party vendors: SMBs may rely on third-party vendors to provide critical services such as cloud computing and data storage, which can introduce additional cybersecurity risks.

7. Cost of cybersecurity solutions: SMBs may struggle to afford robust cybersecurity solutions, which can put them at a disadvantage compared to larger organizations.

8. Lack of regulatory guidance: SMBs may not have clear guidance on regulatory requirements for cybersecurity, which can make it challenging to comply with regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

9. Limited scalability: SMBs may struggle to scale their cybersecurity measures as they grow and face new threats, which can leave them vulnerable to attacks.

10. High impact of cyber attacks: SMBs may be disproportionately impacted by cyber attacks due to their limited resources and smaller customer base, making it challenging to recover from the financial and reputational damage caused by an attack.

Cybersecurity threats are increasingly pervasive and complex, presenting significant challenges for businesses of all sizes. Small and medium-sized businesses (SMBs) are particularly vulnerable to cyber threats due to their limited resources and expertise in cybersecurity. In recent years, there has been a growing trend towards outsourcing cybersecurity needs to third-party providers who specialize in delivering cybersecurity-as-a-service (CSaaS). CSaaS providers offer a range of cybersecurity services, including vulnerability management, threat detection and response, network security, endpoint security, and data protection, which can be accessed through a cloud-based platform. This model of delivering cybersecurity services can provide businesses, including SMBs, with the expertise and resources needed to address their cybersecurity needs effectively. In this article, we explore the concept of CSaaS, its benefits, and its potential to help businesses better protect themselves against cyber threats.

By outsourcing cybersecurity to a third-party provider that specializes in delivering cybersecurity services, businesses can take advantage of a range of benefits, such as:

1. Access to expertise: Many SMBs lack the expertise and resources needed to effectively manage their cybersecurity needs. By outsourcing cybersecurity to a CSaaS provider, businesses can leverage the expertise and

resources of a dedicated team of cybersecurity professionals who can help them address their specific cybersecurity challenges.

2. Scalability: CSaaS providers offer a range of services that can be scaled up or down based on the needs of the business. This allows SMBs to adjust their cybersecurity measures as their business grows and evolves, without having to invest in additional resources or expertise.

3. Cost-effective: Outsourcing cybersecurity to a CSaaS provider can be a cost-effective way for SMBs to manage their cybersecurity needs. CSaaS providers typically offer subscription-based pricing models, which can be more affordable than investing in in-house cybersecurity solutions.

4. Compliance: Many SMBs are required to comply with industry regulations and standards related to cybersecurity. CSaaS providers can help SMBs ensure that they are meeting these requirements, and can provide documentation and evidence of compliance to auditors or regulators.

5. 24/7 monitoring: CSaaS providers typically offer 24/7 monitoring of cybersecurity threats, which can help businesses identify and respond to cyber threats in real-time, before they cause significant damage.

6. Focus on core business: By outsourcing cybersecurity to a CSaaS provider, SMBs can focus on their core business activities, rather than spending time and resources on managing their cybersecurity needs.

In addition to these general benefits, CSaaS can also help SMBs address specific cybersecurity challenges that are unique to their business. For example, CSaaS providers can help SMBs manage their supply chain risks by assessing the cybersecurity risks associated with their vendors and suppliers. They can also help SMBs manage their data protection needs by implementing data backup and recovery solutions, and providing data protection training to employees.

Here is a list of CSaaS companies that specialize in providing cybersecurity services to SMBs and the services they provide:

1. Alert Logic: Provides threat detection and response, vulnerability management, and compliance solutions to SMBs.

2. Arctic Wolf: Offers managed detection and response, vulnerability management, and risk management services to SMBs.

3. CrowdStrike: Provides endpoint security, threat intelligence, and incident response services to SMBs.

4. Sophos: Offers endpoint security, network security, and data protection solutions to SMBs.

5. Barracuda Networks: Provides email security, network security, and data protection services to SMBs.

6. Perch Security: Offers threat detection and response, vulnerability management, and compliance solutions to SMBs.

7. Zscaler: Provides cloud security, network security, and data protection solutions to SMBs.

8. SonicWall: Offers firewall, email security, and network security services to SMBs.

9. Webroot: Provides endpoint security, DNS protection, and threat intelligence services to SMBs.

10. Bitdefender: Offers endpoint security, network security, and threat intelligence solutions to SMBs.

In conclusion, Comprehensive Security-as-a-Service (CSaaS) is an effective solution for SMBs to address their unique cybersecurity challenges. By outsourcing their cybersecurity needs to a third-party provider, SMBs can access expertise, scalability, and cost-effective solutions that can help protect their business against cyber threats. CSaaS can also help SMBs address specific cybersecurity challenges, such as endpoint security, vulnerability management, threat detection and response, network security, data protection, and employee training. Overall, CSaaS has the potential to provide SMBs with the resources and expertise needed to effectively manage their cybersecurity needs, while also freeing up resources to focus on their core business activities.

References:

1. Cybersecurity for Small Businesses. https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

2. Small Business Cyber Security Guide. https://www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide

3. Russell Nicolet. Cybersecurity Statistics All Small Businesses Should Know. https://nicolettech.com/cybersecurity-statistics-all-small-businesses-should-know/

4. Poppy Gustafsson. 4 Cybersecurity Strategies for Small and Midsize Businesses. https://hbr.org/2021/09/4-cybersecurity-strategies-for-small-and-midsize-businesses

5. Edward Segal. Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report. https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=63c838d652ae

6. Lisa Ward. Small Businesses Struggle With an Increase in Cyberattacks. https://www.wsj.com/articles/small-business-cyberattacks-increase-11654540786

7. Rob Sloan. Which Industries Aren't Ready for a Cyberattack? https://www.wsj.com/articles/the-industries-most-vulnerable-to-cyberattacksand-why-11592786160

Oleksandr Butyrin

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

REDUCTION OF Security RISKS WITH IT GOVERNANCE PROCEDURES

Article [1] was dedicated to classification of security-related trade-offs which arise in the IT environment. The following main sources of contradictions were identified:

A) regulations
B) business requirements
C) technology

There are numerous techniques which address requirement gathering, trade-off negotiation and resolution [2]. However, if the decision favors business or technical considerations at the expense of security, the company is exposed to security risks and accumulates technical debt [3].

In this paper we will consider best practices and processes which should reduce security-related technical debt and related risks.

To ensure smooth IT operations, every company needs IT governance. The rules and scope can differ depending on company size, industry or location. Big corporations use well-established frameworks to implement IT governance. The TOGAF [4] is one of such frameworks. However, for smaller companies this approach is too cumbersome. They need to undertake a focused approach to implement some critical steps from enterprise frameworks and software development best practices:

1. Establish clear security standards including requirements for design, development and support. These standards can address

a) general principles, like information classification, data processing rules, storing credentials, logging;

b) mandatory and recommended tooling to perform specific security functions

c) specific recipes to implement certain functions

d) security processed to be followed, like vulnerability checking

2. Create Solution Design Authority with mandatory representation of security experts. That body must review and approve all significant changes to the IT environment. Additional tasks should include periodic review of applications and IT environment for compliance with company's standards, establishing

enterprise architecture, early review of the prospective projects and informing respective teams about potential issues.

3. Instantiate software development security standards into specific tooling, like

a) implementation of rigorous automated quality gates in CI/CD pipeline. The word „automated" is the key. In fact, some quality gates should be used on each step of SDLC (Software Development Life Cycle). Automated quality gates at build, test, release phases would prevent deviations from security standards. In particular, that approach should be used by companies, which use small frequent updates, like microservice architecture.

b) Performing automated security tests, either independently or as an integral part of overall test scenarios. That approach is attractive, among others, for companies that perform Test-Driven Development [5].

4. Instantiate security standards, which are related to support, into specific tooling and processes. The tasks covered should be:

a) check reports on vulnerabilities and bugs for standard software used in the company

b) perform periodic patching of software according to the level of vulnerability

c) check software dependencies and perform required updates or fixes

d) perform regular testing of the overall IT environment. The examples of such tests are penetration testing, search for credit card numbers on disks and in logs, disaster recovery exercises, etc.

Let's consider how these actions affect trade-off resolution. We will consider it by groups indicated above.

A. Changes required by regulations.

These changes are usually announced well in advance. As a rule, companies start specific projects to preserve compliance. In that case, setting clear security standards will help consolidating project requirements, and establishing Solution Design Authority will help on solution design phase.

A specific role of Solution Design Authority and Project Management Office would be to align projects. There will be a need to update some existing IT components and to introduce new ones. Since compliance could affect almost all IT components, Solution Design Authority (or similar technical function) must agree on a strategy to implement the changes. Then, both Solution Design Authority and Project Management Office should carefully track dependent projects.

B. Changes initiated by business.

These changes can be significant, like adding new applications, or small, which affect just one feature.

The approach to big changes is similar to the above. In this case, a project is started. Security standards will be used to gather all the requirements in time.

While big changes are usually considered in sufficient detail, small ones can slip past the Solution Design Authority. They are handled differently. Small changes can be caused by a bug fix or slight modification of functionality. No company can review in detail all the security requirements for each of these changes, primarily, because of their volume and urgency. Here, automation is the key. Developers and quality engineers can focus on delivering value, and, at the same time, they can be confident that deviations from security policies would be immediately detected.

Despite the work on a technical debt can not be classified as initiated by business, the same approach might apply.

C. Technology trade-offs.

Technology challenges can have a different nature. When technological advances are considered, Solution Design Authority must perform thorough analysis. As a result, this body can both accept perspective technology for a specific purpose, and initiate updates to the standards and procedures.

Another technological task, support, must rely on firm procedures. There should be no dispute if a team needs to implement high-value business changes and a critical fix at the same time. The procedures should define how the criticality is estimated and which action should be performed first. Clear procedures save time, which would be consumed by custom decision-making process. Also, a deviation from standards becomes an exception, which is easy to document and track.

Let us summarize. The best way of resolving contradictions and agreeing on reasonable trade-offs is „shifting trade-offs left", in other words, highlighting them as early as possible. That gives enough time to implement the required features or to review the release schedule.

Secondly, if standards are clearly defined and automated quality gates are implemented, then the security requirements will be enforced for any new or updated component. Any security exception will be subject to a specific discussion and special approval. Without automated quality gates, the company can expect unpleasant surprises at any time.

The four steps, indicated above, would minimize contradictions and misunderstanding between business, technical, support and security departments.

References:

1. Butyrin, O. (2022) "Security trade-offs in IT change management", Modern ways to solve the latest science problems: collection of abstracts of International scientific-practical conference, Kunovice, Czech Republic, November 27-28, 2022. Kunovice: Akademie HUSPOL, 2022, pp. 78-81. ISBN 978-80-7314-404-3.

2. Bass, L., Clements, P., Kazman, R. (2013). Software Architecture in Practice (3rd ed.). Addison-Wesley. ISBN 978-0-321-81573-6.

3. Technical debt definition https://en.wikipedia.org/wiki/Technical_debt

4. The TOGAF® Standard, Version 9.2. The Open Group. ISBN 1-947754-11-9.

5. Beck, Kent (2002). Test-Driven Development by Example. Vaseem: Addison Wesley. ISBN 978-0-321-14653-3.

Kostiantyn Chapistrak

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

INTERNAL THREATS TO INFORMATION SECURITY IN SMALL BUSINESSES

Information and data security is an essential concern for small businesses, which often have limited resources and lack the expertise to ward off the insidious threat of cyber-attacks.

Internal threats to information security refer to the vulnerabilities and risks that arise from within an organization, as opposed to those originating from external sources. These insidious threats can arise from many sources, including current or former employees, contractors, vendors, or anyone else possessing authorized access to the organization's information systems and data.

Internal threats to information security may be either intentional or unintentional, and the consequences of these threats can be devastating for the organization, such as data breaches, loss of intellectual property, financial loss, reputational harm, or other negative outcomes. Examples of internal threats include insider attacks, accidental data leaks, unauthorized data access, and data theft by employees or third-party vendors. These perils are not to be taken lightly, as they can quickly lead to dire consequences and lasting harm to the organization.

Importance of Information Security in Small Businesses

The importance of information security in small businesses can be summarized as follows:

1. **Protection of Sensitive Information:** Small businesses collect and store sensitive information, including customer data, financial information, and intellectual property. Information security ensures it is protected from unauthorized access, theft, or disclosure.

2. **Maintaining Business Continuity:** Cyberattacks can disrupt business operations, leading to downtime, lost productivity, and revenue loss. Information security measures such as backups, redundancy, and disaster recovery plans can help small businesses resume operations quickly after an attack.

3. **Compliance with Regulations:** Small businesses must comply with various data privacy and security regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Failure to comply with these regulations can result in legal and financial penalties.

4. **Protecting Business Reputation:** A data breach or cyber attack can damage a small business's reputation and lead to a loss of customer trust. Information security measures such as encryption, access controls, and monitoring can help prevent such incidents and maintain customer trust.

5. **Preventing Financial Loss:** Cybercrime can result in financial loss due to theft of funds, ransom demands, or costs associated with remediation efforts.

Internal Threats to Information Security in Small Businesses

In general, there are two broad categories of internal threats to information security in small businesses:

1. Malicious Insider Threats

Malicious insider threats refer to threats from insiders who intentionally cause harm to an organization's information security. These insiders can be current or former employees, contractors, or vendors with authorized access to the organization's systems and data.

There are several types of malicious insider threats that small businesses should be aware of, including:

- **Employee Theft:** Employees who have access to sensitive information can steal it for personal gain or to sell to outsiders. This can include stealing customer data, financial information, or intellectual property.
- **Sabotage:** Employees who are unhappy with their job or want to seek revenge can sabotage the organization's information security by deleting files, introducing malware, or disrupting business operations.
- **Insider Trading:** Employees who have access to confidential information can use it for personal gain or share it with outsiders for financial gain.
- **Cybercriminals:** Cybercriminals can pose as insiders to gain access to the organization's systems and data. They can then steal data, launch attacks, or extort money from the organization.

2. Accidental Insider Threats

One of the most common internal threats to information security in small businesses is employee negligence. Employees may accidentally disclose sensitive information or fall for phishing scams, opening the door for cybercriminals to access company data.

These are types of accidental insider threats:

- **Human Error:** Employees can accidentally delete or modify data, send sensitive information to the wrong recipient, use weak passwords, share login credentials, or fall for phishing scams that lead to data breaches.
- **Misconfigured Systems:** Employees can inadvertently misconfigure systems, leaving them vulnerable to cyber attacks.

- **Third-party Vendors:** Vendors who have access to the organization's systems and data can inadvertently cause harm through misconfigured systems, lack of security controls, or other vulnerabilities.

Mitigating Internal Threats for Information Security in Small Businesses

To protect sensitive information and maintain business continuity, small businesses must implement strong security measures to mitigate the risk of internal threats. This section will discuss some best practices for mitigating internal threats to information security in small businesses.

1. Implement Access Controls

Access controls are an essential component of any security program. Small businesses should implement access controls that limit access to sensitive information and systems based on the principle of least privilege. This means that employees should only have access to the data and systems they need to perform their job functions.

2. Conduct Employee Screening

Small businesses should conduct background checks and screening of all employees, contractors, and vendors who have access to sensitive information and systems. This can include criminal background checks, credit checks, and reference checks.

3. Provide Security Awareness Training

The training should cover topics such as password hygiene, phishing attacks, and social engineering tactics. Employees should be taught to recognize and report suspicious activity and to follow established security protocols.

4. Implement Incident Response Plans

The plan should include a defined chain of command, communication protocols, and procedures for containing and mitigating the incident. Small businesses should also conduct regular security drills and tabletop exercises to test the effectiveness of their incident response plans.

5. Regularly Review and Update Security Policies and Procedures

The policies and procedures should be accessible to all employees, contractors, and vendors and outline the acceptable use of company resources, data access privileges, and consequences for policy violations.

Case Study 1: Accidental Insider Threat

HypeAds is a small marketing agency with eight employees. One of their employees, a graphic designer, unintentionally sent an email with private client information to the incorrect person. The recipient was a rival, and the information contained specifics of a secret marketing plan. The competitor used the information to gain an advantage in the market, and the client subsequently

terminated their contract with HypeAds. HypeAds suffered severe brand harm and financial loss due to the unintentional insider threat.

Information Security recommendations:

1. Security awareness training should be provided to all employees to prevent such incidents.
2. Employees should double-check recipient email addresses before sending sensitive information.
3. Encryption and digital signatures can be used to secure sensitive information sent via email.

Case Study 2: Malicious Insider Threat

Protaxes is a small accounting firm with ten employees. One of their employees, an accountant, was terminated due to poor performance. The accountant was unhappy with the termination and decided to seek revenge on the company. This employee had access to both client and financial information for the business. Using this access, the accountant deleted all client files and the company's financial information from its servers. The erasure of the data severely disrupted business operations and cost the corporation a sizable sum of money. The business discovered the nefarious insider and filed a lawsuit against them.

Information Security recommendations:

1. Termination of employees should be handled with care and with proper documentation to avoid misunderstandings.
2. Access control measures should be implemented to restrict access to sensitive data to authorized employees only.
3. Regular backups of important data should be taken and stored offsite to mitigate the risk of data loss.

Conclusion

In conclusion, internal threats to information security are a significant risk for small businesses. While these companies may face unique challenges in implementing effective security measures, there are many affordable and effective solutions available that can help them protect themselves from internal threats.

This requires a multi-layered approach to information security that involves access controls, employee screening, security awareness training, incident response plans, regular policy and procedure review.

However, such measures alone may not be enough, and businesses must conduct regular security audits and risk assessments to identify potential vulnerabilities. By doing so, even small companies can safeguard their information assets and protect their reputation and financial stability.

References:

1. McKeever, G. (2019, December 29). What Is an Insider Threat, Malicious Insider Attack Examples, Imperva. Learning Center. https://www.imperva.com/learn/application-security/insider-threats/

2. Smith, C. (2023, March 1). How can you prevent insider threats when none of your insiders are actually "inside"? Delinea Inc. https://delinea.com/blog/insider-threats-in-cyber-security

Maksym Kozachenko

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

GLOBAL EFFORTS BY LEADING COUNTRIES IN CYBERSECURITY STRENGTHEN

Due to the frequency and severity of cyberattacks, cybersecurity is a crucial issue in today's world. By 2025, cybercrime-related losses are projected to cost the global economy $10.5 trillion annually [1], according to a report by Cybersecurity Ventures. Costs associated with data breaches, cyberattacks, intellectual property theft, and other cybercrimes are included in this amount.

The number of daily cyberattacks serves as additional evidence of the significance of cybersecurity. A daily average of 2,000 complaints about cybercrime were made to the FBI's Internet Crime Complaint Center in 2020 [2]. This demonstrates the severity of the issue and the requirement for robust cybersecurity measures to safeguard people, organizations, and governments.

Cyber attacks can have a devastating effect, with possible repercussions ranging from monetary losses to reputational harm and, in some cases, even physical harm. For instance, it is estimated that the 2017 NotPetya ransomware attack cost the world between $10 billion and $15 billion in damages [3].

Effective cybersecurity measures are becoming more and more essential as a result of the ongoing development of technology and its integration into daily life. Countries all over the world are making serious efforts to protect their citizens and infrastructure from cyber threats as the threat of such attacks increases.

United Kingdom. The National Cyber Security Strategy, which outlines the government's strategy for enhancing cybersecurity in the UK, was introduced in the United Kingdom in 2016 [4]. The plan calls for strengthening vital infrastructure, developing cybersecurity expertise, and enhancing the UK's capacity to identify and respond to cyberattacks.

The National Cyber Security Centre (NCSC) [5], which offers direction and support to government agencies, companies that operate critical infrastructure, and other businesses, has also been established in the UK. The national cybersecurity incident response team for the UK is run by the NCSC.

The UK government has started several programs like the Cyber Schools Programme, Cyber Discovery Programme, and CyberFirst Programme [6] to help young people develop their cybersecurity skills. To combat cybercrime, the

government has also created the National Cyber Crime Unit and the Cyber Security Information Sharing Partnership [7].

United States. For many years, the US has led the world in cybersecurity initiatives. The US government has set up a number of cybersecurity initiatives, such as the Cybersecurity and Infrastructure Security Agency (CISA), which is in charge of defending the country's vital infrastructure against cyberattacks [8].

The US government has also started some programs to advance cybersecurity expertise, such as the CyberCorps Scholarship for Service Program, which offers financial aid to students majoring in cybersecurity in exchange for their service in government cybersecurity positions [9].

The National Initiative for Cybersecurity Education (NICE), which the US government also established, aims to improve the overall cybersecurity posture of the country by accelerating the accessibility of educational and training resources created to enhance the knowledge, skills, and abilities of every segment of the population [10].

In 2021, an executive order was issued by the President of the USA with the aim of bolstering cybersecurity. The order details various measures, including but not limited to, fortifying the security of federal networks, broadening the exchange of information between the public and private domains, and devising a uniform playbook for addressing cybersecurity breaches. [11]

Israel. Israel is widely regarded as a leader in cybersecurity on the international stage. The nation has a highly developed cybersecurity ecosystem made up of governmental organizations, academic institutions, and for-profit businesses. The National Cyber Directorate, established by the Israeli government, is in charge of safeguarding Israel's critical infrastructure and online presence [12].

Israel has also launched several programs to advance cybersecurity research and development, including the National Cyber Security Research and Development Center and the CyberSpark Industry Initiative, which aims to create a cybersecurity ecosystem in southern Israel.

The Israeli government created the Cyber Education Center, which offers cybersecurity education programs to students, teachers, and the general public, in order to promote cybersecurity education and training. Additionally, the government launched the Cyber Girls program intending to entice more girls to pursue careers in cybersecurity [13].

Overall, countries all over the world are taking action to strengthen their security strategy and safeguard their infrastructure and population against online threats. The above-mentioned programs are just a few examples of the initiatives that governments are taking to deal with this pressing issue. Cybersecurity will

probably continue to be a top priority for nations around the world as technology develops and cyber threats become more complex.

References:

1. Cybersecurity Ventures. (2020). https://web.archive.org/web/20230212110526/ https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

2. FBI. (2020). IC3 Annual Report Released. https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

3. Wired. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

4. National Cyber Security Strategy 2016-2021. (2016). HM Government. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

5. National Cyber Security Centre. https://www.ncsc.gov.uk/

6. CyberFirst. National Cyber Security Centre. https://www.ncsc.gov.uk/cyberfirst

7. National Cyber Crime Unit. National Crime Agency. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/national-cyber-crime-unit

8. Cybersecurity and Infrastructure Security Agency. Department of Homeland Security. https://www.dhs.gov/cisa

9. CyberCorps Scholarship for Service Program. National Science Foundation. https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5517

10. National Initiative for Cybersecurity Education. National Institute of Standards and Technology. https://www.nist.gov/itl/applied-cybersecurity/nice

11. Executive Order on Improving the Nation's Cybersecurity. The White House. (2021). www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

12. National Cyber Directorate. https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page

13. Israel Ministry of Foreign Affairs. https://mfa.gov.il/MFA/AboutIsrael/Science/HighTech/Pages/Cybersecurity.aspx

Viktor Moskvych

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

FORMAL METHODS FOR SECURE CYBER SYSTEMS

As technology continues to advance, the importance of cybersecurity grows as well. With the rise of the internet and the increasing amount of sensitive information being stored online, it's essential to have strong security measures in place. One way to ensure the security of cyber systems is by using formal methods.

Formal methods are mathematical techniques used to analyze and verify the correctness of systems. They provide a systematic way to validate security properties of cyber systems. The goal of using formal methods is to minimize the likelihood of security vulnerabilities and ensure that systems work as intended.

The use of formal methods in cybersecurity is not a new concept. In fact, formal methods have been used for decades to design and verify hardware and software systems. However, their application to cybersecurity is relatively new, and there is still much to be explored.

One significant advantage of using formal methods in cybersecurity is that they provide a way to test systems in a controlled environment. By using mathematical models to simulate cyber attacks, potential vulnerabilities can be identified and addressed before they can be exploited by attackers.

Moreover, formal methods can also be used to verify that security properties hold for a system. This can include properties such as confidentiality, integrity, and availability, which are critical for ensuring the security of cyber systems. By using formal methods, security properties can be verified without having to rely on subjective assessments.

In addition to analyzing and verifying security properties, formal methods can also be used to develop secure systems. By using formal methods during the development process, security requirements can be incorporated into the system's design, rather than being added as an afterthought. This can result in a more secure system overall.

Formal methods have been applied in a variety of practical use cases, spanning from operating systems to aerospace and healthcare. Here are some examples of how formal methods have been used in practice:

Operating Systems: Operating systems provide many services that applications rely on, such as a network stack, a file system, process isolation, inter-

process communication, and so on. The security of applications depends pervasively on the underlying OS, making operating systems an appealing target for applying formal methods. For instance, if a system executes multiple applications (or virtual machines) on the same computer, the OS kernel is responsible for ensuring that a malicious (or compromised) application is unable to tamper with the execution of other applications. Even if the computer is used for running just one application, OS-level process isolation is often used to isolate less-trustworthy components of a large application to mitigate the damage from a potential compromise. Ensuring the correctness of process isolation in an OS kernel could provide stronger assurance that compromised components cannot tamper with the rest of the system [1].

Aerospace and Defense: Formal methods have been used in the design and verification of aircraft systems, such as avionics and flight control systems. By using formal methods, engineers can verify the safety and correctness of aircraft systems, ensuring that they meet the high standards required for aerospace applications.

Cryptography: Formal methods have been used in the design and analysis of cryptographic protocols to ensure their security properties. Formal methods can be used to prove that a cryptographic protocol is secure, or to identify potential vulnerabilities in the protocol that could be exploited by attackers.

Healthcare: Formal methods have been used in healthcare systems to ensure the safety and correctness of medical devices and software systems. By using formal methods, engineers can verify that medical devices operate as intended and do not pose a risk to patients.

Banking and Finance: Formal methods have been used in banking and finance to verify the correctness of financial systems and transactions. By using formal methods to ensure the correctness of financial systems, potential errors can be caught early on, preventing issues such as financial fraud.

Overall, the use of formal methods in practice has shown promising results in ensuring the correctness and safety of complex systems. While the application of formal methods may be challenging and time-consuming, the benefits of using them can be significant, particularly in fields where safety and correctness are critical, such as aerospace and healthcare. As the use of formal methods continues to grow, it's likely that we will see even more practical use cases emerge in the future.

One of the implementations of formal methods that is used in practice nowadays is TLA+. TLA+ is a formal specification language that can be used to model and verify complex systems. It was developed by Leslie Lamport, a computer scientist who is well known for his work on distributed systems and

algorithms. TLA+ is based on temporal logic, which is a logic that can reason about systems that change over time.

TLA+ provides a way to specify a system's behavior in a precise and unambiguous way. By using TLA+, engineers can create a model of a system and then use that model to check the system's behavior against a set of desired properties. This process is known as model checking, and it allows engineers to catch potential errors or bugs early in the design process.

One of the main benefits of using TLA+ is that it allows engineers to reason about the behavior of a system as a whole. This can be particularly useful in the design of complex distributed systems, where it can be challenging to reason about the behavior of individual components in isolation. By using TLA+, engineers can create a model of the entire system and reason about its behavior as a whole.

TLA+ has been used in a variety of practical applications, including the design of distributed systems, network protocols, and algorithms. It has also been used in the development of software and hardware systems, as well as in the verification of cryptographic protocols.

One notable example of the use of TLA+ is in the design of the Amazon Web Services Simple Storage Service (S3). S3 is an object storage service that provides industry-leading scalability, data availability, security, and performance [2]. To ensure the correctness and scalability of the system, Amazon used TLA+ to model the system's behavior and verify its properties. This process helped to identify and correct potential issues before the system was deployed, ensuring its reliability and scalability.

Despite the benefits of using formal methods in cybersecurity, there are some challenges that must be addressed. One such challenge is the difficulty of applying formal methods to large, complex systems. Formal methods can be computationally expensive, and analyzing large systems can be time-consuming.

Another challenge is the lack of expertise in formal methods among cybersecurity professionals. While the use of formal methods is becoming more widespread, there is still a need for more education and training to ensure that cybersecurity professionals can effectively use them [3].

In conclusion, formal methods provide a powerful tool for ensuring the security of cyber systems. By using mathematical techniques to analyze and verify security properties, potential vulnerabilities can be identified and addressed, and security can be incorporated into system design. While there are still some challenges to overcome, the benefits of using formal methods in cybersecurity are clear. As technology continues to advance, it's essential to have

strong security measures in place, and formal methods can help to achieve this goal.

References:

1. Report on the NSF Workshop on Formal Methods for Security, https://arxiv.org/pdf/1608.00678.pdf

2. Use of Formal Methods at Amazon Web Services, https://lamport.azurewebsites.net/tla/formal-methods-amazon.pdf

3. Formal methods as a path towards better cybersecurity, https://www.brookings.edu/techstream/formal-methods-as-a-path-toward-better-cybersecurity/

Andrii Radahuz

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

CHAT-BASED ROLE-PLAYING GAMIFICATION OF CYBERSECURITY REVIEW

The aim of this thesis is to high-level design a Slack chatbot that facilitates a text-based role-playing game for security review. The game is aimed at improving the cybersecurity skills of players, and the chatbot will serve as the main interface for game interactions. The research methodology involves an analysis of existing text-based role-playing games, review of relevant literature on cybersecurity, and a user-centered design approach to the development of the chatbot. The thesis concludes that text-based role-playing games can be a useful tool for improving cybersecurity awareness, and Slack chatbots can serve as an effective interface for such games. The appendices contain technical documentation on the design and implementation of the chatbot.

[1] Text-based role-playing games have been a popular genre since the dawn of computer games. In recent years, chatbots have become more advanced, and so has their integration into online gaming communities. Slack is one of the most widely used communication tools in the corporate world, but it can also be used for recreational purposes. In this thesis, we investigate the design of a Slack chatbot for a text-based role-playing game of security review.

The design of such a chatbot must take into account the requirements of the game, the constraints of the Slack platform, and the best practices in chatbot design. Our literature review covers various aspects of chatbot design and implementation, including dialogue systems, natural language processing, and game design.

By building a prototype of the chatbot and conducting user tests, we explore the effectiveness of our design and the user experience it provides. The results of our study will inform future work on designing chatbots for other types of games and applications.

Literature

- Zhou, L., Parra, D., & Xiang, C. (2019). Dialogue systems: Advances and challenges. IEEE Intelligent Systems, 34(4), 4-10.
- Li, B., Li, J., Li, H., & Li, X. (2018). Chatbot research: A literature review. International Journal of Social Robotics, 10(3), 351-364.

- Björk, S., & Holopainen, J. (2005). Patterns in game design. Hingham, MA: Charles River Media.

High-level Architecture

- The chatbot will be implemented as a serverless application using a cloud platform such as AWS Lambda or Google Cloud Functions.
- The chatbot will interface with the Slack platform using the Slack API and will accept only text commands.
- To integrate the chatbot into the team's DevSecOps pipelines, it will be connected to the team's source control system (e.g. GitHub), and will automatically execute security review tasks on new code commits or pull requests.
- The chatbot will use a combination of static code analysis and dynamic security testing techniques to identify security vulnerabilities and provide feedback to the developers.
- The chatbot will store information about identified vulnerabilities and the corresponding remediation steps in a database, which can be used to track the progress of security reviews over time.
- To ensure scalability and high availability, the chatbot will be designed to run across multiple geographic regions and will leverage auto-scaling features provided by the cloud platform.

User Interface and Process

The user interface for the Slack chatbot for our security review RPG game will consist of text-based commands. The bot will be integrated into the team's DevSecOps pipelines, facilitating the three main tasks of the security review campaign: Threat Modeling, Code Review, and Security Testing.

For Threat Modeling, each user will be able to brainstorm threats on their own, during the development process, and can submit their ideas through the Slack chatbot by typing the /add-threat command, which will prompt the user to describe the threat. The submitted text will be stored in a shared document accessible to all team members, who can add to or refine the threat descriptions as necessary.

For Code Review, once the Threat Modeling process is complete, each member of the development team will be assigned a specific code snippet to review, based on their chosen race and class. By using the /code-review command, developers can retrieve their assigned code snippet within the Slack chatbot and perform their review.

During Security Testing, one part of the team will write down the test plan using the /security-test-case command, while the other part of the team will conduct the testing. The specific roles of the team members will depend on their chosen race and class.

In conclusion, this thesis presented the design of a Slack chatbot for a text-based role-playing game of security review, which allows developers to identify potential threats, conduct code reviews, and security testing through an intuitive user interface. The chatbot provides an engaging and collaborative approach to DevSecOps processes and promotes a more efficient way of conducting security reviews.

By facilitating the identification of potential security threats, improving the efficiency of code review, and promoting security testing, the chatbot can significantly enhance the security review process and prevent potential security breaches. The integration of the chatbot into the DevSecOps pipeline allows for a more streamlined approach to security review, which can result in cost savings and faster time-to-market.

The chatbot's high-level architecture was designed with Slack's text commands in mind, making it easily accessible to developers. By utilizing the chatbot's commands, developers can perform tasks such as adding threats to a shared document, reviewing code snippets, and writing test plans. The chatbot has the potential to transform security review into an engaging and fun experience for developers, while also promoting a more secure software development process.

Future work could include expanding the range of available quests and further testing and optimizing the chatbot to improve the user experience. Overall, the Slack chatbot offers a promising tool for improving the security of software development and promoting a more engaging and fun approach to DevSecOps.

References:

1. Turner, E. (2020). Chatbots in Gaming: A Comprehensive Guide to Chatbots for Games. New York: Apress.

Ihor Roid

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

INFORMATION SECURITY CONCERNS IN ONLINE PAYMENT PROCESSING

Most of today's software solutions are distributed benefitting from a service model, where the customer pays a subscription fee to gain temporary access to a certain set of services or digital goods. This model is constantly expanding and today it can even be found in automotive industry, where vendors offer subscription based model for such services as navigation or seat heating. As a result, the paramount component of every software solution today is its payment processing engine. Although it does not necessarily mean that this engine will have to deal with is the payment data directly, it still remains one of the most sensitive components of a system in terms of information security. Information security is a critical concern for businesses operating in today's digital landscape. As more and more transactions are conducted online, the risk of cyber threats and data breaches increases. In particular, payments are a sensitive area where security is of paramount importance. In this article, we will explore different aspects of information security, points for consideration when dealing with payments, and ways to address possible cybersecurity threats in software solutions.

Different Aspects of Information Security

Information security encompasses a wide range of practices and technologies that are designed to protect data and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The key aspects of information security are confidentiality, integrity, availability, authentication and authorization. Confidentiality refers to the protection of sensitive information from unauthorized access or disclosure. Confidential information can include personal data, financial information, trade secrets, and other sensitive data. Integrity is about protection of data from unauthorized modification or deletion. Ensuring data integrity is essential to prevent fraud or data loss. Any breach of integrity may lead to severe consequences that may even lead to crash of business, legal responsibility, reputational damage etc. Availability stands for the ability of authorized users to access data and systems when needed. Ensuring availability is crucial to maintain business continuity and avoid disruption. Today's services operate 24/7 and are typically available world-wide. Therefore poor availability directly leads to potential loss of profit. Another crucial aspect of information

security in payment processing is authentication. This refers to the process of verifying the identity of users or devices to ensure that they are authorized to access data or systems. Authorization on the other hand should not be confused with the prior term, as it stands for the process of granting users or devices access to specific data or systems based on their identity and privileges.

Points for Consideration When Dealing with Payments

Payments are a particularly sensitive area of information security because they involve the transfer of financial information and funds. Payment processing cannot be implemented today without taking the following points into consideration, because not only will it expose the company but also its customers to significant risks.

Compliance: Businesses that handle payments must comply with various regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). Compliance with these standards is critical to ensuring the security of payment data. If those are ignored, the company is highly likely to fail in obtaining their license to provide services on the territory where these regulations take place. [1]

Encryption: Payment data should be encrypted to protect it from unauthorized access. Strong encryption algorithms should be used to ensure that payment data cannot be decrypted by unauthorized parties. With growth of computational velocity algorithms should use long encryption keys (today a common option is 512Kb keys). Depending on the business case additional measures should be taken, such as asymmetric encryption (using public/private key pairs) and key rotation as an extra effort to protect data from key compromisation. [2]

Two-Factor Authentication is an access control standard of every commercial solution nowadays. It should be used to ensure that only authorized users can access payment data. Two-factor authentication requires users to provide two forms of identification, such as a password and a security token or biometric data. The idea behind it lies in the concept of two factors: one access key is something a person knows (passphrase or PIN) and another one is something a person owns (like a physical key or an electronic device). [3]

Limit Access: Access to payment data should be limited to authorized users and systems. Access controls should be implemented to ensure that only those with a need to know can access payment data.

Regular Audits: Regular audits should be conducted to ensure that payment systems and processes are secure and compliant with relevant regulations and standards.

Ways to Address Possible Cybersecurity Threats in Software Solutions.

It’s crucial to establish measures addressing the cybersecurity in the early stages of a solution design. Implementing those afterwards may lead to additional problems at integration phase, refactoring or technological incompatibility. There are several ways to address possible cybersecurity threats in software solutions.

Secure coding practices should be followed to ensure that software is not vulnerable to common attacks, such as SQL injection or cross-site scripting. This involves using secure coding frameworks, regularly testing code for vulnerabilities, and implementing security controls. Software quality is evaluated on different levels, including static vulnerability analysis of code and its deployment, dependency and software environment analysis, infrastructure etc. For best results the software should be constantly analyzed against common security frameworks, such as OWASP TOP 10, STRIDE, MSDL, CIS and others. [4]

Threat modeling involves identifying potential threats and vulnerabilities in software systems and designing countermeasures to address them. This approach can help to identify potential weaknesses and improve the overall security of software solutions. Penetration testing involves testing software systems to identify vulnerabilities and weaknesses. This can be done by simulating attacks and assessing the ability of software systems to withstand them. [5]

Regular patch management is critical to ensuring that software systems are up-to-date and protected against known vulnerabilities. Software vendors should release patches and updates regularly, and businesses should ensure that these are installed promptly.

The most vulnerable point in each system is the end user. User education is essential to ensure that employees and customers are aware of potential threats and are equipped to identify and report suspicious activity. Whereas software systems strictly follow the implied rules, human beings tend to simplify their interactions with the systems, typically neglecting certain rules over time, mostly due to the fact that no issues take place for a certain period of time. That’s why it’s very important to conduct trainings and educate users on a regular basis, identify new types of threats and adapt the training protocols accordingly.

Information security is a critical aspect of software development, and the risks posed by cyber threats can have significant consequences. Effective approaches must be implemented to manage these risks, including encryption, authentication, access control, and regular security audits. To ensure the security of software solutions, best practices should be followed throughout the development process, and security should be considered as an integral part of software design, development, and maintenance. Indulgent attitude to information security may lead to significant consequences, including collapse of ones business or even criminal liability.

References:

1. *Zalewski M. The Tangled Web: A Guide to Securing Modern Web Applications. No Starch Press. 2011*
2. *Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley. 1995*
3. *Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley. 2008*
4. *Shostack, A. Threat Modeling: Designing for Security. Wiley. 2014*
5. *J. Erickson. Hacking: The Art of Exploitation. No Starch Press. 2008*

Ievgenii Zhmur

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

INFORMATION SECURITY CONCERNS OF CIVILIAN INFORMATION SYSTEMS IN WARTIME CONDITIONS

Information security concerns in wartime conditions are not limited to military information systems alone. Civilian information systems are also vulnerable to a range of threats, from cyber-attacks to physical sabotage. The disruption of civilian information systems can have significant consequences, affecting critical infrastructure, healthcare, and other essential services. In this article, we will examine the key information security concerns of civilian information systems in wartime conditions.

Cybersecurity.

One of the most significant information security concerns in wartime conditions is cybersecurity. Cyber-attacks on civilian information systems can be launched by nation-states, non-state actors, or even opportunistic cybercriminals seeking to take advantage of the chaos of war. Cyber-attacks can take many forms, including ransomware, DDoS attacks, and phishing attacks. These attacks can result in the loss of sensitive information, the disruption of critical infrastructure, and even the destruction of physical infrastructure.

To mitigate the risk of cyber-attacks, civilian organizations need to adopt robust cybersecurity measures. This includes implementing strong encryption protocols, establishing secure communication channels, and regularly updating software and hardware systems. It also requires developing a robust incident response plan to quickly detect and respond to cyber-attacks.

Encryption is a crucial element in protecting sensitive information from unauthorized access during wartime conditions. A strong encryption protocol ensures that data is not easily accessible to hackers, which can prevent or minimize the loss of sensitive information. Military-grade encryption protocols are often used to secure data transmission and storage, but civilians can also use encryption tools to protect their information.

Establishing secure communication channels is another critical aspect of mitigating the risk of cyber-attacks. In wartime conditions, there may be a need for alternative communication channels to ensure secure and reliable communication. Civilians can use secure messaging apps that utilize end-to-end encryption, which ensures that only the sender and recipient can read the message.

Regular updates to software and hardware systems are also crucial in mitigating the risk of cyber-attacks. Updates often contain security patches that address vulnerabilities, making it harder for hackers to exploit them. Failing to update software and hardware systems may result in vulnerabilities that hackers can exploit to launch attacks.

It is also important for civilian organizations to develop a robust incident response plan that outlines the steps to be taken in the event of a cyber-attack. The incident response plan should include steps to identify the nature and scope of the attack, contain the attack, and recover from the attack. Regular testing and updating of the incident response plan can help ensure that it remains effective and relevant. [1]

Physical security.

In addition to cyber-attacks, civilian information systems are also vulnerable to physical attacks. This includes attacks on critical infrastructure, such as power grids, water systems, and transportation networks. In wartime conditions, physical attacks can be particularly devastating, disrupting essential services and causing significant damage.

To protect against physical attacks, civilian organizations need to establish strong physical security measures. This includes securing critical infrastructure with physical barriers, surveillance systems, and access controls. It also requires developing contingency plans to quickly restore operations in the event of an attack.

Physical security measures should include barriers that make it difficult for attackers to access critical infrastructure. This can include fencing, walls, and gates. Surveillance systems such as cameras and motion detectors can also help detect and deter attackers.

Access controls are also critical in ensuring physical security. Access control measures should limit access to critical infrastructure to authorized personnel only. This can be achieved through the use of key cards, biometric scanners, or other access control systems.

Contingency plans are also essential in restoring operations in the event of a physical attack. The contingency plan should outline the steps to be taken to restore critical infrastructure, including identifying alternative infrastructure or resources that can be used temporarily. [2]

Human factors.

Human factors are another critical information security concern in wartime conditions. Civilians, like military personnel, are under a significant amount of stress and pressure during wartime conditions, which can lead to lapses in

judgment or mistakes. This can result in information security breaches, either through accidental or intentional actions.

To mitigate the risk of human error or intentional sabotage, civilian organizations need to establish strict security protocols and procedures. This includes implementing strict access controls, monitoring employee activity, and providing regular training and education on information security. [2]

Access controls should be implemented to limit access to sensitive information and systems to only authorized personnel. Monitoring employee activity can help detect any suspicious behavior or actions that may indicate an intentional breach. Regular training and education on information security can help ensure that employees are aware of their roles and responsibilities in protecting sensitive information.

It is also important to establish a culture of security within the organization. This includes promoting a culture of security awareness, encouraging employees to report any suspicious behavior, and rewarding good security practices. [3]

Backup and recovery.

During wartime conditions, it is essential for civilian organizations to ensure that they have a backup and recovery plan in place. This includes regularly backing up critical data and ensuring that the backup systems are secure and accessible.

A backup and recovery plan can help ensure that essential data is not lost in the event of a security breach or physical damage to information systems. It can also help organizations quickly recover from an attack or disruption.

Organizations should regularly test their backup and recovery plans to ensure that they are effective and that they can be implemented quickly and efficiently in the event of an emergency. [4]

International and regulatory compliance.

Civilian organizations operating in wartime conditions may also face international and regulatory compliance concerns related to information security. These can include compliance with international treaties and agreements related to cyberwarfare, as well as compliance with local regulations related to data privacy and protection.

Organizations should stay informed of international and regulatory compliance requirements and ensure that their information security measures are in line with these requirements. This can include implementing strong data protection measures, such as encryption and data anonymization, and ensuring that all data handling and processing activities are compliant with relevant regulations. [5]

Collaboration and information sharing.

During wartime conditions, civilian organizations may also need to collaborate and share information with other organizations, including military

organizations. This can raise information security concerns related to data confidentiality and integrity.

To ensure the security of collaborative efforts and information sharing, organizations need to establish secure communication channels and protocols. This includes using encryption and other security measures to protect sensitive data and ensuring that only authorized personnel have access to this data.

Organizations should also establish clear guidelines and protocols for information sharing and collaboration to ensure that all parties are aware of their roles and responsibilities in protecting sensitive informational event of a disruption. [5]

Conclusion

In conclusion, information security concerns in wartime conditions are not limited to military information systems. Civilian information systems are also vulnerable to a range of threats, from cyber-attacks to physical sabotage. To mitigate the risk of information security breaches, civilian organizations need to adopt robust cybersecurity measures, establish strong physical security measures, address human factors, and ensure supply chain security.

Establishing a culture of security within the organization is also critical in promoting awareness and encouraging good security practices. Regular testing and updating of security measures and incident response plans can help ensure that they remain effective and relevant. By addressing these information security concerns, civilian organizations can help ensure the continuity of critical services and infrastructure during wartime conditions.

References:

1. Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. 2014.

2. Alexander, D. Information Security Management Principles. BCS. 2020.

3. F. Tipton Information Security Management Handbook. Auerbach Publications. 2006.

4. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley. 2008.

5. Steinberg, J., O'Hanlon, M. The Art of War in the Network Age: Back to the Future. Routledge. 2017.

ПСИХОЛОГІЯ; ПЕДАГОГІКА (в т. ч. ФІЛОЛОГІЯ)

Мороз Л. І.

доктор психологічних наук, професор,
професор кафедри психології

Андрусик О. О.

аспірантка, викладач кафедри психології
Уманського державного педагогічного університету імені Павла Тичини,
м. Умань, Україна

ХАРАКТЕРИСТИКИ ЕМОЦІЙНОСТІ ВИКЛАДАЧА ЯК ЧИННИК ФОРМУВАННЯ ТВОРЧОЇ ОСОБИСТОСТІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Системотвірною складовою освітнього процесу, на якій він будується і без якої втрачає сенс, є явище педагогічної взаємодії як сукупності навчальних, виховних, соціальних, міжособистісних інтеракцій у діаді «педагог - здобувач освіти». Освітній процес неможливий без педагогічної комунікації, у ході якої виникають та отримують розвиток різноманітні взаємопов'язані між собою соціально-психологічні явища та прояви міжособистісного впливу. Первинним змістом педагогічного спілкування є організація різнорівневої навчально-пізнавальної, творчої активності здобувачів освіти з метою досягнення комплексного розвиваючого ефекту. Тому очікується, що закономірним наслідковим результатом педагогічної взаємодії буде прогресивний розвиток, покращення та вдосконалення особистісно-пізнавальних ресурсів здобувачів освіти до рівня їх готовності та спроможності здійснювати самостійний творчий пошук та внесок у межах тієї чи іншої царини знань або галузі майбутньої професійної діяльності. Численні соціально-психологічні явища у площині педагогічної взаємодії, їх закономірні зв'язки й ефекти впливу ставали предметом численних наукових досліджень. Результати їх вивчення висвітлювались у працях як психологів, так і педагогів, а саме Н. Грисенко, М. Кулеши, І. Ломпшера, А. Макаренка, С. Максименка, Е. Носенко, О. Погрібної, В. Росохи, О. Саннікової, Б. Фредріксон, Ф. Шрадера тощо.

Враховуючи те, що у будь-якому спілкуванні спостерігаються численні ефекти міжособистісного впливу, важливим «інструментом» праці

викладача, як провідного суб'єкта навчально-виховного впливу, є його особистість. Саме у безпосередній взаємодії зі здобувачами освіти відбувається маніфестація більшості особистісних якостей педагога. При цьому варто розрізняти два рівні педагогічної комунікації – міжособистісний та власне навчальний. Міжособистісний рівень педагогічного спілкування, характеризуючи особливості взаємостосунків та ставлення суб'єктів освітнього процесу один до одного, визначає емоційну компоненту навчально-пізнавальної діяльності та проявляється у вигляді різноманітних ефектів міжособистісного впливу на емоційну сферу здобувача освіти шляхом зараження, наслідування тощо. Змістом навчального рівня педагогічного спілкування є комунікація щодо змісту навчального матеріалу, що передбачає активне залучення та використання потенцій когнітивної сфери здобувача освіти з метою її інтенсивного розвитку.

Характеристики емоційності педагога визначають експресивну сторону педагогічного спілкування та, безпосередньо спостерігаючись здобувачами освіти, позначаються на перебігу їх навчально-пізнавальної діяльності шляхом створення специфічного афективного тла її здійснення, що у свою чергу, може впливати на процес формування їх творчого потенціалу. Творчій особистості притаманні такі особистісні характеристики як виражена потреба в самоактуалізації та самоствердженні, спонтанність та чутливість, емоційна зрілість, критичність та самостійність мислення, нонконформізм. Необхідно зазначити, що плекання творчої особистості в освітньому середовищі можливе шляхом першочергового забезпечення творчої ідентичності здобувачів освіти, що безпосередньо залежить від характеру та стилю професійної активності викладача [3]. Очевидним є те, що характер та стиль професійної діяльності викладача залежить від стійких характеристик його емоційності.

За визначенням О. Саннікової, емоційність являє собою комплекс індивідуально-стійких властивостей, які відображають особливості виникнення і перебігу емоційних переживань і характеризують стійке відношення до навколишнього світу і особливості взаємодії з ним. На відміну від актуальних або ситуативних (транзитних) переживань (емоційних реакцій або емоційних станів) емоційність характеризує позаситуативну, стійку схильність до переживань емоцій певного характеру та модальності [4]. Для результативності педагогічної діяльності досить важливими є динамічні та якісні параметри емоційності. Під динамічними параметрами емоційності розуміється експресія, сила, інтенсивність, тривалість, швидкість виникнення, перебігу та зміни емоційних переживань. Якісні параметри емоційності несуть інформацію про модальність та знак провідних емоцій.

Структура якісних характеристик емоційності передбачає виділення стійкої схильності до переживання позитивних або негативних емоцій, а також таких їх модальностей як радість, гнів, страх, сум, спокій [4].

Природа творчої активності має в своїй основі стратегію мисленнєвого комбінування, що передбачає вільне володіння навичкою цілісного сприйняття того чи іншого об'єкту в усій його багатогранності та вміння диференціації, розчленування цього ж об'єкта на окремі складові [2]. Тобто очевидним є те, що творчий процес органічно поєднує такі процеси мислення як аналіз та синтез на вершині їх інтенсивності та продуктивності. Творчий студент кмітливий, вільно орієнтується у навчальному матеріалі, спроможний його переосмислити та продукувати на цій основі нове знання.

Творчий процес в освітньому середовищі може значно інтенсифікуватися за умови створення сприятливої психологічної атмосфери з вираженим превалювання позитивних емоцій серед його учасників. Емоційний стан та настрій – важливий чинник вільного прояву творчих потенцій, формування готовності до творчості під час навчальних занять, що при постійному вправлянні перетворюється на стійку особистісну рису. При цьому очевидним є те, що викладач з превалюючою емоційною модальністю «Радість» за рахунок психологічних механізмів емоційного зараження та наслідування буде створювати комплементарний позитивний емоційний стан у студентів. У той же час педагоги з провідною модальністю «Гнів» з високою часткою вірогідності будуть продукувати в студентській аудиторії емоції негативного спектру або ж у випадку превалювання астенічних емоцій («Сум», «Страх») взагалі втрачати увагу студентів та мати значні труднощі контролю ходу занять.

Психологічний механізм впливу особливостей емоційності викладача на формування творчих здібностей здобувачів вищої освіти розкривається завдяки накопичених станом на теперішній час емпіричним даним про характер зв'язку позитивних емоцій з функціонуванням когнітивної сфери особистості. Б. Фредріксон експериментально довела корисний вплив позитивних емоцій на перебіг інтелектуальних процесів, що виражається в підвищенні різноманіття, нестандартності та варіативності когнітивного «продукту» (думок, рішень, ідей) [5]. М. Кузнєцова, підсумовуючи результати свого дослідження щодо ролі оптимізму в структурі саморегуляції навчально-пізнавальної діяльності здобувачів вищої освіти, зазначає, що студенти з оптимістичним пояснювальним стилем та відповідно превалюванням позитивного емоційного фону демонструють більш адаптивні показники структури психічної саморегуляції, що зумовлює їх успішність при вирішенні творчих навчальних завдань [1]. Відповідно можна

очікувати більш оптимальний перебіг пізнавальних процесів студентів на заняттях, під час яких вони перебувають в позитивному психоемоційному стані, що лежить в основі креативності та підвищення рівня їх творчої продуктивності.

Отже, природа творчої активності вимагає забезпечення внутрішньої розкутості та свободи суб'єкта навчально-пізнавальної діяльності, що під силу досягти тільки педагогу, у якого під час професійної діяльності превалюють позитивні емоційні стани: радість, натхнення, оптимізм, задоволення від спілкування зі студентами.

Список використаних джерел:

1. *Кузнєцова М. М. Оптимізм в структурі психічної саморегуляції навчальної діяльності студентів : дис. ... к-та психол. наук : 19.00.07 / Харківський національний педагогічний університет імені Г. С. Сковороди. Харків, 2018. 258 с.*

2. *Литвинчук Л. М. Стимуляція творчої активності суб'єктів освітнього простору як технологія забезпечення психологічного здоров'я. Вісник Національного університету оборони України. 2020. № 3(56). С. 70-75.*

3. *Матвійчук О. О., Краєва О. А. Проблема формування ідентичності в підлітковому віці у контексті розвитку творчої особистості. Вісник Національного університету оборони України. 2022. № 1(65). С. 64-71.*

4. *Санникова О. П. Эмоциональность в структуре личности. Одесса: Хорс, 1995. 334 с.*

5. *Fredrickson B. L., Branigan C. Positive emotions broaden the scope of attention and thought-action repertoires. Cognition and Emotion. 2005. № 19(3). P. 313-332.*

Зубченко Л. В.

кандидат педагогічних наук, доцент,
доцент кафедри спеціальних дисциплін та професійної підготовки
факультету №2 Криворізького навчально-наукового інституту
Донецького державного університету внутрішніх справ,
м. Кривий Ріг, Україна

МОЖЛИВОСТІ ВИКОРИСТАННЯ ФІТБОЛ-АЕРОБІКИ НА ЗАНЯТТЯХ З ФІЗИЧНОГО ВИХОВАННЯ В ДОНЕЦЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Збереження та зміцнення здоров’я студентської молоді є одним з найбільш важливих завдань сучасного суспільства, яке відіграє важливу роль у соціальноекономічному, політичному та культурному розвитку України. Однак, стан здоров'я молоді загрозливий. Обмеження спеціально організованої рухової активності є одним з провідних чинників зниження фізичної підготовленості молодих людей та резервів їх здоров'я.

Актуальною є проблема пошуку ефективних шляхів підвищення рухової активності студентів та поліпшення їхньої фізичної підготовленості за рахунок впровадження сучасних фізкультурно-оздоровчих технологій, які б сприяли розвитку позитивної мотивації до занять фізичним вихованням, формували основи самостійної оздоровчої діяльності [4, с. 19].

Система найважливіших завдань, які стоять перед вищою юридичною освітою – створення системи навчання та виховання, яка б забезпечила майбутнім фахівцям разом із практичною й теоретичною підготовкою за фахом міцне здоров’я та високу працездатність. Заняття фітбол-аеробікою значною мірою можуть допомогти у розв’язанні цієї проблеми.

Вплив фітбол-аеробіки на фізичний і психоемоційний стан студентів досліджували: Н. Базилевич, В. Завадич, С. Кузьміна, Н. Москаленко, Т. Овчинникова, А. Потапчук, О. Тонконог, Е. Сайкина, П. Самсонова та інші.

Фітбол-аеробіка - це один з напрямків аеробіки, де в якості основного снаряда для виконання вправ виступають еластичні м'ячі різної величини. Історія фітболу почалася в Швейцарії, де в 50-х роках минулого століття швейцарський лікар-фізіотерапевт Сьюзан Кляйнфогельбах запропонував виконувати вправи з м'ячем як реабілітаційна гімнастики для хворих на ДЦП. Основний інструмент фітбол-аеробіки - великий і легкий пружний м'яч, ще

званий фітболом. М'ячі мають розмір від 50 до 85 см і здатні витримувати вагу до 300 кг. Кругла форма даного гімнастичного снаряда дозволяє робити вправи з великою амплітудою, а нестійкість м'яча підтримує м'язи у постійному тонусі. Крім того, фітбол коштує набагато дешевше, ніж, наприклад, велотренажер, степпер або бігова доріжка, при цьому не поступається даним пристроям в ефективності [2, с. 36].

Сидіти на фітболі виходить тільки з випрямленою спиною, тому заняття футбол-аеробікою сприяють поліпшенню постави і надзвичайно корисні для хребта. Також треба відзначити, що постійні коливання м'яча стимулюють роботу внутрішніх органів і систем, включаючи шлунково-кишковий тракт, ендокринну та нервову системи, а його нестійкість змушує м'язи перебувати в постійній напрузі, щоб утримувати рівновагу.

Користь регулярних вправ з великим м'ячем багатогранна: по-перше, навантаження йде на усі групи м'язів; по-друге, здійснюється розвиток спритності, гнучкості та координації; по-третє, можливість виправлення неправильної постави, також ефективне спалювання калорій й як наслідок, стрункість фігури без використання складних тренажерів.

Для підвищення позитивної мотивації студенток до занять фізичним вихованням і з метою покращення їх фізичного стану, ми вирішили застосувати фітбол-аеробіку як один з ефективних засобів їх фізичного вдосконалення.

Дослідження проводилося на базі Донецького державного університету внутрішніх справ (м.Кривий Ріг). У дослідженнях взяла участь група студенток жіночої статі, яка була розподілена на дві підгрупи (експериментальну та контрольну) по 20 осіб в кожній. Контрольна група (КГ) займалася два рази на тиждень за традиційною програмою з фізичного виховання, а експериментальна (ЕГ) також два рази на тиждень за програмою, яка грунтувалася на заняттях з використанням вправ з фітбол-аеробіки. Дослідження проводилось впродовж I навчального семестру зі студентками I курсу віком 18–19 років.

Заняття фітбол-аеробікою ми починали зі звичайної розминки й закінчували повільною розтяжкою й дихальними вправами.

Вправи з використанням фітболв зовсім нескладні, вони включають різні варіанти кроків, випадів й підскоків на м ячі в комбінації з різними рухами та силовим навантаженням.

Ми дотримувались основних принципів оздоровчого тренування: – систематичність; – рівень навантаження має відповідати рівню підготовленості студентков у групі; – поступовість збільшення навантаження; – доступність для основної маси студенток; – перехід до

нових вправ лише після засвоєння попередніх; – індивідуальний підхід; – постійний візуальний контроль; – сприятливий емоційний фон; – дотримуватися правил техніки безпеки.

Також наголос робили на тому, що базове положення на заняттях – пряма спина, голова високо піднята, плечі розпрямлені, живіт і сідниці втягнуті. Заняття складалися з комплексу базових вправ фітбол-аеробіки. Починали завжди з загально-розвиваючих вправ, також вправ з на гнучкість і рівновагу, потім в основній частині заняття - вправи на м'язи рук; вправи на м'язи ніг; різноманітні комбінації вправ і комплексів фітбол-аеробіки; вправи на м'язи преса; вправи на м'язи спини; вправи на рівновагу; функціональні вправи. В заключній частині заняття використосували вправи дихальної гімнастики, на розслаблення м'язів. Обсяг засобів, їх зміст і різноманітність рухів підбирали в залежності від основної мети заняття і фізичної підготовленості студенток ЕГ.

В процесі занять фізичного виховання з використанням вправ фітбол-аеробіки ми приділяли увагу розвитку таких фізичних якостей: сили та витривалості, гнучкості, рівноваги й спритності. Ефективність запроваджених вправ полягала в тому, що, виконуючи їх, студенткам ЕГ доводилось постійно утримувати рівновагу, тому окрім гнучкості розвивалась і спритність, і стійкість, і координація, і навіть, загальна витривалість і сила м'язів всього тіла, а не певної однієї ланки тіла у момент утримання положення [1, 3].

В процесі проведення запропонованих занять, ми чітко слідкували за регулюванням фізичного навантаження як в процесі кожного окремого занятя, так і в системі навчальних занять протягом всього експерименту. Діяльність студенток на заняттях з фітбол-аеробіки організовувалась з допомогою таких форм:

– фронтальна (усі водночас виконують вправи);

– індивідуальна (самостійне виконання завдання під керівництвом викладача);

– коловий спосіб (виконання вправ почергово на «станціях» з різною цільовою спрямованістю в складі невеликої групи) [3, 4].

Треба відмітити, що ще одним потужним мотиваційним засобом був музичний супровід занять зі студентками в ЕГ.

При підборі музичного супроводу керувались принципами, що надавали можливість ефективно використовувати музику: урахування психовікових особливостей студентської молоді, характер рухів, що виконуються, художньо-естетичні вимоги до якості звучання музичного твору, відсутність одноманітності музичних творів [4, с. 21].

Отже, заняття фітбол-аеробікою – це один із сучасних напрямів фізкультурно-оздоровчих технологій з використанням еластичних м’ячів. Вправи з використанням фітболів несуть комплексну користь: зміцнюється прес, відмінно формується постава й зміцнюють м’язи хребта, розвивається координація. зникає жир з живота і інших частин тіла, в роботу включаються ті групи м'язів, які зазвичай не задіяні.

Список використаних джерел:

1. *Базилевич Н. О., Тонконог О. С., Божко С. А. Організаційно-методичні особливості занять фітбол-аеробікою у фізичному вихованні студенток. Wielokierunkowosc Jako Gwarancja Postępu Naukowego: kolekcja prac naukowych «ΛΌГОΣ» z materiałami Międzynarodowej naukowo-praktycznej konferencji (T. 2), 21 lutego 2020 r. – Warszawa : Europejska platforma naukowa, 2020. P. 107-113.*

2. *Боляк Н. Л. Історія розвитку оздоровчої аеробіки. Теорія і методика фізичного виховання. Київ, 2006. № 5. С. 36-38.*

3. *Глоба Г. В. Актуальні аспекти застосування комбінованої аеробіки в процесі занять з фізичної культури учнів основної школи. Педагогіка, психологія та медико-біологічні проблеми фізичного виховання і спорту. Харків, 2011. № 3. С. 30–34.*

4. *Гружевський В. О. Доцільність використання інноваційних технологій у формуванні особистісно-орієнтованої мотивації студентів до фізичного виховання. Педагогіка, психологія та медико-біологічні проблеми фізичного виховання і спорту. Харків, 2014. № 3. С. 19–24.*

ЕКОНОМІКА

Ромнов А. И.

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

ПРОБЛЕМЫ И ВОЗМОЖНОСТИ, СВЯЗАННЫЕ С ВНЕДРЕНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН В ЛОГИСТИКЕ И ТРАНСПОРТЕ

Развитие различных отраслей экономики невозможно представить без своевременного внедрения новых технологий, позволяющих более эффективно использовать имеющиеся ресурсы, осуществлять контроль и планирование. Так в транспортной логистике, охватывающей большинство аспектов транспорта, складирования и управления запасами, практическое внедрение современных инструментов способных повысить эффективность цепочек поставок является одной из главных задач. А набирающая популярность в последние годы технология блокчейн способна привнести новые возможности в данную сферу.

«Блокчейн может преобразовать цепочки поставок, создавая более эффективные и прозрачные системы, которые снижают затраты, повышают прозрачность и улучшают отслеживаемость. Обеспечивая безопасный и прозрачный обмен информацией в цепочке поставок, блокчейн может помочь предотвратить мошенничество, ошибки и задержки, а также укреплять доверие и сотрудничество между участниками.» [1, с. 195]

Возможно выделить следующие преимущества внедрения данной технологии в сферу логистики и транспорта:

1) Повышенная прозрачность. Технология блокчейн обеспечивает прозрачную и неизменную запись транзакций, к которой могут получить доступ все участники цепочки поставок. Это позволяет в режиме реального времени отслеживать движение товаров и материалов, обеспечивая высокий уровень прозрачности. Повышение прозрачности может помочь повысить эффективность и надежность цепочки поставок, снизить риск мошенничества и повысить доверие клиентов и партнеров.

2) Улучшенная отслеживаемость. Технология блокчейн может помочь улучшить отслеживаемость в цепочке поставок, обеспечивая защищенную от несанкционированного доступа запись о перемещении товаров и материалов. Это может помочь улучшить контроль качества и снизить риск подделки и мошенничества. Технология блокчейна также может помочь повысить

точность соответствия продукции требованиям клиента и способствовать целевой обратной связи, уменьшая нагрузку на потребителей и сводя к минимуму затраты для компании.

3) Повышение эффективности. Технология блокчейн может помочь повысить эффективность цепочки поставок за счет автоматизации ручных процессов и сокращения потребности в посредниках. Смарт-контракты можно использовать для автоматизации транзакций, сокращая время и затраты, связанные с ручной обработкой. Это может помочь сократить расходы и повысить скорость транзакций, что приведет к повышению эффективности.

4) Улучшенная безопасность. Технология блокчейн часто рекламируется за ее функции безопасности, включая использование криптографии для защиты транзакций. Это может помочь снизить риск мошенничества и кибератак в цепочке поставок. «Технология блокчейн также может помочь обеспечить конфиденциальность данных, поскольку конфиденциальная информация зашифрована и доступна только авторизованным сторонам.» [2, с. 74]

5) Улучшение сотрудничества. Технология блокчейн может помочь улучшить сотрудничество в цепочке поставок, предоставляя общую платформу для обмена информацией. Это может помочь уменьшить потребность в посредниках и повысить скорость и точность транзакций. Все участники цепочки поставок могут получать доступ к одним и тем же данным в режиме реального времени, что снижает риск ошибок и задержек.

6) Повышение доверия. Технология блокчейн может помочь повысить доверие к цепочке поставок, обеспечивая прозрачную и неизменную запись транзакций. Это может помочь снизить риск возникновения споров и повысить доверие клиентов и партнеров. «Технология блокчейн также может помочь обеспечить соблюдение правил и стандартов, снижая риск штрафных санкций за несоблюдение.» [2, с. 24]

Также вместе с возможностями, которые открывает внедрение технологии блокчейн в логистике и транспорте, существует и ряд проблем. А именно:

1) Технические проблемы. Технология блокчейн сложна, и может быть сложно настроить, развернуть и поддерживать сети блокчейна. Одной из главных технических проблем является масштабируемость. По мере роста числа участников сети блокчейн увеличивается объем хранимых и обрабатываемых данных. Это может привести к увеличению времени обработки транзакций, высоким комиссиям и повышенному

энергопотреблению. Другие технические проблемы включают совместимость, конфиденциальность данных и управление данными.

2) Проблемы интеграции. Интеграция технологии блокчейн с существующими системами и процессами может быть сложной задачей. Одной из основных проблем интеграции является отсутствие стандартизации в индустрии блокчейнов. Различные сети и платформы блокчейнов используют разные протоколы и форматы данных, что может затруднить их интеграцию с устаревшими системами. Это может привести к дополнительным затратам и задержкам в процессе внедрения.

3) Проблемы интероперабельности. Интероперабельность относится к способности различных сетей блокчейнов взаимодействовать друг с другом. По мнению исследователей Мехди Мохаммади и Ашкан Халили, между различными блокчейн-сетями и платформами отсутствует функциональная совместимость, что может затруднить обмен информацией и эффективное сотрудничество. [3] Это может ограничить потенциальные преимущества технологии блокчейн в логистике и транспорте.

4) Проблемы регулирования. Неопределенность регулирования в локальном законодательстве различных стран является препятствием для внедрения технологии блокчейн в логистике и транспорте. В настоящее время отсутствуют некоторые ньюансы в отношении правил и стандартов для технологии блокчейн. Это может затруднить для компаний инвестирование в технологию блокчейн и может привести к отсутствию доверия к технологии. Кроме того, некоторые нормативно-правовые базы традиционного сектора электронных коммуникаций могут быть несовместимы с технологией блокчейн, что может ограничивать скорость ее внедрения.

5) Проблемы безопасности. Технология блокчейн часто рекламируется за ее безопасность, но с ее реализацией все еще связаны проблемы безопасности. Одной из основных проблем безопасности является управление закрытыми ключами. Закрытые ключи используются для доступа к учетным записям и кошелькам блокчейна, и в случае их утери или кражи доступ к учетной записи блокчейна может быть потерян навсегда. Кроме того, смарт-контракты могут быть уязвимы для взлома и других типов атак, которые могут поставить под угрозу безопасность сети блокчейн.

На сегодняшний день законодательство Европейского Союза позволяет компаниям, внедряющим технологию блокчейн в логистике и транспорте работать полностью в правовом поле. Предприятия должны соблюдать ряд нормативно-правовых актов, касающихся защиты данных, платежных услуг, финансовых рынков, электронных коммуникаций и интеллектуальной

собственности. Таких как, например, GDPR, который регулирует обработку персональных данных в ЕС, в том числе данных, обрабатываемых с использованием технологии блокчейн. Компании, внедряющие технологию блокчейн в логистике и транспорте, должны соблюдать требования GDPR, такие как получение согласия на обработку данных и обеспечение прав субъекта данных. Для компаний важно знать об этих правилах и обеспечивать их соблюдение, чтобы избежать юридических и финансовых рисков.

Список использованных источников:

1. *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.*
2. *Kevin Werbach. The Blockchain and the New Architecture of Trust. Massachusetts: The MIT Press, 2018. 344 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.*
4. *The General Data Protection Regulation (GDPR). European Parliament, the Council of the European Union, and the European Commission, 2016.*

ФІЛОСОФІЯ

Герасимова Е. М.

професор кафедри філософії і соціальної антропології імені професора І.П. Стогнія Університету Григорія Сковороди в Переяславі

ГЕНДЕРНА ПРОБЛЕМАТИКА ВІТЧИЗНЯНОГО ОСВІТНЬОГО ПРОСТОРУ: ДІЯЛЬНІСНИЙ ПІДХІД

В умовах військових дій на території нашої держави відбувається процес формування нових реалій суспільного життя, де кардинально змінюється значення всього науково-освітнього потенціалу, а також особливої гостроти набуває проблематика глибинного осмислення концепту гендерної рівності. Мова йде про те, що знання існують незалежно від просторових особливостей, більше того, вони можуть знаходитися у багатьох місцях водночас. Відповідно результати діяльності людини в освітній сфері позбавлені не тільки просторових або адміністративно-правових меж, а також й гендерних відмінностей. Сучасна модель освіти є результатом складної соціальної еволюції суспільства та системних метаморфоз у порівнянні з історичними формами організації трансляції знань на суспільному рівні. Сьогодні процеси глобалізації у сучасному світі призвели до появи нових форм дискурсивних практик, які забезпечують цивілізаційний поступ суспільства за допомогою трансляції знань, цінностей, норм культури та досвіду. Крім того, сьогодні ми констатуємо появу нової якості стосунків між чоловіком та жінкою, які породжують неординарні ситуації у процесі постійної як професійної взаємодії, так і в побуті. Ідея рівності у стосунках між чоловіком і жінкою стає абсолютно прийнятною у більшості країн світу, причому визначається дієва необхідність доведення її до реального партнерства у соціальному житті. Тим більше, що всі плідні тенденції у сучасному світі характеризуються спрямованістю людства до комунікативної відкритості, діалогічності, толерантності як найважливіших людських цінностей, що долають відчуження та екзистенційну самотність. Історія на зламі тисячоліть вчить, що зазначені потенціали повинні об’єднатися, причому не просто механічним шляхом, а на засадах творчої взаємодії та самовдосконалення: «любовь-цілісність об’єднує чоловіка і жінку у гармонійній комунікації метабуття, суттю якої є взаємовідкриття, натхнення і співтворчість. Це зумовлює широке розгортання потенціалу

чоловіка і жінки як в родинному колі, так і в просторі мегаполісу, співтворцями якого вони стають» [1, с. 308].

В історії філософської думки першою найбільш завершеною гендерною концепцією є теорія Платона про те, що стать з'явилась у результаті трагічного розриву андрогінної цілісності. Заздрість богів призводить до руйнації такої цілісності та появи статі, тому тільки через любов між чоловіком і жінкою, на думку Платона, можна подолати відчуженість людського буття. На основі ідей персоналізму М. Бердяєв розвиває міркування Платона, визначаючи ідею андрогінізму центральною у філософії статі. Процес подолання статевої розірваності Бердяєв вбачає в подоланні статі завдяки ствердженню нової цілісної індивідуальності, надалі відбувається процес з'єднання з іншою цілісною індивідуальністю через любов-андрогінізм. Принципово іншу позицію зустрічаємо у О. Вейнінгера, який є одним з небагатьох філософів, які свідомо постулюють позицію зневаги до жіночого начала. Якщо ця зневага у більшості мислителів патріархальної доби існує на підсвідомому та контекстуальному рівні (наприклад, у З. Фрейда та його школи), то у текстах Вейнінгера вона виривається на поверхню. Він послідовно постулює тезу про те, що жіноче є вторинним по відношенню до чоловічого начала, так як у західній культурі з моменту ствердження патріархату жіноче та чоловіче стали порівнювати як матерію та дух.

Відповіддю патріархальним поглядам на стать формуються феміністичні ідеї. У феміністичних теоріях відбувається спроба надати жінкам рівні права з чоловіком. Наприклад, у працях американського антрополога і психолога К. Гілліган доводиться положення про те, що особистісний розвиток жінки визначається усвідомленням значущості взаємодії між людьми, а тому головна проблема жінки – це збереження відносин між людьми. До патріархального і феміністичного направлень сьогодні додається андрогін-аналітичний підхід, автором якого є Хамітов Н. Сутність андрогін-аналітичного підходу полягає у визнанні не лише рівноправності чоловічого та жіночого начал, а й необхідності їх партнерської взаємодії на психологічному, соціальному та екзистенційному рівнях. В андрогін-аналізі ключовим стає концепт екзистенційного андрогінізму, який описує динамічну цілісність людської особистості та відносин між такими особистостями завдяки гармонійному зростанню як чоловічого, так і жіночого начал людського буття. Міркуючи з мета антропологічних позицій над проблемою поза-тілесних виявів статі, Хамітов Н. вважає: «екзистенційним проявом чоловічого духовне начало - здатність до творчості, виходу за свої межі, самотрансцендування, а екзистенційним

проявом жіночого називає душевне начало - здатність до любові та співчуття» [3, с. 225-228], - на відміну від О. Вейнінгера, який ототожнює жіноче начало з матеріальним та буденним.

Погоджуючись з позицією, що гендерна проблематика діяльнісного підходу в освітньому просторі займає унікальне положення в системі гуманітарного знання звертається увага на такі загальнотеоретичні роботи зарубіжних і вітчизняних науковців, як М. Бубер, А. Камю, Н. Луман, Н. Маркузе, Е. Муньє, П. Рікер, З. Фрейд, П. Тейяр де Шарден, А. Швейцер, К.-Г. Юнг та ін. Започатковується розгляд теоретико-методологічних засад сучасного вітчизняного простору освіти, у тому числі дослідження гендерних ресурсних можливостей в роботах таких українських філософів як Н. Доній, О. Зайченко, М. Препотенська, О. Рубан, Л. Тілеженко, Т. Троїцька та ін.

Отже, звертаючись до патріархального, феміністичного та андрогін-аналітичного підходів у вирішенні гендерної проблематики, можемо стверджувати, що головною сьогодні стає ідея трьох екзистенційних вимірів людського буття, яка відкриває нові обрії для осягнення гармонічної взаємодії чоловічого та жіночого начала, а також осмислення деструктивних позицій в їх стосунках. Як бачимо, подолати розірваність і роздільність людини можна завдяки аналізу особливостей внутрішнього світу чоловіка і жінки, а також процесу створення внутрішньої цілісності та знаходження своєї любові.

Визначаючи найважливіші особливості чоловіка та жінки, ми звернемося до тези про те, що окрім біологічної статі, кожна людина має й соціальну стать, яка формується під впливом виховання у сім'ї та завдяки існуючому оточенню. Останнім часом, переважно у феміністичній літературі, найчастіше говориться про гендер як соціальний вимір статі, зміст його складається із соціальних стереотипів щодо ролей чоловіка або жінки. Біологічну і соціальну стать у процесі їх поєднання можемо охарактеризувати як зовнішню стать, причому вона не обирається людиною - це якби її припис. Натомість психологічний, а тим більше екзистенційний виміри статі завжди є результатом вільного вибору особистості за межами буденного буття людини. Психологічну та екзистенційну стать можна умовно назвати внутрішньою статтю або внутрішнім виміром статі. У тій мірі, в якій буття чоловіка та жінки є людським буттям, його визначає саме внутрішня стать.

У контексті сьогодення надзвичайно актуальним є звернення до гендерних стратегій освіти, які передусім реалізуються через особистість викладача. Найбільш розповсюдженою залишається маскулінна або

патріархальна стратегія особистості викладача, який застосовує субординацію в навчальному процесі. Дійсно, субординація в освіті є необхідною умовою ефективного процесу навчання, але недостатньою, а також, виходячи за певну межу, така стратегія побудови стосунків призводить до панування авторитарності та відношення до іншого як до об'єкту. З іншого боку, останнім часом все більше поширюється координатна освітня стратегія, яку в контексті нашого дослідження можна було б назвати фемінно-координативною. Вона має таки позитивні риси як гнучкість, терпимість, поблажливість, але паралельно часто спостерігається відсутність стратегічного підходу, системності та визначеної структурності. Протягом останніх років досліджуються теоретико-методологічні можливості процесу конвергенції позитивних рис маскулінно-субординативного та фемінно-координативного підходів в освіті. У результаті таких міркувань було запропоновано андрогінно-цілісну або гуманістичну стратегію. Вона передбачає вихід за межі монологічного характеру навчального процесу у площину співтворчого діалогу зі студентами, аспірантами, учнями. Проте така стратегія освіти може бути плідною та конструктивною, за умови синтезу маскулінно-субординативного і фемінно-координативного підходів, який відбувається не лише у навчальному процесі, а й у життєвому світі особистості.

Значною мірою сьогодні можна стверджувати, що андрогенною особистістю є така людина, яка здатна сприймати любов як самотворення і творення стосунків з Іншим: «Якщо ти любиш себе, ти любиш усякого іншого також, як себе. Поки ти любиш іншого менше, ніж себе, тобі не вдасться любити себе як треба; але якщо ти любиш всіх однаково, і себе також, то ти любитимеш їх як єдиного, і цей єдиний є і Бог, і людина. Отже, великий та праведний той, хто люблячи себе, любить також й усіх інших» [2, с. 143]. Любов до себе надає можливість кожній людині зрозуміти, що окрім тілесності, вона також має духовне і душевне начала, які у поєднанні складають особистість. Саме такий процес взаємодії зазначених начал особистості створює екзистенційне підґрунтя толерантного ставлення до інших людей. Справжня любов і повага до себе дозволяє вихователю так само ставитися і до своїх учнів, і до колег.

Отже, можемо сформулювати декілька умовних гендерних стратегій, за допомогою яких забезпечується ефективний діяльнісний підхід в процесі функціонування сучасного освітнього простору. Дотепер найбільш розповсюдженою у застосуванні є маскулінно-субординативна стратегія, яка спрямована на підтримку чіткої субординації та монологічного характеру освітнього процесу. Домінантна присутність такого підходу може мати як

позитивний, так і негативний характер впливу на освітньо-науковий процес. Фемінно-координативний підхід так само може мати, як позитивні риси у вигляді забезпечення гнучкості і толерантності в освітньо-виховному процесі, так і негативний аспект за рахунок недостатньої системності та чітко визначеної структурності. Спроби поєднання позитивних моментів у зазначених діяльнісних підходах відбувається на гуманітарних освітніх засадах андрогінно-цілісної стратегії, де головною цінністю проголошується актуалізація цілісної особистості.

Список використаних джерел:

1. *Препотенська М. П. Homo urbanus: феномен людини мегаполісу: монографія. Дніпропетровськ: Вид. Середняк Т. К., 2014. 420 с.*

2. *Цит. по: Фромм Э. Искусство любить // Душа человека. М.: Изд-во политической литературы, 1992. 434 с.*

3. *Хамітов Н. Екзистенційний вимір статі // Людина в есенційних та екзистенційних вимірах. К., 2004. С. 225 - 227.*

Вихованець З. С.

доцент кафедри іноземних мов з
курсом латинської мови та медичної термінології
Вінницького національного медичного університету ім. М. І. Пирогова

КОНЦЕПТУАЛІЗАЦІЯ ЦІЛІСНОГО ЛЮДСЬКОГО БУТТЯ У ФІЛОСОФІЇ ТЕЇЗМУ

Еволюційний шлях перетворень, попри постійні революційні катаклізми та військові руйнування, сприяв збереженню традиційно прийнятих способів організації колективної взаємодії та консолідації українського суспільства на основі тисячолітнього потенціалу її духовних цінностей. У свою чергу, категорія «філософського теїзму» завжди носить характер філософської концептуалізації, яка здійснюється на засадах певної релігійно-національної традиції та має конкретний культурно-семантичний вимір. Звідси випливає ідея поєднання соціального та духовно-культурного проєктів формування життєдіяльності суспільства у філософії теїзму, а процес їх реалізації та спосіб органічного поєднання забезпечує механізм концептуалізації цілісного людського буття та соціального порядку. Феномен цілісного людського буття в конструкціях філософського теїзму уособлює собою унікальне поєднання ґрунтовних ідей християнської православної традиції та базових принципів європейської філософської думки. Європейська культурна традиція на будь-якому історичному етапі свого розвитку постійно ототожнювала релігію з теїзмом, визнаючи пізнавальні та нормативні можливості філософії. Результатом такого поєднання стає той факт, що філософський теїзм поступово набуває ознак легітимізації разом з процесом набуття християнською теологією наукового значення, тобто саме філософія починає виконувати функцію наукової рефлексії й саморефлексії у західній християнський теології.

Базовими для даного дослідження стали праці теоретико-методологічного рівня таких відомих українських філософів як Бичко І. В., Кримський С. Б., Нічик В. М., Попович М. В. та багато інших науковців. Безпосередніми першоджерелами при вирішенні зазначених в публікації проблем є твори Вишенського І., Грушевського С., Барановича Л., Гізеля І., Могили П., Прокоповича Ф., Куліша П. та роботи багатьох інших відомих українських мислителів різних історичних епох. Автори у багатьох випадках знаходять собі точку опори в християнсько-богословський та «книжницькій» традиції. Крім того, необхідно враховувати той факт, що багато класичних

соціологічних теорій XIX – початку XX ст. прогнозували зникнення релігії як самостійного інституту у сучасному суспільстві або значне падіння її впливу. Реальні події останніх десятиліть не підтвердив цього прогнозу, тому дане питання потребує додаткового спеціального дослідження.

Отже, саме філософський теїзм завдяки своїм формам існування забезпечує відтворення базових цінностей культурно-релігійного характеру.

У свою чергу, людина у концептуальних підходах філософського теїзму єдина в світі істота яка об'єднує собою тварну природу та буття Абсолюту. Ідея триєдиної структури людини у християнський теології набуває в системі соціальних відносин свого діяльнісно-практичного значення. Відбувається концептуалізація цілісного образу людини, в якому дух, як структурний компонент, виконує домінантну роль у таких побудовах. Ціннісно-символічний зміст філософського теїзму також проявляється і на лінгвістичному рівні, він дозволяє конструювати не лише терміни, а бере участь у формуванні категорій як такого способу поняттєвого узагальнення досвіду, який уможливлює опис світу загалом, водночас формуючи відчуття приналежності до такого способу бачення дійсності кожного члена групи, адже «категорії – це, головним чином, колективні уявлення» [3, с. 192]. Лише описаний за їх допомогою світ стає «своїм» світом відображаючи спосіб життя спільноти.

Водночас сформовані у межах філософського теїзму поняття стосуються і регламентації життя суспільства, перетворюючи його не в сукупність індивідів, що ситуативно проживають на певній території та пов'язані спільними інтересами, а закладає ціннісне підґрунтя співжиття. Такий підхід підтримує тезу про те, що релігія завершує оформлення розуміння взаємодії людини і світу, при цьому розділяючи світ як природне довкілля, так і комунікаційний світ між людьми. Т. Парсонс також визнає релігію базовим чинником, який закладає основні ціннісні орієнтації функціонування суспільства. З нашої точки зору, ціннісні конструкції філософського теїзму мають принципове значення у комунікаційних процесах різного роду суспільних перетворень: «символічних значень..., що формують людську поведінку» [2, с. 691], - тобто здійснюють вплив на систему дій у виборі певних альтернатив.

Людина у реальному житті не може завжди обирати максимально раціональний шлях досягнення певних цілей, вона діє під впливом емоцій, особистих можливостей та культурно-ціннісних мотивацій. Наприклад, можна зазначити декілька основних направлень суттєвого християнського впливу на національну специфіку соціально-економічного життя України: 1) християнство, на відміну від ісламу та іудаїзму не містить жорсткої

регламентації соціально-економічної діяльності, але впливає на визначення людиною її головних цілей і пріоритетів; 2) моральна система християнських міркувань обмежує використання таких способів досягнення блага як вбивство, шахрайство тощо; 3) християнські інститути історично могли виконувати роль самостійних економічних агентів тощо. Як бачимо, християнська релігія впливає на соціально-економічну сферу не тільки змістом свого віровчення, скільки самим фактом того, що навколо нього формуються стійкі ділові кола спілкування, які визнають християнські етичні норми.

Безперечно, мова не йде про те, що на шляху національного відродження України необхідно штучно поновлювати релігійну систему цінностей, йдеться про збереження глибинної системи цінностей українського народу, про підвалини духовної свідомості українського народу, які зберігалися протягом століть та передавалися від покоління до покоління. Навіть у XIX ст. Куліш П. підкреслював: «Заберіть у нашого українця його дідів та звичаї і нічого християнського в ньому не побачите. Українець - християнин доти, доки його діди і звичаї при ньому» [1, с. 343]. Важливими рисами української ментальності в світлі характеристик П. Куліша постають орієнтація на «вічну правду» та «простоту», тобто на національно організований та естетичний побут; пріоритет «святої волі», гуманності, всепрощення та громади; орієнтація на спільність і рівність, неприйняття соціальної несправедливості. Християнське вчення впливає на процес соціально-економічного пізнання і набуває при цьому значної варіативності внаслідок пристосування до конкретних умов людського буття. Воно здатне виступати у формі нібито санкціонованої Богом раціональної ідеї чи відкриття. Поширення християнсько-богословської схоластики вело до модифікації початкових уявлень про християнські засади соціокультурного життя, котрі не зникають, а зберігаються і видозмінюються дотепер.

Отже, формування такого ціннісного потенціалу має свої ментальні особливості та соціально-економічні умови розвитку того або іншого народу. У свою чергу, філософський теїзм має величезне культурологічне та соціальне значення, саме він завдяки диференційної сукупності своїх форм завжди здійснює функцію посередника між релігійними засадами та соціокультурним середовищем. Ідеї філософського теїзму завжди носять характер філософської концептуалізації, яка здійснюється на засадах певної релігійно-культурної традиції та має конкретний історико-семантичний вимір. Філософський теїзм завдяки можливостям формування ідеального бачення соціальної діяльності забезпечує процес унікального поєднання

духовного потенціалу християнської традиції та сучасної соціально-правової структури базових європейських цінностей для забезпечення принципово-стабільних засад функціонування соціального порядку. Європейське розуміння індивідуальної свободи набуває сьогодні якісно нової ознаки, яка проявляє себе у процесі постійного засвоєння морально-правових норм сумісного існування, що забезпечує практичне розуміння відмінностей між свободою і свавіллям. Запорукою сучасної самореалізації індивіда виступає наявність та можливості прояву його внутрішньої свободи, яка уособлює собою автономне буття особистості, що передбачає розумне ставлення людини до зовнішніх впливів і збереження себе як цілісності.

Список використаних джерел:

1. *Куліш П. Твори. У 2-х т. К. : Дніпро, 1989. Т. І. 482 с.*
2. *Парсонс Т. Понятие культуры и социальной системы // О социальных системах. М.: Академический проект, 2002. С. 687-692.*
3. *Хайек Ф. А. Общество свободных. Лондон, 1990. 204 с.*

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ПРИКЛАДКА ІНФОРМАТИКА

Dmytro Levkin

Candidate of Engineering Science, Associate Professor,
Associate Professor of the Department of Physics and Mathematics,
State Biotechnological University,
Kharkiv, Ukraine

Oksana Zhernovnykova

Doctor of pedagogical science, Professor,
Head of the Department of Mathematics,
H.S. Skovoroda Kharkiv National Pedagogical University,
Kharkiv, Ukraine

INFORMATION AND ANALYTICAL PROVISION OF MATERIAL PREPARATION FOR THE TECHNOLOGICAL PROCESS

The report presents mathematical models and computational methods for determining the quality of seed. It is expedient to apply the developed technique for mathematical modeling and optimization of material preparation for the technological process of seed preservation. From the considered and analyzed in detail results of publications [1, 2], it can be seen that the main parameters for the classification of crop seeds and weed seeds are geometric parameters, namely: thickness – A, width – B, length – L. Based on this statement, a mathematical model for assessing the quality of seeds was built.

Cereal seeds have the ratio of parameters:

$$A_1 < B_1 < L_1, \qquad (1)$$

buckwheat seeds (and those close to it) have the shape of a trihedral pyramid, and the dimensions:

$$A_2 < B_2 < L_2, \qquad (2)$$

legume seeds have the shape of an ellipsoid of revolution and their characteristic sizes are related as follows:

$$A_3 = B_3 < L_3, \qquad (3)$$

spherical seeds, for example, peas, have such parameters:

$$A_4 = B_4 = L_4, \qquad (4)$$

weed plant seeds:

$$A_5 < B_5 = L_5, \quad (5)$$

the seeds of some cultivated plants and weeds have a flat shape, and their size:

$$A_6 \le B_6 < L_6. \quad (6)$$

Having the characteristic geometric dimensions of the seeds, it is easy to determine other parameters. For example, the volume of seeds can be calculated from the following ratios:

$$V_1 = \frac{\pi}{6} A_1 B_1 L_1; \quad (7)$$

$$V_2 = \frac{A_2 B_2 L_2}{6}; \quad (8)$$

$$V_3 = \frac{\pi}{6} A_3^2 L_3; \quad (9)$$

$$V_4 = \frac{\pi}{6} B_4^3; \quad (10)$$

$$V_5 = \pi A_5 \left(\frac{L_5^2}{8} + \frac{B_5^2}{24} \right); \quad (11)$$

$$V_6 = A_6 B_6 L_6. \quad (12)$$

As for the area of the outer surface of the seeds, the ratio of volume to the area of the outer surface, sphericity and other characteristics, they are easy to calculate.

We write down the deviations of the optimized parameters from their reference values:

thickness:

$$|A - A'| \le \Delta a, \quad (13)$$

width:

$$|B - B'| \le \Delta b, \quad (14)$$

length:

$$|L - L'| \le \Delta L, \quad (15)$$

volume:

$$|V - V'| \le \Delta V, \quad (16)$$

outer surface area:

$$|F - F'| \le \Delta F, \quad (17)$$

grain sphericity:

$$|S - S'| \le \Delta S, \quad (18)$$

where A', B', L', V', F', S' – are the given reference values of the corresponding parameters;

$\Delta a, \Delta b, \Delta L, \Delta V, \Delta F, \Delta S$ – deviations of parameters from their reference values.

If in the system of constraints (13)–(18) minimization of deviations of the values of seed parameters from their reference values is achieved, then the seeds are counted among the number of grains that meet the necessary requirements.

Note that since the quality of the fixed amount of seeds is studied first of all, then on the object table in the field of view of the objective, the seeds should not touch or obscure each other. When optimizing, we formulate this constraint as follows. Let the seeds under study be closed objects N_i, including foreign bodies. The seeds to be tested are placed in a rectangular area Ω (field of view of the technical system for determining the quality of seeds). The seeds must not touch each other, which means that:

$$N_i \cap N_j = \varnothing \text{ at } i \neq j, \qquad (19)$$

where $i, j = 1, \ldots, K$.

Seeds must belong to the field of view Ω, that means:

$$\bigcup_{i=1}^{K} N_i \cap \Omega = \bigcup_{i=1}^{K} N_i. \qquad (20)$$

The seeds under study can be considered as a function of the image $B(x, y)$, which characterizes the division of brightness in the field of view of the system. Image $B(i, j)$ – is a collection of images of individual objects and background:

$$B(i, j) = H_i(i, j) + \ldots + H_s(i, j) + H_b(i, j), \qquad (21)$$

where s – number of seeds;

$H_e(i, j)$ – image of the e-th object;

$H_b(i, j)$ – background image.

Wherein:

$$H_e(i, j) = 0, \text{ if } (i, j) \notin N_e; \qquad (22)$$

$$H_b(i, j) = 0, \text{ if } (i, j) \notin \Omega_b, \qquad (23)$$

where $N_e \subset \Omega$ – area of the e-th object;

$\Omega_b \subset \Omega$ – background area;

$N_1 \cup \ldots N_s \cup \Omega_b = \Omega$ и $N_i \cap N_j = \varnothing$, if $i \neq j$.

Consequently, the image becomes discrete and it is possible to obtain information about the analyzed image and continue its further research. Let us note the results of publication [3], where some applied optimization problems of other complex systems are solved. The results of the research can be applied to solve

many applied problems of determining the quality of the source material before the implementation of technological and biotechnological processes, which will increase the accuracy of calculating and optimizing the parameters of complex systems.

References:

1. *Savchenko V., Synyavskiy O., & Nesvidomin A. (2022). Pre-sowing treatment of sunflower seeds in a magnetic field. 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek). Kharkiv. 1–5. doi: 10.1109/KhPIWeek57572.2022.9916403*

2. Dovbush O.S., Shpak D.V., Shpak T.M., & Melnichenko H.V. (2022). Influence of seed heterogeneity on sowing and yielding parametersof rice cultivars. Selectsiia i nassinnytstvo. 121. S. 15–20. DOI 10.30835/2413-7510.2022.260988

3. Levkin A., Abuselidze G., Berezhna N., Levkin D., Volkova T., & Kotko Y. (2022). The Quality Function in Determining the Effectiveness of Example Bioeconomics Tasks. Rural Sustainability Research. 48 (343). 91–102.

DOI 10.2478/plua-2022-0019

Курочка С. В.

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

БЕЗПЕЧНІСТЬ ТА ПРОБЛЕМИ ВИКОРИСТАННЯ ГОТОВИХ РІШЕНЬ ДЛЯ СИСТЕМ РОЗУМНОГО ДОМУ ТА ЇХНЄ ВИРІШЕННЯ

Розумний будинок включає величезну кількість IoT-пристроїв, що збирають і обробляють дані. Таким чином, в ручному або автоматичному режимі, ці установки надають користувачам деякі можливості контролю за житлом. У «розумному середовищі» пристрої періодично обмінюються даними по Мережі. Це відбувається безпосередньо від пристрою до пристрою, або через хмару.

Через те, що всі елементи ланцюжка мають доступ в Інтернет, це робить їх вразливими до атак ззовні і наражає на небезпеку не тільки інформацію користувача, але також його здоров'я. Все це змінює парадигму мислення, яка свідчить: «Мій дім – острівець безпеки» [3, с. 116]. Однак безпека - це 100% вимога для розумного будинку, хто б що не казав. Сьогодні до його складу можуть входити системи спостереження, системи моніторингу (зокрема здоров'я) та системи безпеки, до яких можна отримати віддалений доступ. Їх просто потрібно захищати від зловмисників.

Відповідальність за це повинні нести виробники цих гаджетів. Однак вони часто заявляють, що займатися подібними питаннями немає жодного сенсу.

Не можна виключати, що зі зростанням числа розумних пристроїв почне зростати і кількість зламів систем керування. Зловмисники, які отримали доступ до таких систем, можуть за допомогою електронного ключа відчинити двері або вікно, отримати доступ до банківських рахунків мешканців розумного будинку. Більше того, злочинці зможуть вручну спричинити збій медичних пристроїв.

Переглянувши проведення досліджень ринку інтелектуальних систем, з'ясувалось, що практично всі мають проблеми з безпекою.

Перша проблема – недостатньо надійна перевірка автентифікації [1, с. 36]. Незважаючи на те, що системи мали хмарні та мобільні інтерфейси, не потребували встановлення паролів належної довжини та складності. Крім того, після декількох безуспішних спроб ввести пароль ніяка із систем не блокувала обліковий запис. Це означає, що був відсутній банальний захист від перебору.

Друга проблема – пов’язана з конфіденційністю. Усі системи збирали будь-які види персональної інформації: імена, адреси, номери телефонів та кредитних карток [1, с. 36]. Дана проблема продукує небезпеку крадіжки облікових даних.

Зазначимо, що головною ознакою багатьох домашніх пристроїв із системою безпеки є застосовування відео. Переглядаючи його, ми застосовуємо багато різних інтерфейсів, і тому через це - конфіденційні дані теж під питанням викрадення.

Остання, третя проблема – під час передачі даних відсутнє шифрування. Хоча у всіх системах реалізовані механізми шифрування на транспортному рівні, такі як SSL/TLS, багато хмарних підключень залишаються вразливими для атак [1, с. 36]. Вкрай важливо: обмін між контролером і сервером має проходити в зашифрованому за допомогою ключа виді, для того щоб, забезпечити несанкціоноване втручання в роботу пристрою. Неефективною є передача даних для автентифікації у відкритому вигляді у випадку комп’ютерних систем.

Для вирішення цього компанії Google, Samsung Electronics, Silicon Labs та інші об'єдналися з метою розробити новий бездротовий мережевий стандарт спеціально для розумних будинків. Він отримав назву Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а основною його перевагою є безпека. Одночасно в мережі можуть бути до 250 пристроїв, які захищаються шифруванням рівня банківської системи [2].

Прозорість – це властивість Thread. Тобто, можна легко встановити що і з чим зв’язано, тому що користувачу видно всі підключені пристрої. Зараз вже є багато вирішень для Smart будинків: ZigBee і 6LowPAN, які з легкістю розпочнуть приймати запропонований стандарт без апаратних змін, але за однієї умови - оновити програмне забезпечення. З пристроїв, які вже підтримують Thread, варто відзначити термостати Nest.

Але щоразу на ринку з'являється все більше продуктів, які спілкуються на власній «мові». Виробники напевно з маркетингових питань не поспішають запроваджувати єдиний протокол і повну сумісність пристроїв від різних компаній за для того щоб не зменшувати свої прибутки. Але як знати, може саме Thread стане тим протоколом, який вирішить усі вищеописані проблеми.

Також для вирішення проблем з сумісністю пристроїв та повною кастомізацією можна використати власний сервер для управління системою розумного дому. В якості сервера можна використовувати Raspberry Pi для вирішення схожих задач або навіть відійти за межі. Зазначимо, що для багатьох завдань і навіть застосування в ролі концентратора (хаба) розумного

будинку, ідеально підходить Raspberry Pi, що дозволяє різним електричним пристроям та обладнанням взаємодіяти один з одним.

Зокрема, за підтримки Web Things Gateway для автоматизації апартаментів можна зробити сервер Raspberry Pi. Так як варіантів використання автоматизації в розумному будинку дуже багато, обмежена лише чисельністю електроприладів і мудруванням, то простіше, для порівняння, реалізувати відому систему для керування світлодіодним освітленням, як поодинокий випадок застосування цього мікрокомп'ютера в смарт-системах. Через використання програмного забезпечення з відкритим вихідним кодом OpenHAB, імовірне створення центру керування на Raspberry Pi з сенсорним екраном. Котрий буде взаємодіяти з 150-ма і більше різноманітними продуктами для Smart будинку та надавати інтерфейс для управління та планування завдань. Із сервером на Linux є більше можливостей, що значно розширює використання. Це перспектива запуску особистих серверів, які можна потім розробляти під свої потреби. Пристрої можна підключати як по безпровідній мережі, так і застосовуючись кабельні, що є перевагою. Використання кабельної передачі даних з протоколом Modbus дає широкі можливості для використання пристроїв, які можуть керувати великими струмами. Приміром, за допомогою протоколу Modbus RTU, застосовуючи 8-канальний модуль реле, кероване шиною RS485.

Дуже просте Реле Modbus RTU у використанні. Завдяки швидкому зв’язку, стабільності, надійності та безпеці це ідеальний вибір для промислових пристроїв управління з високими вимогами до зв'язку. При такому підключенні пристрою з сервером не буде можливості впливати на роботу методами створення безпровідних перешкод.

Список використаних джерел:

1. Овчиннік, С. О. Метод захисту інформаціїї «системи Розумний Дім» на базі нового протоколу обміну даних / С. О. Овчиннік; О. А. Лаптєв; А. Б. Гребенніков // Актуальні проблеми кібербезпеки. – К.: Державний університет телекомунікацій, навчально-науковий інститут захисту інформації, 2020. – С. 35-39.

2. Хабр. IoT: Вопросы безопасности умного дома [Електронний ресурс]: https://habr.com/ru/company/gsgroup/blog/394343/

3. Науково-технічна конференція «Проблеми розвитку глобальної системи зв’язку, навігації, спостереження та організації повітряного руху CNS/ATM» : 21-23 листопада 2016 р. / [редкол.: В. І. Чепіженко, С. М. Креденцар та ін.]. – К.: НАУ, 2016. – 124 с. - Кобець А. С. «Основні вимоги до безпеки системи розумний будинок» / А. С. Кобець; А. О. Пашко; Р. В. Ткаченко. – С. 116

4. Kaspersky. How safe are smart homes? [Електронний ресурс]: https://www.kaspersky.com/resource-center/threats/how-safe-is-your-smart-home

Трофименко О. В.

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

ОГЛЯД ПРОГРАМНИХ РІШЕНЬ ДЛЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Розвиток інформаційних технологій трансформує сферу управління інформаційною безпекою. Через поширення витоків даних і кібератак, організації шукають нові рішення для захисту своєї конфіденційної інформації. Рішення на основі ШІ (штучного інтелекту) набувають популярності, оскільки пропонують проактивний підхід до управління безпекою. Зокрема, він досліджуватиме як штучний інтелект може допомогти організаціям виявляти кібератаки та своєчасно реагувати на них, зменшувати вразливості та надавати повніше уявлення про їхній стан безпеки.

Метою статті є огляд наявних програмних рішень для управління інформаційною безпекою. Аналіз їх реальних спроможностей та доцільності використання.

Переваги використання ШІ. Однією з ключових переваг ШІ є його здатність виявляти загрози та реагувати на них у реальному часі. Алгоритми машинного навчання можуть аналізувати величезні обсяги даних і виявляти шаблони, які звичайні спеціалісти можуть пропустити [2, с. 289]. Це дозволяє організаціям швидко виявляти атаки та реагувати на них, зменшуючи шкоду, спричинену порушенням безпеки.

Ще однією перевагою рішень на основі ШІ є їх здатність автоматизувати рутинні завдання безпеки. Це дозволяє персоналу зосередитися на більш складних питаннях, таких як аналіз ризиків безпеки та розробка нових стратегій безпеки. Рішення на основі штучного інтелекту також можуть надати більш повне уявлення про безпеку організації [3, с. 112], дозволяючи командам безпеки виявляти вразливості та визначати пріоритети для їх усунення [4, с. 51].

Огляд наявних програмних рішень. Існує багато компаній, які пропонуюсь програмне забезпечення на основі ШІ для кібербезпеки. Ось декілька з них:

- *Cylance* – це компанія з кібербезпеки, яка використовує штучний інтелект для захисту APIs [1, с. 120] від передових загроз. Її технологія на основі штучного інтелекту може виявляти та запобігати зловмисному

програмному забезпеченню та іншим атакам до того, як вони завдадуть шкоди. Ключовою відмінністю Cylance є використання алгоритмів машинного навчання для прогнозування майбутніх загроз, що дозволяє йому випереджати нові та нові загрози.

- *Vectra AI* – компанія з кібербезпеки, яка використовує ШІ та машинне навчання для запобігання кібератакам. Її платформа безпеки на основі штучного інтелекту може виявляти та запобігати загрозам у багатьох середовищах, включаючи хмару, мережу та кінцеву точку.
- *Palo Alto Networks* – компанія з кібербезпеки, яка використовує ШІ та машинне навчання для запобігання кібератакам. Ключовою відмінністю Palo Alto Networks є використання централізованої платформи керування, яка дозволяє організаціям керувати та контролювати стан безпеки з єдиного місця.
- *Darktrace* – провідна компанія з кібербезпеки, яка використовує ШІ для виявлення кіберзагроз і реагування на них у реальному часі. Її технологія штучного інтелекту розроблена для навчання та адаптації до середовища організації, що робить її ефективнішою у виявленні нових загроз і реагуванні на них. Ключовою відмінністю Darktrace є її зосередженість на неконтрольованому машинному навчанні, що дозволяє виявляти раніше невідомі загрози та реагувати на них.

Окрім наведених прикладів існує багато інших компаній (Tessian, SparkCognition, Anomali, Crowdstrike і десятки інших), що пропонують аналогічні рішення, і їх кількість, якість і надійність тільки зростає.

Розглянуто наявні програмні рішення, які використовують штучний інтелект для захисту від кібератак та інших загроз. Використання алгоритмів машинного навчання може допомогти виявляти та реагувати на атаки у реальному часі, зменшуючи шкоду, яку можуть спричинити порушення безпеки. Штучний інтелект також може автоматизувати рутинні завдання безпеки та надати більш повне уявлення про безпеку організації, що дозволяє командам безпеки виявляти вразливості та розробляти нові стратегії. Використання ШІ може бути корисним для організацій, які шукають нові рішення для захисту своєї конфіденційної інформації в сфері управління інформаційною безпекою.

Список використаних джерел:

1. Luis Weir. Enterprise API Management: Design and deliver valuable business APIs. London: Packt Publishing Ltd, 2019. 270 c.

2. Alessandro Parisi, Hands-On Artificial Intelligence for Cybersecurity. London: Packt Publishing Ltd, 2019, 307 c.

3. Leslie F. Sikos, AI in Cybersecurity. Cham: Springer International Publishing, 2018, 205 c.

4. Ishaani Priyadarshini, Rohit Sharma. Artificial Intelligence and Cybersecurity: Advances and Innovations. Chennai: CRC Press, 2022, 209 c.

Mykhailo Bentsa

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

GAP ANALYSIS: IDENTIFYING CURRENT SECURITY POSTURE AND AREAS FOR IMPROVEMENT

ISO 27001 certification requires a significant investment of time, resources, and effort. The preparation process involves several stages, including GAP analysis, documentation preparation, and implementation of controls. This section will discuss each of these stages in detail and provide practical tips and best practices for medium-sized IT companies.

The first step in preparing for ISO 27001 certification is to conduct a GAP analysis. A GAP analysis is a systematic review of the organization's current information security management practices, policies, and procedures, against the requirements of the ISO 27001 standard. The GAP analysis helps identify areas where the organization needs to improve and where it already complies with the standard's requirements.

To conduct a GAP analysis, the company should form a project team that includes representatives from all relevant departments, such as IT, finance, legal, and human resources. The team should review the ISO 27001 standard and compare it to the organization's current practices, policies, and procedures. The team should identify the areas where the organization falls short of the standard's requirements and develop an action plan to address these gaps.

Some practical tips for conducting a GAP analysis include:

- Use a checklist or template to facilitate the review process and ensure that all relevant areas are covered.
- Assign responsibility for each identified GAP to a specific team member and set deadlines for completion.
- Use a risk-based approach to prioritize the identified GAPs and focus on the most critical areas first.
- Involve senior management in the review process to ensure that they understand the importance of ISO 27001 certification and the organization's commitment to information security.

The next stage in preparing for ISO 27001 certification is to prepare the documentation required by the standard. The ISO 27001 standard requires a set of documents that define the organization's information security policies, procedures, and controls. The documentation serves as evidence of compliance with the

standard's requirements and provides a framework for implementing and maintaining an information security management system.

To prepare the documentation, the company should use a top-down approach, starting with the development of an information security policy. The policy should be aligned with the organization's overall objectives and values and should define the scope and objectives of the information security management system. The policy should also establish the roles and responsibilities of all relevant stakeholders, including senior management, employees, and external partners.

Once the information security policy is in place, the company should develop the supporting documentation, including procedures for risk assessment, asset management, access control, incident management, and others. The documentation should be reviewed and approved by senior management and should be easily accessible to all employees who need to use it.

Some practical tips for preparing documentation include:

- Use plain language and avoid technical jargon to ensure that the documents are easy to understand.
- Ensure that the documentation is consistent with the organization's actual practices and procedures.
- Use a version control system to track changes to the documents and ensure that the latest version is always available.
- Assign responsibility for maintaining the documentation to a specific team member and set regular review intervals to ensure that the documents remain up-to-date.

References:

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

2. *Naveed, T., & Hussain, M. (2017). A comprehensive review of ISO 27001 standard: Its strengths and weaknesses. International Journal of Advanced Computer Science and Applications, 8(3), 11-18.*

3. *Verma, A., & Jain, R. (2017). ISO 27001: A study on its implementation in organizations. Journal of Business and Management, 19(7), 66-73.*

Serhii Hrytsai

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

MIGRATE TO THE CLOUD: WHY, WHEN, STAGES

Why migrate to the cloud: Why migrate to the cloud if everything already works? Each organization answers this question in its own way, but there are global statistics collected by the Rackspace company as part of the report "The anatomy of cloud migration" [1]. According to the data, which was obtained on the basis of in-depth personal interviews with managers of hundreds of companies representing various sectors of the economy, the main motive for migrating to the cloud was to increase fault tolerance and/or the possibility of disaster recovery of IT infrastructures. More than 80% of respondents called these factors the most important. In third place is the stabilization of applications, which is important for more than 70% of companies, and only in the fourth position (a little less than 70%) is the reduction of IT costs. At this case, the business sees the cloud as a method of protecting its information assets from potential threats, while not forgetting about the optimization of investments. The second important point is that cloud solutions are becoming more and more widespread, and the migration to the cloud of at least part of the IT infrastructure will soon be inevitable for any enterprise. It can be private, public or hybrid, but still cloud. At some point sooner rather than later, you will have to modernize your IT systems, and new platforms are more dependent on cloud technologies. Therefore, it is necessary to prepare for migration today. At the same time, the cloud can still be a factor of competitive advantage and has economic benefit now, sooner the cloud becomes routine.

Stages of cloud migration. Then migration to the cloud is reduced to three simple stages: virtualization of physical resources, moving virtual machines to the cloud, data synchronization to account for changes that occurred during the migration. All these stages are largely automated today, thanks to advanced virtualization software platforms and the efforts of cloud operators who strive to make their services as convenient and customer-friendly as possible. And developers of application software, in any case, of new versions, often equip their products with their own tools for migration to the cloud - so before starting the migration, it is worth checking whether there is something similar in the software that your organization is preparing for transfer to the cloud. In general, after transferring the main version of the data to the cloud, a copy of the changes that

occurred during the migration is made on the client side. It is called "incremental backup", its volume is usually many times smaller than the main data array, and it can be transferred almost instantly over the network for full synchronization of changes (in some cases, this operation may need to be performed several times).

The main stages of migration to the cloud. The migration process can be carried out both in-house and with the help of specialists from a partner company for example a system integrator or the cloud operator itself. Each option has own advantages. Migrating yourself will provide a deeper understanding of the internal task and possibly some cost savings (although this is highly debatable). The involvement of an integrator is justified in the case when the cloud is part of a more general IT infrastructure, which this integrator created at the enterprise. This option will ensure closer interaction of all other systems. But the most common option for medium and large companies is a situation in which the migration to the cloud is carried out by the operator - in this case, it is easier to choose the optimal configuration, form the correct Service Level Agreement (SLA) requirements, adhere to all technical details, etc. In order for the migration to be successful, it is necessary to go through several stages. At this stage, let's call it "zero", it is necessary to collect and analyze the maximum available information on the topic of cloud technologies - about their types, options for use, areas of application, etc. It is also worth studying and comparing the offers of different cloud providers in order to understand, at least in general terms, exactly what functions may be needed and what is really worth paying for. It will not be superfluous to study the experience of cloud migrations of other companies. At the first technical stage, it is necessary to determine what exactly is planned to be transferred to the cloud (which servers, data, applications, services) and to form requirements for the cloud provider. Note that, although clouds are elastic, their capacity can be increased and decreased as needed. It is still worth immediately defining, at least in general terms, the main needs for computing power, the amount of disk resources and the speed of communication channels. The correct calculation will help to make the migration almost seamless. This stage is about money. Here you need to carefully calculate how much the migration to the cloud will cost and whether it will, taking into account all factors, be more profitable than maintaining your own equipment. The answer will not always be clear - the cloud is not a panacea. One of the stages of TCO assessment should be the inventory of own IT resources. It is quite likely that many of the outdated services and applications can be completely abandoned and, accordingly, you can save on the capacity of the rented cloud. Therefore, the question of the total cost of ownership should be given increased attention. Technologies allow you to implement a very wide set of possibilities, many can be adjusted, but the money spent cannot be returned. If only a part of the IT

infrastructure is transferred to the cloud, it is necessary to consider the question of how the new virtualized environment will interact with those applications and services that remained on local platforms.

Especially if we are talking about legacy software, that connecting it to the cloud infrastructure will require the creation of intermediate (not always free) software layers. The use of an external cloud imposes certain requirements in the field of ensuring information security, which differ from those that were sufficient in the conditions of the internal IT infrastructure. It is necessary not only to expand the perimeter of cyber security and protect external communication channels, but also to ensure the possibility of repelling DDoS attacks. All this can be solved today, but requires professional expertise. After all preliminary calculations and selection of a suitable provider, it is necessary not only to conclude a contract for the provision of services, but also to carefully familiarize yourself with its SLA. When getting acquainted with the terms of the SLA, it is worth paying attention to the degree of responsibility of the operator - for providers who are really confident in the reliability and fault tolerance of their infrastructure, it is at least six full monthly payments for the service. In the event of a failure due to the fault of the operator, the client will use the cloud for free for six months, or even a year. But, for the sake of fairness, we note that this does not happen in practice, because if a company promises such insurance, the degree of reliability of its infrastructure is measured by the number of nines. After theoretical preparation, you can start with practical questions. At this stage, the selection of software platforms for virtualization, between which the migration of resources (data, virtual machines, applications, services) will be carried out. Software tools are being selected to facilitate or automate this process. Network connectivity between the local site and the operator's cloud is ensured, stable and reliable data transmission channels are configured. Migration plan and schedule is drawn up, with a mandatory indication of the permissible downtime, making test migration. When everything is configured, checked and tested, you can start transferring productive systems and important data. By the way, if we are talking about very large volumes of data (from several tens of terabytes), sometimes it is better to move them physically - with the help of a special container equipped with protected and reliable drives. In this case, external communication channels will not be needed - all data and images of virtual machines can be overwritten on this mobile storage, and then physically transport this system to the operator's platform and deploy all the necessary infrastructure there, on the spot. It is imperative that an instruction is drawn up in case of unforeseen events, including specifying the emergency data recovery algorithm and virtual IT infrastructure. It is important to understand that migration to the cloud is not a goal - it is just one of the tools of "digital

transformation" of business, which is used to increase its efficiency. Therefore, at the first stages, it is necessary to predict how technical support, management and development of your virtual cloud platform will be carried out. To do this, it is necessary to immediately assign clear roles to all participants in the process, divide the areas of responsibility between the IT service and the specialists of the cloud operator, develop a plan ("road map") for the further development of the cloud infrastructure, and create detailed instructions for prompt response to sudden incidents. At the same time, the cloud is not a case where everything can be done once and forgotten forever. You can have done, but then the service user is deprived of the profit that regular optimization can bring. Fine-tuning and detailing the use of resources will allow you to save money and increase the reliability of the IT infrastructure. You can always go back to using the local infrastructure, migration can be done in any direction. This is also one of the important advantages of cloud technologies.

How long does it take to migrate to the cloud. Depends on how much data, applications, and services need to be transferred, as well as how critical they are to temporary ones. The stage of technical migration itself can take days or even hours (in the case of small infrastructures). But the time required for all stages of project preparation and evaluation is often calculated in months. Thus, according to the above-mentioned Rackspace study "The anatomy of cloud migration" [1], out of a hundred surveyed large companies, in almost every third case, the total time spent on all aspects related to the migration of IT infrastructure to the cloud was up to three months. About a third of the respondents reported that the complete "relocation" took them from 3 to 6 months. But in some cases, the project was delayed for a year, two or even more.

Data above suggest that, if we are dealing with large and even medium-sized IT infrastructures, the migration to the cloud, carried out according to all the rules, will be a complex process that requires complex preparation, planning and time. The use of cloud technologies is a sustainable global trend. Sooner all companies will switch to working with cloud infrastructures. Some earlier, others later, but it is necessary to prepare for this process now. Technologies are developing rapidly, reliability and ease of use are increasing, and many functions are being automated. As a result, migrating to a cloud environment has become a much simpler and more understandable process.

References:

1. Rackspace technology The Anatomy of a Cloud Migration. https://www.rackspace.com/resources/anatomy-cloud-migration

Volodymyr Kovbasiuk

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

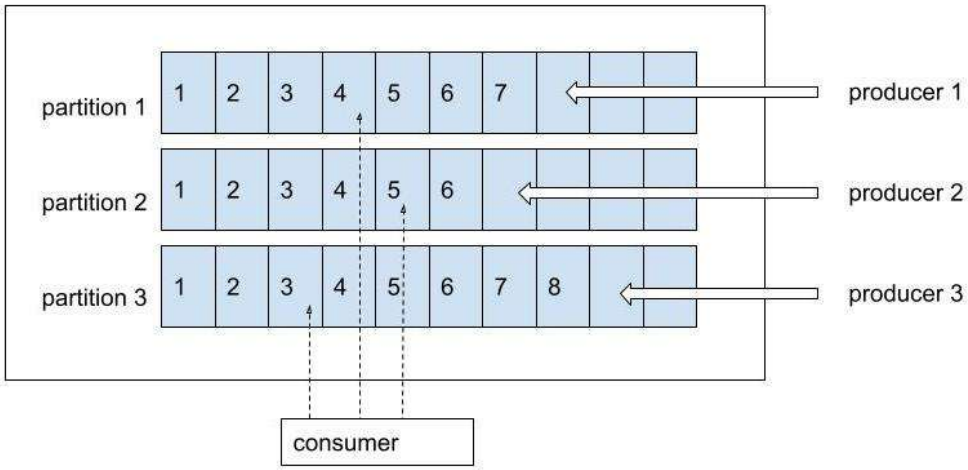
PRACTICAL ASPECTS OF PARALLEL DATA PROCESSING AT HIGH LOAD WITH APACHE KAFKA

Apache Kafka is a great tool for data steams processing. It provides high performance and scalability at distributed event streaming and is widely used for real time application, Big Data, monitoring etc.

These notes are not about Kafka basics but what particularities can be faced with when using Kafka for parallel data handling.

1. Short context intro

Data in Kafka are stored in so called topics with publishes – subscriber scenario, when publisher producer data to topic and subscriber read data from it. Topic is temporary, distributed data store where messages have fixed order defined by offset id. Offset id is sequence number of the message inside partition. Partitions are topic "data storage" that allows to split data into separate independent streams.

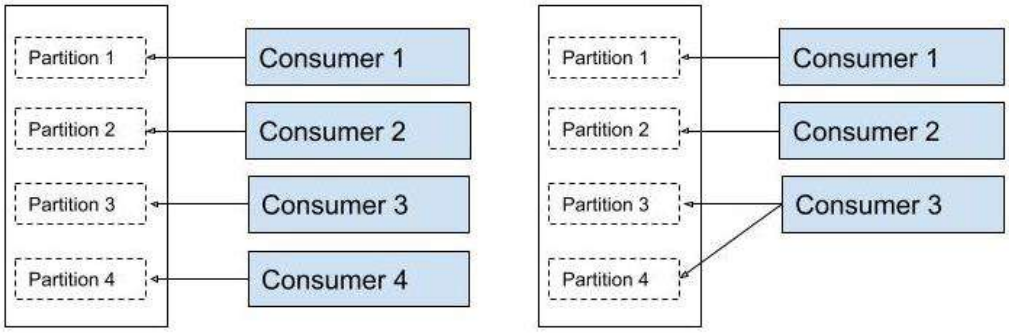


Topic structure example

2. Data splitting by partitions

Well known pattern of parallel data processing is splitting topic into several partitions and combining consumers into single consumer group so Kafka can evenly assign partitions per each consumer. This process is called a rebalance. The

rule is to make partition number that it will has max possible dividers. E.g., good example is topic with 18 partitions when consumers number can be 1/2/3/6/9/18. This brings some hardcoded conditions to have fixed number of consumers and scaling can only be done gradually by numbers above. It's still possible to add like 5 consumers to 18-th partitions topic but in this case three consumers will get 4 partitions each and rest two only 3 partitions each. For optimal performance it better to have same partitions number for each producer.



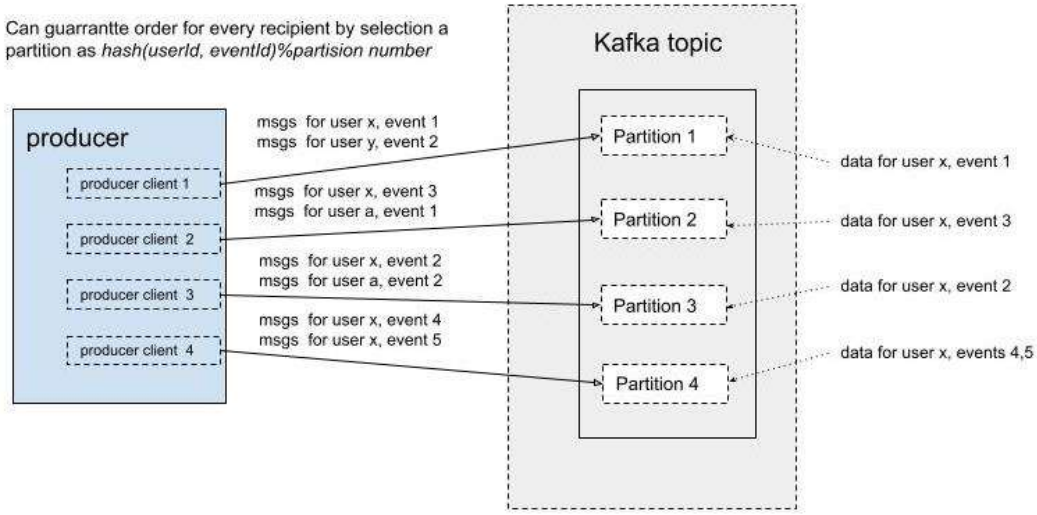
Optimal and non-optimal partitions assigning example

It can become challenging when additional requirement is to keep messages handle order for timeline consistence. Good example can be notification system where user gets sequential notifications about some events. Keeping order for pair userId and eventId is extremely important.

Adding performance requirement adds more complexity especially in case when one data source is single instance. Let's view some real use cases.

3. Producing from same instance with multiple Kafka clients

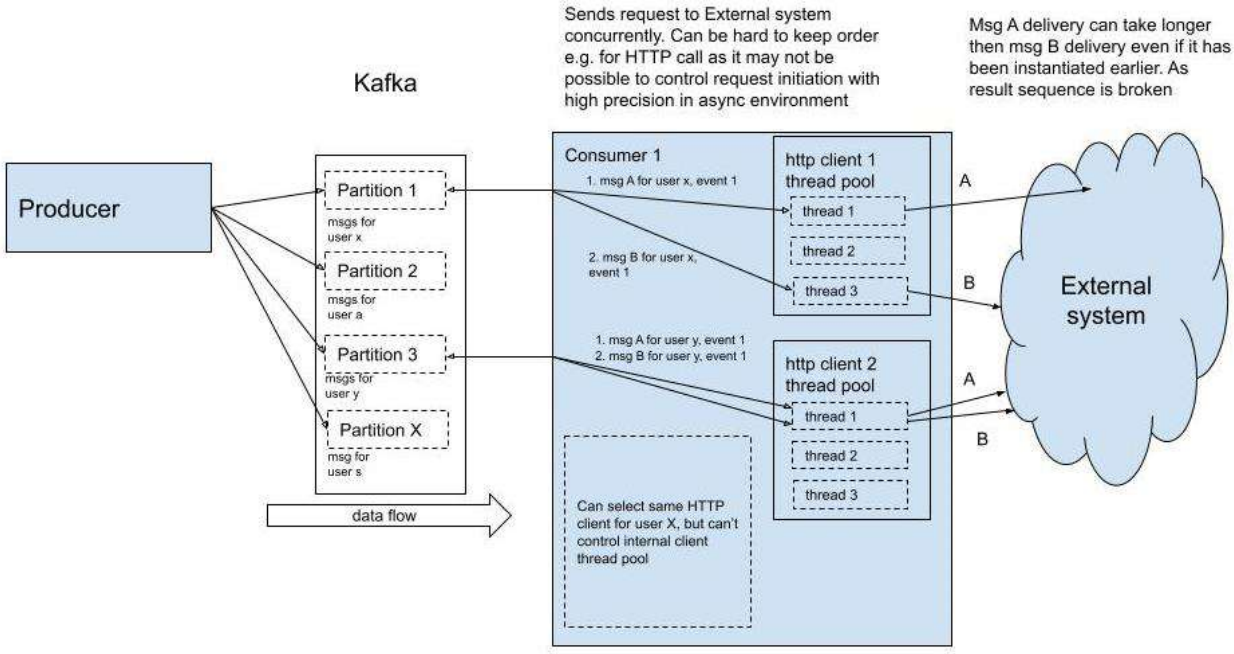
Two or more producer clients works faster than one. So, data can be written to Kafka faster. Then logical requirement is to select same producer for same user and same event. This can be done by calculation constant partition number for user and event pair. For example this can be division reminder of hash from concatenation of user an event id divided by number of partitions: hash(concat(userId, eventid))%partitionsNumber



Example of data distributions across partitions for user X

4. Order break at non fully controlled environment

It could be tricky to keep same sync at consumer side. If performance is a need and data are handled asynchronously order chain can be out of control sometimes:



Keeping handling order can be hard with external system interaction

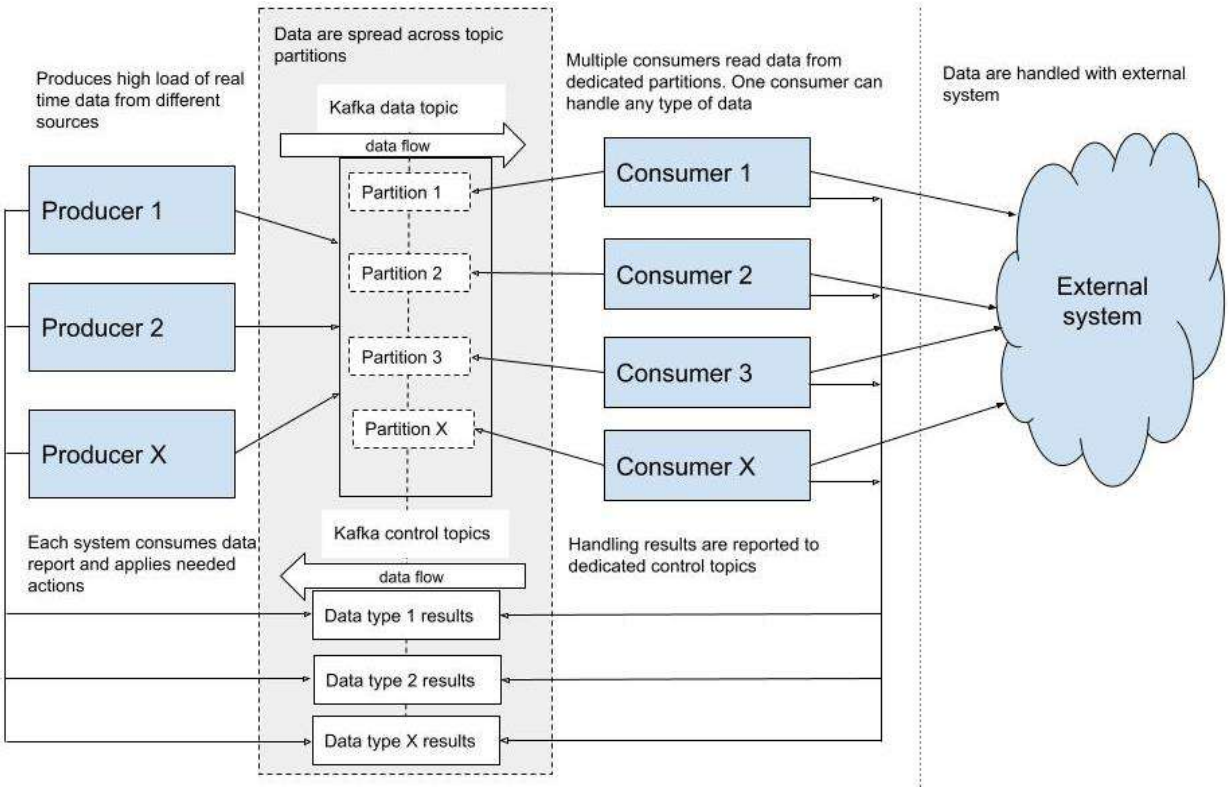
Example shows that user X can got message B before A even if they came to consumer in right sequence

5. Message size to keep performance but minimize risks

Other question is how much notifications can one Kafka message contains? It should be a compromise between max size of Kafka message, number of notifications one consumer can handle in single transaction and impact of message lose or receiving a duplicate. Kafka can provide different delivery guarantees - “at least once”, “at most once” and “exactly once”. Depending of this and producer/consumer stability it’s important to keep message size reasonable. Losing some info notification once per month can be acceptable, but for financial transaction it’s critical not to happen.

6. Back connection to track results

Splitting entities from single producer to multiple consumers allows to increase data throughput. The other side of this is isolation each consumer and no ability to analyze whole results and system performance at this consumer level. Fortunately, it can be easy handled by Kafka with providing dedicated topic for results reporting.



Data parallel processing and reporting results back in control topics

Each consumer knows how to handle data and how to select topic to report result. This can be just performance metrics or control message to adjust input

according to handle result. Multiple consumers write results for same data type into single topic. Producer from the other side read this control topic and can act accordingly.

The open question is how to aggregated results in high-load environment. For example, processing 10 million for messages by single consumer may produce just 1000 messages of aggregated control data to keep performance at high level.

These are just some basic points that everyone who involves Kafka into high load system can face. Kafka use so called “dumb server smart client” where clients (producer, consumer) is responsibe for correct faults handling and tracking data consistency. It offers great features, but complex use scenarios may not be easy to implement.

References:

1. *Kafka docs [https://kafka.apache.org/documentation/]*
2. *Exactly Once Processing in Kafka [https://www.baeldung.com/kafka-exactly-once]*
3. *Ways to balance your data across Apache Kafka® partitions [https://aiven.io/blog/balance-data-across-kafka-partitions]*
4. *Best practices and strategies for Kafka topic partitioning [https://newrelic.com/blog/best-practices/effective-strategies-kafka-topic-partitioning]*
5. *Why do we need partitions in Apache Kafka at all? [https://www.kadeck.com/blog/how-many-partitions-do-i-need-in-apache-kafka]*

Maksym Proniaiev

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

IMPACT OF TECHNOLOGIES ONTO THE FIELDS OF MANAGEMENT AND SALES. USES OF ARTIFICIAL INTELLIGENCE'S SUCH AS CHATGPT

Various technologies and their use in sales has become more and more important as customers demanded an experience which is more personalized and provides seamless shopping. According to a report by Salesforce [1], 84% of customers say that the thing that is as important as company's products and services is a customer experience the very same company provides.

Now, every interaction a customer has with a product or service, from browsing online to speaking with a customer service representative, requires businesses to pay increased attention.

The way businesses operate was revolutionized by Information Technologies (IT), which also has had a significant impact on sales.

IT itself is a broad field that includes, but not limited to, the use of computers, software, and other technologies. Word processing, data analysis, and communication are one of many functions perform by IT. Additionally, IT includes various networking and communication technologies that allow users to share information across different devices all around the globe.

Applied informatics is a subfield of IT that focuses on the practical application of technology to solve real-world problems. The goal of applied informatics is to use technology to improve processes, eliminate human factor and enhance decision-making.

Healthcare, finance, manufacturing, and logistics rely heaving on development and use of software, hardware, and other tools to solve field specific problems and achieve greater efficiency.

Applied informatics is used in management and sales in many ways. Sales professionals are increasingly using social media platforms to reach new potential customers. Social media platforms provide an excellent opportunity to engage with wide range of audience and promote products and services.

Additionally, data analytics and business intelligence are heavily invested in by different companies. Collecting and analyzing large amounts of data helps sales teams and managers in making informed decisions. Data analytics tools are

allowing management to clearly see trends and patterns in sales data and customer behavior. All of them helps management teams to tailor their sales strategies accordingly. Many other metrics also serve their purpose to help people make better decisions about how to allocate resources, improve customer engagement and target specific markets.

Customer relationship management software (CRM) is used in tracking customer interactions and relationships. For example, such system can provide sales teams with a detailed view of their customer's activity, including their buying history, preferences, and overall behavior. This information can help sales teams to adjust their approach to individual customers and provide a more personalized service.

By using automation tools, sales teams can save time and focus on high-value activities, such as building relationships with customers and closing deals. Lead generation, prospecting, and follow-ups are already automated by many businesses.

Another technology that is being used in sales is augmented reality (AR). AR provides an interactive experience that allows customers to see products in a new way. For example, IKEA uses AR to allow customers to visualize furniture in their homes before making a purchase. According to a report by Gartner [2], by 2022, 70% of enterprises will be experimenting with immersive technologies for consumer and enterprise use, and 25% will have deployed them to production.

Virtual assistants, such as chatbots, can help sales teams manage daily customer interactions or to delegate frequent inquiries. Chatbots can be programmed to answer sets of questions in a lively manner, freeing up sales teams to focus on more complex tasks. According to a report by Juniper Research [3], chatbots will save businesses over $8 billion per year by 2022 via providing a cost-effective way to handle customer support, answer queries, and manage transactions.

Such assistants allow to offer 24/7 customer service, which means that customers can get help and answers at any time of the day without real employee present. Chatbots are also providing a more personalized experience by using customer data to adjust responses to each individual. Many of chatbots are using natural language processing (NLP) and machine learning algorithms to understand customer preferences better and provide more personalized recommendations.

Chatbots popularity have been significantly increased in recent years, and businesses are exploring ways to integrate them into their sales operations. According to a report by MarketsandMarkets [4], the chatbot market is expected to grow from $2.6 billion in 2019 to $9.4 billion by 2024.

ChatGPT is a language model developed by OpenAI that can be used to develop chatbots for businesses. According to a report by Forbes, "Chatbots can greatly benefit from the most advanced NLP techniques such as GPT-3". [5] ChatGPT uses machine learning algorithms to understand natural language and provide accurate responses to customer queries. It can assist sales representatives by generating leads, answering routine queries, and identifying potential customers.

For example, Mastercard has developed a chatbot named KAI that uses ChatGPT to help small business owners with everyday tasks. KAI can help businesses with frequents time consuming tasks such as sending invoices, processing payments, and tracking expenses. This allows business owners to save time and focus on other aspects of their business.

ChatGPT can also be used in management assist managers in decision-making or to automate some of their tasks. According to a report by Deloitte [6], 57% of organizations are already using AI to automate tasks, and this number is expected to grow in the coming years. ChatGPT can be used for scheduling meetings and sending reminders, which can save managers time and increase efficiency.

Providing data-driven insights and analyzing business trends is other possible use of AI. For example, McKinsey & Company [7] developed a chatbot named Horst that uses ChatGPT to provide insights to managers. Horst can analyze business data and provide insights on topics such as employee productivity and customer behavior.

In conclusion, the use of technology in sales has become increasingly important as customers demand a more personalized and seamless shopping experience. Chatbots, augmented reality, and other technologies provide businesses with new ways to engage with customers and provide a better overall experience. ChatGPT is an example of a technology that can be used to automate routine tasks and assist sales representatives and managers in decision-making. As technology continues to advance, it is likely that we will see even more innovative ways that businesses can use technology to improve sales and management or to remain competitive by staying up to date.

References:

1. Salesforce. (2021). State of the Connected Customer. https://www.salesforce.com/content/dam/web/en_us/www/documents/white-papers/state-of-the-connected-customer-2nd-edition.pdf

2. Gartner. (2019). Top 10 Strategic Technology Trends for 2020: Immersive Experience. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/

3. Juniper Research. (2017). Chatbots: Retail, eCommerce, Banking & Healthcare 2017-2022. https://www.juniperresearch.com/document-library/white-papers/chatbots-retail-ecommerce-banking-healthcare

4. MarketsandMarkets. (2019). Chatbot Market by Component, Usage, Application, Deployment Channel, End User and Geography - Global Forecast to 2024. https://www.marketsandmarkets.com/Market-Reports/chatbot-market-61414111.html

5. Forbes. (2021). The Benefits of Using GPT-3 for Chatbots. https://www.forbes.com/sites/forbestechcouncil/2021/01/11/the-benefits-of-using-gpt-3-for-chatbots/?sh=7148318e1dc9

6. Deloitte. (2019). State of AI in the Enterprise, 2nd Edition. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/center-for-process-bionics-ai-enterprise.pdf

7. McKinsey & Company. (2021). Harnessing the power of chatbots for financial services. https://www.mckinsey.com/business-functions/risk/our-insights/harnessing-the-power-of-chatbots-for-financial-services#

Artur Stepashkin

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

VIRTUAL PRODUCTION IN FILMMAKING

This paper presents Virtual Production — a pivotal innovation that has irreversibly changed the production process. Virtual Production is a collaborative technique that combines the physical world of filmmaking (actors, sets, props) with the digital world (lighting, VFX) in a single process. It is gaining widespread attention granting digitally created content, which was traditionally done after filming, to the film set in real-time [10]. The broad term Virtual Production refers to an array of computer-aided production and visualization filmmaking approaches [5; p. 5].

Furthermore, the whole process is enabled by sophisticated Unreal Engine algorithms. Unreal Engine is globally the most transformative real-time 3D creation engine for creating photorealistic visuals and immersive experiences [12]. In general, game engines are the common name term for the tools that developers make use of to produce and manipulate the visuals, sounds, physics, and other aspects of a 3D production, whether in a game, film, or something less well defined like an augmented reality experience [4]. Unreal Engine 4 was extensively studied in a number of scientific publications. Unreal Engine 5 (UE5) is currently the most advanced and integrated engine. It combines high-end graphics and visual design with audio, lighting, animation, and other capabilities [4].

In addition, Unreal Engine can be partially considered a product of AI. Nowadays, it allows users to generate training data for machine learning models and other AI software [3]. Customers' projects can incorporate believable AI entities due to the systems available within Unreal Engine [11]. From now on, creatives are enabled to modify the sets in unprecedented ways, which contributed to the rising popularity of Virtual Production in filmmaking. As previously stated, Virtual Production combines physical and virtual filmmaking techniques to create cutting-edge media. During the process, teams use real-time 3D engines (game engines) to create photorealistic sets, then display them on large LED walls behind physical sets using the real-time rendering capabilities of the game engines. The camera is synchronized with the game engines to achieve enhanced realism and depth of perspective [6].

Moving Picture Company (MPC) expands this definition with more technical detail, "VP combines virtual and augmented reality with CGI and game-

engine technologies to enable production crews to see their scenes unfold as they are composed and captured on set" [5, p. 3]. The technique acquired vogue during the pandemic and played a crucial role in mitigating the corona-crisis in the film industry. When the world was suddenly halted to a full stop, and the film and advertising industry was frozen, Virtual Production studios emerged as a viable, cost-effective, and minimal intrusive option. Virtual Production technology has rapidly become very popular. Currently, it is used everywhere, from big-budget blockbusters to inexpensive commercial filming.

The most notable titles are *Lion King* and *Mandalorian*, while there are many more that have already benefited from the convenience and effectiveness of Virtual Production. There are currently 100 LED stage volumes worldwide, with another 150 on the horizon [10]. The big visual effects (VFX) industry players have instantly caught up with the technology. In particular, we can mention MPC, which worked on *Lion King* (2019), and Industrial Light & Magic (ILM), which worked on *Mandalorian* (2019 – present). They have their own Virtual Production LED-stage studios that can offer various exquisite services for affluent movie projects.

At the same time, small and medium production companies have emerged to cover a broader range of more humble productions that can benefit commercial filmmaking and small-budget movie-making. A few new names in the field, like British Quite Brilliant [7] and Dimension [1], have made Virtual Production their core business strategy.

Some independent project has also emerged. For instance, the Entertainment Technology Center at the University of Southern California has created a short film, "Ripple Effect," using Virtual Production to respond to the challenges of the COVID pandemic. It is an R&D test of educational value to explore the future potential of filmmaking in critical conditions [9].

This is now a mature field since the size of the worldwide Virtual Production market was estimated at USD 1.60 billion in 2021 and is expected to grow at a compound annual growth rate (CAGR) of 17.8% from 2022 to 2030. The increasing demand for visual effects (VFX) in movie production studios worldwide and the rising application of Virtual Production in commercial advertisements will likely improve market growth over the forecast period [13].

To conclude, the collaboration of high-quality visual graphics with a motion-captured imagery character in a three-dimensional environment has become highly popular recently, and the implications for the industry are immense. The significant players are opening additional virtual production divisions.

The smaller and medium companies are either diversifying their studios or investing heavily in expanding into the new lucrative technology. New players

have appeared in the field, encouraged by the potential use of this revolutionary technology. Virtual Production is gaining traction and is likely to influence market growth in the near future positively.

References:

1. *About Dimension. URL: dimensionstudio.*
2. *A list of academic publications that utilise the Unreal Engine. URL: ue4research.org.*
4. *AI and Machine Learning. URL: unrealcontainers.com.*
5. *Coldewey D. Why should you care about Unreal Engine 5? URL: techcrunch.com.*
6. *Kadner N. The Virtual Production: Field guide, 2019. 98 p. URL: unrealengine.com.pdf.*
7. *L'Italien R. What Is Virtual Production? URL: perforce.com.*
8. *Quite Brilliant is a new breed of production studio. URL: quitebrilliant.co.*
9. *Rao N. What is virtual production? URL: cgspectrum.com.*
10. *The ETC Virtual Production R&D Short Film 2020. URL: rippleeffectfilm.com.*
11. *Top 5 reasons to choose virtual production for filmmaking. URL: cgspectrum.com/blog.*
12. *Unreal Engine. URL: docs.unrealengine.com.*
13. *Unreal Engine. URL: unrealengine.com.*
14. *Virtual Production Market. URL: grandviewresearch.com.*

Roman Tsekov

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

THE ADVANTAGES OF MIGRATING THE THE PUBLIC ORGANIZATION EUROPEAN INSTITUTE FOR POSTGRADUATE EDUCATION WEBSITE AWAY FROM THE UCOZ WEBSITE BUILDER AND REDEVELOPING IT WITHOUT RELIANCE ON THE WEBSITE BUILDER JUSTIFY THE RESOURCES AND TIME INVESTED

The first point is that the ethical imperative to support Ukraine and uphold ethical principles justifies the decision to move the website away from the Ucoz Website Builder, which is a Russian platform, and choose a different platform, given the ongoing conflict with Russia.

As a Ukrainian public organization, the European Institute for Postgraduate Education has a responsibility to support the country and its values, including social responsibility and accountability. In the context of the ongoing conflict between Ukraine and Russia, it is crucial that the organization takes a stand and avoids supporting the aggressor nation.

Ucoz is a Russian website builder platform, and by using it, the European Institute for Postgraduate Education inadvertently supports the Russian economy and government. Given the ongoing conflict between Ukraine and Russia, it is essential for the organization to disassociate itself from any ties to Russia, especially given the severity of the conflict and the human rights violations that have been reported.

Moving the website away from the Ucoz Website Builder and choosing a different platform sends a clear message that the organization supports Ukraine and its ethical principles and is committed to upholding them. Additionally, the decision to switch to a different platform may lead to a more robust and reliable website with better features, design, and user experience.

Ultimately, the decision to move the website away from the Ucoz Website Builder should be viewed as a necessary step in supporting Ukraine and its ethical values in this time of conflict. By doing so, the organization demonstrates its commitment to social responsibility and upholding ethical values, which align with the core mission of the Institute.

Moreover, the move away from the Ucoz Website Builder could also have practical benefits for the European Institute for Postgraduate Education. By

switching to a different platform, the organization could have access to better website management tools and features, which could enhance the user experience for visitors and improve the overall functionality of the website.

Furthermore, choosing a platform that is not associated with the aggressor nation sends a strong message to the organization's stakeholders, partners, and clients that the European Institute for Postgraduate Education is committed to upholding ethical principles and is willing to take action to support its values. This move can also enhance the Institute's reputation and credibility as a responsible and ethical organization.

In conclusion, the decision to move the website away from the Ucoz Website Builder is a necessary step to uphold ethical principles, support Ukraine, and demonstrate the organization's commitment to social responsibility. Choosing a different platform can also have practical benefits, including access to better website management tools and features, and can enhance the Institute's reputation and credibility as an ethical organization

The second point is that in today's digital age, having a strong online presence is crucial for any organization or institution, and universities are no exception. A university blog serves as an essential tool to disseminate information about campus events, academic programs, student achievements, and research activities to a broader audience. However, the choice of the website builder platform can impact the blog's functionality, user experience, and search engine optimization (SEO).

The Ucoz website builder is a popular choice for creating websites and blogs, including those of educational institutions. While it offers several templates and features, the limitations of the platform can hinder the blog's growth and reach. The Ucoz platform may not be able to support custom coding or third-party plugins, leading to restrictions on design, functionality, and integrations. Additionally, the platform's SEO capabilities may be limited, impacting the blog's search engine ranking and visibility.

Transitioning the website from the Ucoz website builder to a custom-built platform, without relying on website builder tools, can address these limitations and offer several advantages. A custom-built platform can provide more design flexibility and support custom coding and integrations, enabling the blog to have a unique identity and functionality. It can also improve the blog's SEO capabilities, leading to better search engine rankings and increased visibility. Additionally, a custom-built platform can offer better scalability and security, ensuring the blog can handle increasing traffic and potential threats.

While transitioning the blog to a custom-built platform may require additional effort and investment, the benefits of improved functionality, design,

and SEO make it worth the endeavor. By investing in a custom-built platform, a website can enhance its online presence, attract more visitors, and provide better engagement opportunities with its audience. The transition can also help the university stay ahead of its competition and establish itself as a leader in digital communication and education.

The website builder has prevalent reasons for discontinuation or abandonment:

- poor SEO;

Website builders often generate messy code under the hood. This is bad for your SEO (search engine optimization) and can ruin your rankings on sites like Google.

You don't have control over the code of your website when using a website builder, only some of its design. If you look at the code behind a prebuilt website, it's a complete mess. When you write the code yourself, it'll be at least somewhat cleaner and easier to work with.

In addition, website builders often generate sites that load slowly. The slower your site takes to show up, the more likely visitors are to bounce.

- responsive design;

Most website builders make sites that look decent on a computer, but awful on mobile devices. You need a design that will work for both because people access the Internet in many different ways.

Your website should adapt to just about any screen size dynamically. Otherwise, you could easily lose visitors just because the styling is broken for them.

- not customizable;

With a custom website, you can change almost anything you want. When you use a website builder, the same isn't true. You can easily change some aspects of your site, but it's all determined by a prebuilt template.

When you pick a template for your website, you select a design that will completely drown out your ideas. You can't accomplish whatever you had in mind for your site before finding the template, because it simply isn't possible.

Creating your website from scratch is harder, but it's better than using a website builder. Sites like Ucoz and Wix just copy templates with bad SEO that you can't customize much. If you're looking to make a professional website, do it from scratch.

Kyrylo Zinovyev

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

ARTIFICIAL INTELEGENCE IN LEGAL SPACE

AI, or artificial intelligence, is a type of technology that enables machines to learn from data and perform tasks that would normally require human intelligence.

For example, AI algorithms can analyze large amounts of data and identify patterns, which can help lawyers make better decisions and provide more accurate advice to their clients. AI-powered tools can also automate repetitive tasks, such as document review and legal research, which can save time and reduce costs for law firms and clients.

Just as a human assistant can help with tasks such as scheduling and research, AI-powered tools can assist lawyers with tasks such as document review and legal research. However, unlike a human assistant, AI-powered tools can analyze vast amounts of data quickly and accurately, which can help lawyers make better decisions and provide more accurate advice to their clients. Artificial intelligence (AI) has had a significant impact on the legal space over the last decade. Here are a few ways in which AI has affected the legal industry:

- Automation of repetitive tasks: AI-powered tools can automate many repetitive tasks, such as document review, contract management, and legal research. This has helped to increase efficiency and reduce costs in the legal industry.
- Predictive analytics: AI algorithms can analyze large amounts of data and predict outcomes, such as the likelihood of winning a case or the potential value of a settlement. This has helped lawyers to make more informed decisions and provide better advice to their clients.
- Improved access to legal services: AI-powered chatbots and virtual assistants have made it easier for people to access legal services and get answers to their legal questions without having to meet with a lawyer in person.
- Enhanced cybersecurity: AI-powered cybersecurity tools can help law firms and legal departments detect and prevent cyber threats, such as phishing attacks and data breaches.
- Ethical and regulatory challenges: As with any emerging technology, AI raises ethical and regulatory challenges in the legal industry. For example, there

are concerns about bias in AI algorithms and the potential for AI to replace human lawyers.

Overall, AI has the potential to transform the legal industry by making it more efficient, accessible, and cost-effective. However, it is important for the legal industry to navigate the ethical and regulatory challenges that come with this technology.

Another breakthrough in this space is considered the release of ChatGPT which became extremely widespread now and is widely discussed in legal space and used by various startups and service providers. Passionate discussions about if AI eventually can replace lawyers started to rose again.

So, what is ChatGPT? ChatGPT is a type of large language model developed by OpenAI. The first version of GPT (Generative Pre-trained Transformer) was released by OpenAI in 2018, followed by subsequent versions such as GPT-2 and GPT-3. Now GPT-4 is on it's way. ChatGPT is a variant of GPT-3 that is specifically designed for use in conversational AI applications, such as chatbots and virtual assistants. It was released in 2020 as part of OpenAI's efforts to develop more advanced natural language processing (NLP) technologies. As an AI language model, ChatGPT is a tool that can provide general information and insights on various topics, including legal matters. However, it is important to note that ChatGPT is not a lawyer and is not qualified to provide legal advice or represent individuals in legal cases which is being told by ChatGPT itself. While ChatGPT is trained on a large corpus of text and can generate responses based on that training, it is not a substitute for the legal expertise and judgment of a qualified attorney. Legal cases often involve complex and nuanced legal issues that require a deep understanding of the law and the specific facts of the case. Therefore, relying solely on ChatGPT's responses for legal advice or as evidence in legal proceedings is not recommended.

As an AI language model, ChatGPT can assist lawyers in several ways to better handle a case. Here are a few examples:

- Legal research: ChatGPT can be trained on legal databases and case law to provide quick and accurate legal research. This can save lawyers time and help them to find relevant legal precedents and case law that can strengthen their arguments.
- Document review: ChatGPT can be used to automate the review of legal documents, such as contracts and briefs. This can help lawyers to identify key issues and relevant clauses quickly and efficiently.
- Predictive analytics: ChatGPT can analyze large amounts of data and predict outcomes, such as the likelihood of winning a case or the potential value of

a settlement. This can help lawyers to make more informed decisions and provide better advice to their clients.

- Virtual assistance: ChatGPT can be integrated into legal chatbots and virtual assistants to provide quick answers to legal questions and assist with legal tasks, such as scheduling and document management.
- Case Management: AI tools can help lawyers manage their caseloads by automating administrative tasks, scheduling deadlines, and tracking progress.
- Client Communications: ChatGPT and other conversational AI tools can be used to communicate with clients, answer their questions, and provide legal advice.

What about privacy and compliance which using AI and ChatGPT? As an AI language model, ChatGPT is not designed to handle sensitive or confidential information, such as private data of claimants, without appropriate safeguards in place.

The use of ChatGPT in the legal space to process personal data is subject to various laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These laws require that personal data is collected and processed in a transparent and lawful manner, and that appropriate safeguards are in place to protect the privacy and security of personal data. If you are considering using ChatGPT or any other AI tool in the legal space to process personal data, it is important to ensure that appropriate safeguards are in place to protect the privacy and security of personal data. This may include obtaining consent from claimants to process their personal data, implementing appropriate technical and organizational measures to protect personal data, and ensuring that any third-party services used in connection with ChatGPT are also compliant with applicable data protection laws and regulations. It is also important to consult with legal experts who are knowledgeable about data protection laws and regulations in your jurisdiction to ensure that your use of ChatGPT and processing of personal data is compliant with applicable laws and regulations.

Another hot discussion was around “smartness” of ChatGPT and here it’s important to admit that it does not have thoughts, opinions, or consciousness. It is a machine learning model that has been trained on a vast corpus of text data and uses statistical patterns to generate responses to input text. ChatGPT does not have the ability to form subjective opinions or beliefs, nor does it have the capacity to understand or interpret text in the way that humans do. Instead, it generates responses based on the statistical patterns it has learned from the training data, which are designed to provide the most probable answer based on the context of the input text and the patterns it has learned from the training data.

It is important to remember that while ChatGPT can provide useful information and insights based on the text it has been trained on, it should not be treated as a substitute for human judgment or expertise. ChatGPT's responses should always be evaluated critically and used as a tool to augment human decision-making, rather than replace it. This would mean that output is hardly dependent on quality of information provided meaning it should be evaluated, trusted, well defined, tightly connected to question answered. In other words, lawyer can't just provide all the case materials to ChatGPT and then start asking questions or opinions same as he might do with his colleague or assistance. A lot of preparational work should happen behind the scene.

What for example would happen if you'd provide detailed litigation case description for ChatGPT pretending it's a real case even though it never existed. ChatGPT will provide insights which would be most probable based on all the past cases it learned from. So instead of getting response that such case never existed it will try to predict what might be the output of it and will definitely sounds quite realistic. Because of this it's advised to use ChatGPT as a supervised assistant to find specific information. Then this information is reviewed by lawyer and based on analysis and discoveries made already filtered corpus of data is used for further processing and analysis by AI model. We may describe it as "don't let AI decide but just help you make decision faster and with useful facts in hands".

For example, ChatGPT can be used to find similar litigation cases and help lawyers to compare and evaluate the expected verdict. One way to accomplish this is to train ChatGPT on a dataset of legal cases, along with associated outcomes and other relevant information. This can enable ChatGPT to learn the patterns and relationships that exist between various legal factors, such as the parties involved, the legal issues at stake, and the outcomes of the cases. Once ChatGPT has been trained on a dataset of legal cases, it can be used to identify similar cases based on the relevant legal factors. This can help lawyers to find cases that are similar to their own, and to evaluate the expected verdict based on the outcomes of these similar cases. Similar approach might be used to evaluate expected damage costs etc.

Taking into account all stated above we may conclude that ChatGPT might be helpful and safe to use only by a professional and experienced lawyer who's aware about all the peculiarities of case, knows the domain good enough and set well defined and specific tasks for AI models while still making decisions and conclusions itself. What lawyers should avoid doing:

- Relying Solely on AI: Lawyers should not rely solely on AI tools to make decisions or provide legal advice. AI should be used as a tool to augment, rather than replace, the expertise and judgment of a human lawyer.

- Overpromising Results: Lawyers should avoid overpromising the results that can be achieved using AI tools. AI is not a magic solution that can solve all legal problems, and it is important to set realistic expectations for clients.
- Failing to Address Ethical Concerns: Lawyers should be aware of the ethical concerns associated with using AI tools in legal practice, such as the potential for bias, privacy concerns, and the unauthorized practice of law.
- Ignoring Data Security: Lawyers should take steps to ensure that the data they collect and store using AI tools is secure and protected from unauthorized access or disclosure.
- Failing to Understand AI: Finally, lawyers should take the time to understand how AI works, what its limitations are, and how it can be used effectively in legal practice. This includes staying up-to-date on developments in AI technology and seeking out training and education opportunities.

МЕНЕДЖМЕНТ ТА МАРКЕТИНГ

Андрійчук Я. Р.

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

ОРГАНІЗАЦІЯ ОПЕРАЦІЙНОЇ ДІЯЛЬНОСТІ БІЗНЕС-ОРГАНІЗАЦІЇ

Для того, щоб зберегти позиції на ринку в умовах жорсткої конкуренції, бізнес-організація стежить за всіма змінами, що відбуваються на ринку, та розробляє різні способи пристосування до негативних впливів, щоб вплинути на конкурентоспроможність. Операційна діяльність бізнес-організації завжди націлена на отримання прибутку та/або виконання інших завдань підприємства, до яких можуть відноситись: надання відповідного виду послуг, сільськогосподарська діяльність, виробництво промислових благ, здавання майна в оренду, продаж та транспортування товарів та інше. Тобто це те, заради чого безпосередньо існує бізнес-організація [5].

Операційна діяльність має кілька ключових особливостей:

– є основною діяльністю бізнес-організації;

– значна частина активів компанії спрямовано реалізацію операційної діяльності;

– має пріоритетний напрямок у діяльності бізнес-організації;

– визначає стадію життєвого циклу підприємства;

– складається з господарських операцій, які проводяться на регулярній основі;

– потребує найбільших трудовитрат [3].

Основна мета управління операційною діяльності бізнес-організації – це виявлення потреб для її життєздатності та подальшого вдосконалення. Операційні завдання підприємства обумовлені будь-якою діяльністю, яка приносить прибуток, за винятком фінансової та інвестиційної складових [8]. Операційну діяльність можна розділити на кілька складових – безпосереднє керування операційними процесами підприємства та регламентований облік з оформленням відповідних документів.

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. Операційний менеджмент – це управлінська діяльність, направлена на виконання операційної функції бізнес-організації [10].

Суб'єктами управління операційному менеджменті виступають операційні менеджери. Предметом управління в операційному менеджменті є:

– продукція та виробничі потужності;
– структура;
– контроль за процесами.

Структура операційного менеджменту включає складну схему підпорядкування та команди, якими користуються управлінці у межах роботи. Операційна діяльність підприємства передбачає всі витрати, необхідні щоденної нормальної роботи підприємства [1].

Операційна діяльність є пріоритетною сферою для будь-якої компанії. Серед завдань у рамках операційної діяльності можна виділити:

– виявлення основних потреб бізнес-організації;
– оперування вже вкладеними у компанію засобами;
– оплата всіх витрат, що забезпечують щоденне функціонування бізнесу та виникають у процесі виробничого циклу [9].

Від правильного операційного менеджменту діяльності, пов'язаної з розробкою, використанням та удосконаленням виробничих систем, залежить ефективність і конкурентоспроможність бізнес-організації.

Ресурси – це фактори виробництва, що використовуються людиною, необхідні для нормального функціонування процесів виробництва та його розвитку. Ресурси поділяються на:

– недостатні – це 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;
– надлишкові – це 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) [4].

Етапи здійснення операційної діяльності бізнес-організації включають:

Перший етап операційної діяльності зачіпає проблеми управління та контролю обсягу ресурсів для життєдіяльності бізнесу, бухгалтерські баланси, аналіз показників звіту про фінансові результати підприємства, інформацію з інших джерел за відповідний період. Недостатня кількість ресурсів істотно подовжить період освоєння виробництва, тоді як його надлишок може привести до нераціонального використання виробничого сировини [7].

На другому етапі операційної діяльності відбувається виявлення потреби в певному виді обладнання, перерахунок показників першого етапу і вичленення чистого прибутку.

На другому етапі операційної діяльності відбувається виявлення потреби в певному виді обладнання, перерахунок показників першого етапу і вичленення чистого прибутку.

Подібна схема операційної діяльності застосовується на бізнес-організаціях, які здійснюють виготовлення будь-якої продукції. Фінансові організації та компанії зі сфери послуг мають свій алгоритм операційної діяльності. Важливо відстежувати основні показники ефективності операційної діяльності підвищення рентабельності підприємства [2].

Управління операційною діяльністю бізнес-організації включає комплекс дій, спрямованих на досягнення кінцевого результату – виробництво продукції (надання послуг) належної якості, затребуваної споживачами, за умови забезпечення цільових показників ефективності та надійності діяльності бізнес-організації [6]. Цей комплекс дій повинен мати системний характер, діяльність бізнес-організації має не просто підлаштовуватися під виконання поточних завдань, а мати глобальну мету, сенс та напрямок, тобто мати стратегію [5].

Операційна діяльність бізнес-організації будь-якого типу має показники ефективності. Їхній розрахунок дозволяє оцінити рентабельність бізнесу, внести зміни до організації роботи, оптимізувати виробничі процеси.

Операційний прибуток – це прибуток від основної діяльності підприємства, тобто діяльності, яка приносить найбільшу частину виручки. Він відрізняється від валового прибутку, яка не враховує комерційних та управлінських витрат. До основних показників ефективності операційної діяльності належать:

- коефіцієнт операційних активів;
- коефіцієнт прибутку на одного працівника;
- тривалість операційного циклу;
- рентабельність виробництва [9].

Операційна діяльність компанії має приносити прибуток, інакше підприємство не впорається з конкуренцією та завдаватиме збитків. Аналіз показників операційної діяльності дозволяє виявити слабкі місця у створенні роботи, прибрати непотрібні активи, проаналізувати ефективність основних ресурсів.

Отже, операційна діяльність бізнес-організації - це основна робота компанії, заради якої і створювався бізнес загалом. Операційна діяльність

включає ряд послідовних етапів, які визначаються специфікою роботи бізнес-організації.

Список використаних джерел:

1. *Василенко О. В., Ткаченко Г. І. Виробничий (операційний) менеджмент: Навчальний посібник. К.: ЦУЛ, 2013. 532 с.*
2. *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.*
3. *Коробка С. В. Теоретичні аспекти операційного менеджменту малих підприємств. Економічний простір. 2020. № 153. С.71-74.*
4. *Коцко Т. А. Операційний менеджмент: навчально-методичний комплекс дисципліни: навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2019. С. 120.*
5. *Крамарчук С. П., Лубкей Н. П. Сутність операційного менеджменту та основні етапи його розвитку. Інфраструктура ринку. 2020. №44. С. 83-86.*
6. *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.*
7. *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).*
8. *Таранич О. В. Адаптація системи операційного менеджменту підприємств в умовах цифровізації економіки України. Економіка і організація управління. 2020. №4. С.143-151.*
9. *Ткачова С. С., Іванова Т. П. Операційний менеджмент. Навчальний посібник. Харків 2009. 452 с.*
10. *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

СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ ПРОЕКТІВ ІТ-КОМПАНІЙ

Розглянули можливість інтегрувати процес управління ризиками ІТ-проектів в основні процеси забезпечення діяльності компанії в ІТ-індустрії, з метою забезпечення комплексності та підвищення ефективності. Запропоновано модель зв'язку між бізнес-процесами управління ризиками, ІТ-проектами, ІТ-компаніями та їхніми знаннями. Використовуйте технологію управління знаннями для накопичення, зберігання та повторного використання інформації про процес управління ризиками. Крім того, оскільки основним ресурсом таких компаній є інтелектуальні ресурси, виникає проблема забезпечення надійного та ефективного потоку інформації всередині та за межами компанії. Для підтримки та підвищення конкурентоспроможності продуктів і проектів, які реалізують ІТ-компанії в процесі своєї діяльності, необхідно забезпечити високу якість.

Сьогодні питанням управління ІТ-проектами приділяється достатня увага, особливо з боку спільноти професійних менеджерів у цій сфері [1, 2]. У наукових працях це питання також часто піднімається, але його розуміння і розгляд значною мірою залежить від галузі знань, якою займається вчений. Питанням комплексного управління ІТ-підприємствами як проектно-орієнтованими компаніями з урахуванням усіх особливостей ведення таких підприємств та обмежень реалізації ІТ-проектів присвячено мало наукових робіт [3].

Мета статті. Проаналізувати можливість побудови системи управління ІТ-компанією на основі процесного підходу, використовуючи принципи управління проектами та поєднання методів та інструментів з різних наукових галузей, з метою покращення показників ефективності ІТ-компанії.

Компанії, що працюють у сфері інформаційних технологій, хоч і володіють багатьма відмінними рисами, проте відповідають основним ознакам концепції підприємства, яка полягає в цілеспрямованій концентрації ресурсів для досягнення конкретних цілей. Метою будь-якої підприємницької діяльності є, перш за все, отримання максимального прибутку шляхом зміни форми наявних ресурсів під час послідовного

здійснення взаємопов'язаних процесів усередині бізнесу як цілісної системи [4].

Процесний підхід на сьогодні є одним із найефективніших способів аналізу стану організації та ефективного управління нею. Розгляд ІТ-компанії з точки зору процесного підходу також дає змогу чітко визначити основні процеси, які в ній виконуються. Одним із них можна вважати й процес управління проектами. Досить поширеним явищем сьогодні є розрив загальних методів управління підприємствами, особливо методів управління проектами, які вони реалізують. Переважають два крайні підходи:

1. Керівництво компанії наголошує насамперед на процесі, розглядаючи управління проектом як його невід'ємну частину, не звертаючи належної уваги на окремі питання застосування, які можуть бути джерелом майбутнього ризику.

2. Управління проектами стає домінуючим процесом компанії, тоді як повний контроль і управління другорядними (але не менш важливими) процесами компанії втрачається.

Повертаючись до теми управління ІТ-проектами, варто відзначити той факт, що розробка та впровадження найбільш ефективних проектних методологій може не дати бажаних результатів, якщо решта процесів компанії управляються неадекватно або неефективно. З іншого боку, чітко визначений процес основної діяльності ІТ-компанії не матиме успішного результату, якщо в процесі моделювання не враховуватимуться особливості управління проектами. Звичайно, не всі ІТ-компанії реалізують ті чи інші проекти в рамках своєї діяльності. Але багато великих підприємств у цій галузі можуть запускати кілька портфелів проектів різних типів одночасно, навіть використовуючи ті самі ресурси [5].

Можна зробити висновок, що для побудови справді ефективної системи управління підприємством найбільш доцільно комбінувати методи та прийоми з різних галузей знань. Узагальнено етапи ефективного впровадження процесного підходу до можна описати так: аналіз ефективності та відповідності існуючих процесів поставленим цілям; розробка рекомендації по впроваджувенню змін; постійно контролювати виконання процесу та коригування.

У процесі побудови моделі процесів ІТ-компанії прийнято виділяти 5-6 основних процесів (кількість залежить від розміру організації та сфери діяльності) і достатню кількість допоміжних процесів. Управління проектами, як особливий вид діяльності, можна охарактеризувати як один із основних бізнес-процесів. На Рис. 1 показано схематичне зображення зв'язків між ІТ-процесами компанії. Це частина глобального процесу

компанії та акцентує увагу на процесі управління проектами (подробиці потоку ресурсів та інформації опущено).

Управління ризиками в управлінні проектами – це набір дій і заходів, які включають виявлення ризиків, їх аналіз і формування управлінських рішень, спрямованих на зменшення ймовірності та ступеня їх впливу на прогрес, результати та продукти цих проектів. Існують різні підходи, які надають —керівникам проектів інструменти для ефективного управління ризиками [6].

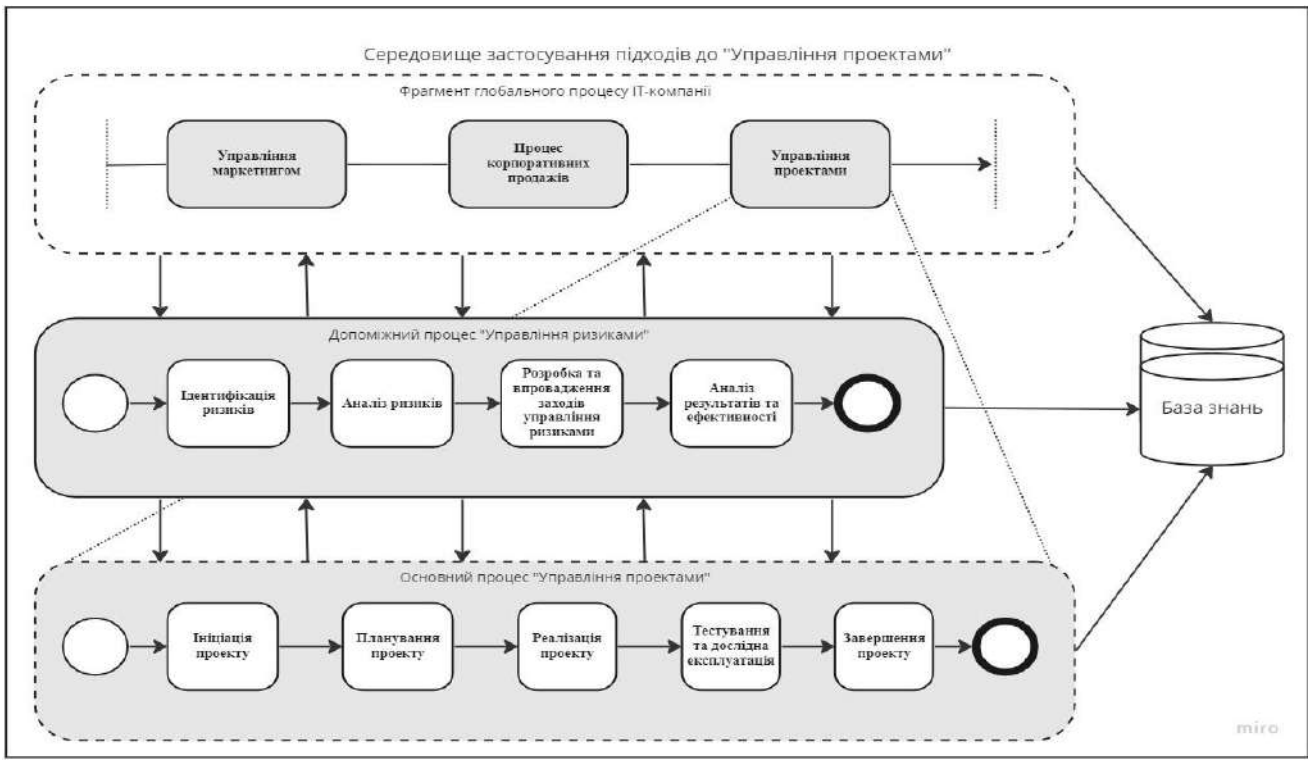


Рис. 1 – Модель зв'язку між бізнес-процесами управління ризиками, IT-проектами, IT-компаніями та їх загальними знаннями.

Також методологія процесного менеджменту не оминає питання управління ризиками. Набір заходів з управління ризиками IT-підприємства може бути представлений як окремий процес або як компонент інших процесів підприємства.

Під час реалізації проектів можуть виникати ситуації, коли той чи інший ризик одного проекту може бути притаманний іншому проекту, реалізованому в портфелі компанії. Управління такими ризиками та тими ризиками, які можуть виходити за межі повноважень керівника проекту, але які можуть вплинути на результат проекту, може здійснюватися повністю або

частково поза межами проекту. Це дає змогу максимально мобілізувати ресурси та підвищити ефективність «загального» управління ризиками.

Виходячи з цього, можна відзначити перевагу моделювання ще одного допоміжного бізнес-процесу для управління ризиками компанії. Він викликається як у процесі операційної діяльності, так і в процесі управління проектами. На Рис. 1 показано зв'язки між бізнес-процесами, які керують IT-підприємством. Тут процес управління проектом вважається одним із основних процесів компанії, а процес управління ризиками – допоміжним.

На Рис. 1 ми також бачимо, що всі вищезазначені елементи бізнес-структури IT-компанії знаходяться в умовному середовищі застосування підходу до «управління знаннями». Оскільки основними ресурсами компаній у сфері IT є люди, інформація та накопичений досвід, особливу увагу слід приділити комунікаційним процесам компаній, які можуть мати як простірову так і часову складову. Перш за все, відповідна модель управління знаннями забезпечує підвищення ефективності процесів управління та виробництва. Слід також зазначити, що накопичення «історичних» знань компанії має велике значення для проведення аналітичних досліджень і розробки нових стратегій розвитку та діяльності. Що стосується ризику, то застосування рудиментарних методів у певних сферах, таких як управління знаннями в IT-компаніях, є однозначно виправданим.

При управлінні IT-проектами в рамках одного підприємства керівникам проектів часто доводиться керувати ризиками, які вже виникли або, принаймні, були предметом аналізу та розробки стратегії контролю. Накопичення бази знань про всі ризики, як в рамках управління проектами, так і в масштабах компанії, забезпечує достатній обсяг інформації для детального попереднього аналізу, потенційної ескалації ризиків на ранній стадії та запобігання надається керівнику проекту. «Подвійний» і, як наслідок, неефективне управління «спільним» ризиком, коли існують паралельні проекти.

Підсумовуючи, зауважте, що моделі та методи управління проектами не матимуть успіху, якщо вони не будуть якісно інтегровані в структуру бізнес-процесів організації. Основною перешкодою для дійсно ефективного управління ризиками зазвичай є відсутність інформації про джерела, характеристики та наслідки можливих ризиків. Комплексний підхід до управління IT-компанією забезпечує інформаційні потреби не тільки керівника проекту, а також і топ-менеджменту компанії.

Список використаних джерел:

1. *Листер Т. Вальсируя с медведями. Управление рисками в проектах по разработке программного обеспечения / Листер Т., ДеМарко Т. – М: Компания р.т. Office, 2005. – 322 с.*

2. *Расмуссон Дж. Гибкое управление IT-проектами. Руководство для настоящих самураев. Как Мастера Agile делают выдающее./ Дж. Расмуссон. – СПб.: Питер, 2012. – 272 с.*

3. *Песоцкая Е.Ю. Управление рисками при внедрении ИТ-проектов / Песоцкая Е.Ю. // Компьютерное моделирование в науке и технике. [Електронний ресурс]. – Режим доступу: http://econf.rae.ru/article/3910.*

4. *Репин В. В., Елиферов В. Г. Процессный подход к управлению. Моделирование бизнес-процессов. / В. В. Репин, В. Г. Елиферов. – М: РИА «Стандарты и качество», 2004. – 408 с.*

5. *Онищенко І. І. Тенденції розвитку управління ризиками проектів ІТгалузі. / І. І. Онищенко // Тези доповідей 11 міжнародної конференції «Управління проектами у розвитку суспільства». Тема: Розвиток компетентності організації в управлінні проектами, програмами та портфелями проектів. – К.: КНУБА, 2014. – 260 с. – с. 150–152.*

6. *Товб А. С., Ципес Г. Л. Управление проектами: стандарты, методы, опыт. – 2-е изд., стер. – М.: ЗАО „ОлімпБизнес”, 2005. – 240 с.*

Белов М. С.

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

ВОСПРИЯТИЕ УКРАИНСКИХ БРЕНДОВ ПОТРЕБИТЕЛЯМИ С МОМЕНТА НАЧАЛА ПОЛНОМАСШТАБНОЙ ВОЙНЫ В УКРАИНЕ

Всем известна сила бренда и его влияние на потребителя. Особенно в современной жизни, когда предложение существенно превышает спрос и все производители борются за внимание и сознание потребителя.

Естественно, это не прошло мимо и украинских производителей. С момента начала полномасштабной войны в Украине сила украинского бренда внутри страны и на мировом рынке возросла многократно.

Так что же такое бренд? Бренд - это товарный знак, торговая марка имеющая высокое признание у потребителя. На самом деле понятие бренда довольно объемно, так как оно содержит в себе массу критериев: сам товар или услугу, отношение, восприятие, ожидание и ассоциации пользователей, характеристики, ожидаемые потребителем, обещание данные производителем своим потребителям о новых преимуществах товара или услуги. Поэтому можно подытожить, что бренд - это то, что находиться в сердцах, на подсознании пользователей и приходит на ум, когда они видят или слышат логотип, мелодию, слоган какой-либо торговой марки. Стоимость ведущих мировых брендов по данным рейтингового агентства Interbrand (www.interbrand.ru) измеряется миллиардными цифрами. Так, например, в 2008 году стоимость торговой марки Coca-Cola составляла 66,7 миллиардов долларов. Причем, зачастую стоимость брендов в несколько раз превышает стоимость материальных активов компаний. Именно поэтому необходимость использования технологии бренда, практически никем не подвергаются сомнению [1].

В последние годы количество украинских брендов стремительно росло, но пик своей популярности и признательности многие, кто устоял и выдержал нагрузку, а так же смог перестроить свой бизнес на новые рельсы с момента начала войны в Украине, получил большую признательность и популярность.

Сейчас каждый украинец в своей стране и за ее пределами всячески поддерживает украинского производителя стараясь приобретать продукцию украинских брендов как для себя, так и для других людей в виде подарков,

поощрений и благодарности. Товары с украинской символикой, фразами и выражениями, "жовто - блакитними" цветами популярны далеко за пределами Украины, так как каждый стремиться приобрести что-то из Украины, таким образом поддерживая ее экономику и приближая победу. Результаты исследования проведенные в декабре 2022 года исследовательской компанией Gradus Research показывают, что в настоящее время 69% опрошенных украинцев заявляют, что намеренно выбирают продукцию украинских брендов. А 56% начавших покупать новые украинские бренды во время войны делают это, чтобы поддержать своих производителей.

В целях поддержки дизайнеров и обеспечения работы украинских fashion - брендов на мировых площадках были организованы разнообразные pop-up ивенты и бутики. Blue Skies — это не только желание в сердце каждого украинца, но концепция нового pop-up от Нью-Йоркского PR-шоурума и e-commerce платформы DOORS NYC. Шоурум, находящийся в центре Сохо, Нью-Йорк, открыл свои двери 13 сентября и будет работать до 3 октября. DOORS NYC появился полтора года назад и сейчас представляет уже более 200 независимых брендов одежды со всего мира. *«Мы годами сотрудничали с украинскими брендами еще до появления DOORS и наладили с ними очень теплые отношения. С началом военных действий многие бизнесы оказались в критической ситуации, особенно молодые бренды. Поэтому мы отменили оплату наших услуг для украинских дизайнеров и оказали помощь всем, кто обратился к нам. Сейчас мы сотрудничаем с некоторыми брендами, которые даже не наладили производство, но им нужны PR-консультации», — объяснила основательница DOORS NYC Элис Траутман-Узунер.* Посетители pop-up в течение месяца смогут не только насладиться шоппингом, но и погрузиться в мир виртуальной моды. Студенты украинской Pushka School подготовили уникальный 3D-fashion проект. В диджитал коллекции присутствуют национальные мотивы и голубые небеса, на которые мы все так надеемся. [2].

Поэтому, в современных условиях при снижении потребительского спроса из-за увеличения количества производителей все большее внимание уделяется брендированию и интерес к нему. Благодаря этому пути производитель преследует две основные цели: закрепиться за определенным сегментом рынка и приумножить прибыль компании. Но не всегда получается достичь желаемого результата. Анализируя причины этого можно рассмотреть основные уровни преобразования бренда (рис. 1).

Рис. 1. Уровни формирования бренда.

По имеющимся данным, привлечение нового клиента в 6 раз дороже повторных продаж. Если же клиент ушел от компании, то его повторное привлечение обходиться в 25 раз дороже, нежели завоевание нового.

Лояльность к бренду компании в современных условиях не означает финансовой сверхприбыли. Инвестируя значительные средства в свой бренд, компании достигают только лояльность потребителей, которая в современных условиях является средством опосредствованной доходности за счет предотвращения затрат на привлечение потребителей. Другой результат можно получить только за счет экономической дифференциации торговой марки [3].

Бренд для потребителя должен сигнализировать качество покупаемой им продукции или услуг. Обладание сильным брендом способно дать человеку ощущение радости. Потребитель должен испытывать от покупки позитивное и теплое чувство.

Существенно значительным для понятия бренда является «капитал бренда». Этот термин предназначен для описания силы бренда. Данная концепция сформировалась в 1980-е годы.

Основными элементами капитала бренда являются:

1. Осведомленность или его узнаваемость,
2. Лояльность к бренду,
3. Воспринимаемое потребителем качество,
4. Ассоциация потребителя с брендом [4].

Подытоживая вышесказанное хочется отметить, что бренды живут в наших головах и сердцах. Они часть нас, нашей культуры и уже являются неотъемлемой частицей нашей жизни.

Бренды отражают нашу идентичность и характер, волю к правде и свободе, свободу мысли и независимость... Мы четко видим сознательное намерение украинцев и иностранных граждан поддержать Украину и ее экономику, выбирая товары и услуги локальных брендов. И даже нынешний фактор экономии граждан не останавливает их перед покупкой привычных товаров в любимых местах продаж, в очередной раз подтверждая, что бренд сейчас важен как никогда. Потому что благодаря этому украинцы пусть и небольшими шагами, но приближают долгожданную победу!

Список использованных источников:

1. *И. А. Быков"Технологии брендинга", Санкт-Петербург, СПБГУ, 2009.- 70 с.*
2. *https://elle.ua/ru/elle-business/bolee-20-ukrainskih-brendov-na-mirovoy-arene-fashion-iniciativi-v-podderzhku-ukraini/*
3. *Reinartz W., Kumar V. The Mismanagement of Customer Loyalty. //Harvard Business Review. – Harvard Business School Publishing Corporation. – July 2002, P. 4-12.*
4. *Герасименко В. В., Очковская М. С. Бренд-менеджмент: Учебное пособие. — М.: Экономический факультет МГУ имени М. В. Ломоносова, 2016. — 100 с.*

Бурлака Ю. В.

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

ВІЙНА ТА ІНШІ КАТАКЛІЗМИ ЯК КЛЮЧОВИЙ ФАКТОР МОТИВАЦІЇ ДЛЯ КОМАНДИ І РОЗВИТКУ ДЛЯ ПРОДУКТУ ТА БІЗНЕСУ

Ми живемо в неймовірний час! Глобалізація, фінансові кризи, хвилі карантину, локальні конфлікти, анексії територій, повномасштабні вторгнення нагадують картину «Крик» Мунка де все завмирає в панічному спокої й нескінченному очікуванні змін. Та на практиці ми спостерігаємо дещо інше і безумовно цікавіше.

З часу свого зародження людство у різноманітних формах своїх цивілізацій невпинно та безперервно, крок за кроком суне спіральними циклами розвитку й занепаду. У відповідь на виклики середовища усталена система або адаптується, отримуючи новий стрибок в розвитку або руйнується під корінь. Як писав в своїй праці Чарльз Дарвін «Походження видів шляхом природного відбору, або збереження придатних порід у боротьбі за життя», або змінюєш щось і живеш або спиняєшся й помираєш.

Жага життя це перша базова мотивація всього живого. Проте, як саме виживати в моменті загрози, це вибір котрий кожному дає еволюція і по суті ми маємо всього 3 базові варіанти: «бий», «завмри» або «біжи». Кожна істота отримує початковий, інстинктивний набір поведінкових моделей з огляду на досвід набутий її предками. Людина та ще кілька видів окрім базового набору варіантів реакції на загрозу має розвинений та багаторівневий інструмент навчання, завдяки якому замість «смертельної» проблеми з'являються нові можливості виживання. Все це дозволяє нам ширше поглянути на цікавий феномен в моменті, коли здавалось би «катаклізм» руйнує всю усталену систему і знищує відчуття безпеки, замість «бігти» чи «завмерти» або «померти» команда починає бачити нові можливості розвитку бізнесу й адаптувати або створювати нові продукти – «бити». Іншими словами з'являється достобіса енергії, котру хочеться кудись направити. Ми навіть можемо спостерігати проходження всіх «5-ти стадій прийняття» за моделлю Елізабет Кюблер-Росс але зазвичай з позитивним фіналом.

24 лютого 2022 року, повномасштабне вторгнення Росії в Україну, вся країна в паніці, люди масово тікають, залишають домівки, у всіх одне

бажання – зберегти життя та бути як найдалі від ракет, вибухів і фронту. Руйнується інфраструктура, руйнується логістика, руйнуються команди, родини, зникає бізнес.

Перша реакція команди – безпека рідних, близьких, безпека бізнесу й продукту. Все завмирає і стає на паузу очікуючи розвитку подій. Паралельно відбуваються дуже цікаві зміни – команда починає діяти. Ключова суть будь-якої команди – дія, дія у відповідь на ціль, у відповідь на зміну зовнішнього середовища. Команда у своєму усвідомленні це автономна істота, живий організм, котрий не хоче вмирати, хоче жити. Якщо команда перестає діяти – вона вмирає, розпадається. Будь-яка дія приводить до результату, будь-який результат це досвід, будь-який досвід це навчання, або навчання на помилках або навчання успіхом.

Ніде не вчать як розвивати бізнес в моменті повномасштабного вторгнення. Або як мотивувати команду коли за вікном вибухи, а над головою літають ракети. Або як пояснити команді що треба щось робити, але без грошей і поки не зрозуміло що. В цей момент є лише команда об'єднана вірою в щось. Віра в будь-що. Віра в справедливість. Віра в життя. Віра в те що ми на своїй землі і до нас прийшли зі зброєю. Віра в те що кожен на своєму місці може зробити те що вміє найкраще для перемоги. В цей момент лідер формує віру і транслює команді. І команда починає діяти. Живий організм з мотивацією до життя.

Війна та будь-який катаклізм створює та феноменально підсилює фактори внутрішньої мотивації найсильнішою базовою цінністю – вижити. Вижити як людині, вижити як родині, вижити як команді, вижити як бізнесу, вижити як нації та демократії. Це те, що не потрібно пояснювати, це те, що не потрібно шукати, це те, в чому не потрібно переконувати, це те, що просто є, тут і зараз, зрозумілим без слів. Це те, що автоматично запускає креативне мислення, генерує та передає енергію, зумовлює вийти з зони комфорту, знайти нові можливості там де, на перший погляд їх нема або не видно. Це те, що об'єднує, знаходить партнерів, гасить будь-які між особові конфлікти. Це те, що змінює процеси без погоджень, бо й так все зрозуміло.

У своїй книзі «Драйв. Дивовижна правда про те, що нас мотивує» Деніел Пінк описує 2 базові системи мотивації: «внутрішня» та «зовнішня». Діаметрально протилежні за своєю суттю та різні за результатом. «Внутрішня» базується виключно на зацікавленості самої людини процесом або результатом її роботи, «зовнішня» – базується на матеріальних або нематеріальних, але завжди «примусових» факторах заохочення до процесу або результату. Результат «внутрішньої» безперервно зростає та самостійно

адаптується до фактичних очікувань середовища, результат «зовнішньої» виключно мінімально достатній, з огляду на поставлені вимоги й на запропоноване заохочення. Популярні методи управління персоналом здебільшого надають перевагу «зовнішнім» факторам мотивації, вбачаючи в них отримання швидкої та контрольованої операційної вигоди натомість отримуючи очікуваний, тимчасовий, але мінімальний результат.

Так от, під час війни, або інших катаклізмів ми стикаємось з тим, що зовнішня мотивація для самої людини втрачає сенс (життя за гроші не купиш), цінність і неможлива загалом з огляду на збереження і заморозку бізнесу, натомість в людини з'являється неймовірна за своєю силою енергія і жага до дії аби подолати, як колосальний стрес, так і страх. Людина шукає можливості виходу для цієї енергії і тут ми бачимо кілька цікавих сценаріїв розвитку.

«Позитивний» сценарій:

1) Людина починає самостійно шукати можливості і джерела цих можливостей;

2) Самоорганізація навколо знайденої, або запропонованої можливості;

3) Самостійний пошук партнерства і допомоги;

4) Надзвичайно швидка і дешева реалізація, або змін в продукті, або нового продукту, або нового бізнесу тощо.

«Негативний» сценарій:

1) Людина займає пасивну позицію;

2) Колосальна енергія сублімується в агресію і конфлікти «без причини»;

3) Агресія досягає неймовірних, для людини, масштабів;

4) Людина змушена постійно змінювати середовище в нескінченному циклі агресія-конфлікт, поки не вийде на позитивний сценарій.

В результаті «позитивного» сценарію команда, яка до війни займалася розробкою та розвитком «мирного» маркетплейсу на спокійному ринку з усталеною та прибутковою бізнес моделюю:

1) Відмовилась від зарплатні, що б зберегти бізнес і команду;

2) Відмовилась від доходів з клієнтів для їх адаптації до «воєнного» часу;

3) Адаптувала всі процеси для допомоги та виживанню бізнесу клієнтів;

4) Створила нові інструменти для допомоги волонтерам та державі;

5) Адаптувала маркетплейс під нові потреби покупців та продавців;

6) Створила нові локальні та міжнародні продукти для захисту економіки держави;

7) Створила внутрішній, волонтерський напрямок для гуманітарної та військової допомоги;

8) Після адаптації бізнесу клієнтів побудувала нові умови монетизації;

9) Розробила план виходу на точку окупності й прибутку для бізнесу в нових реаліях та відновила повну винагороду всім співробітникам.

Звісно, модель поведінки людини й відповідно напрямок її мотивації в будь-якій ситуації залежить від системи цінностей самого соціуму, або іншими словами ментальних моделей нації, рольових прикладів, які транслює та підтримує нація своєму народу протягом всієї історії її становлення як нації.

Ми бачимо приклади як, здавалось би в однакових ситуаціях (і на полі бою і в тилу) зовсім по різному діють в Україні та Росії, навіть попри фундаментальні розбіжності в системах цінностей, рушійною силою українців є «внутрішня» мотивація «до незалежності та демократії» з повним розумінням що, де потрібно і навіщо, з постійним зворотним зв'язком, натомість рушієм росіян є виключно «зовнішня» мотивація «кнутом» та «рубльом» котру марно прагнуть загорнути під вигляд «внутрішньої», ідейної пропаганди, яку ніхто з них не розуміє і не усвідомлює, отримуючи «молітвослови» там де потрібні тепловізори, а відтак «разброд і шатанія» та поразку за поразкою. Як би це не звучало дивно, але різниця колосальна, уявити собі що 30 з лишком мільйонів українців, без армії та внутрішніх ресурсів, стримали навалу 150 мільйонів розгніваних незрозуміло на що росіян, з регулярним постійно діючим і розвиненим військом, ядерним потенціалом, з незрівнянно більшою економічною міццю.

Це безумовно найяскравіший прояв «внутрішньої» мотивації та результату котрий ми отримуємо як команда, як бізнес, як нація.

Список використаних джерел:

1. *Liz Wiseman. Multipliers: How the Best Leaders Make Everyone Smarter*
2. *Daniel H. Pink. Drive: The Surprising Truth About What Motivates Us*
3. *Mihaly Csikszentmihalyi. Flow: The Psychology of Optimal Experience*
4. *Чарльз Дарвін. «Походження видів шляхом природного відбору, або збереження придатних порід у боротьбі за життя»*
5. *Кріс Фріт. Мозок і душа. Як нервова діяльність формує наш внутрішній світ.*
6. *Дмитрий Жуков. Стой, кто ведет? Биология поведения человека и других зверей*

Ващенко С. А.

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

ВЛИЯНИЯ ТЕХНОЛОГИЙ НА СТРУКТУРУ И ОРГАНИЗАЦИЮ РАБОЧЕГО ПРОЦЕССА В IT-КОМПАНИЯХ

В современном мире IT-технологии проникают во все сферы жизни, и, несомненно, они имеют большое влияние на структуру и организацию рабочего процесса в IT-компаниях. Мы рассмотрим основные аспекты влияния технологий на IT-компании.

Одним из наиболее влиятельных аспектов является автоматизация процессов. Многие задачи, которые раньше выполнялись вручную, теперь могут быть автоматизированы. В IT-компаниях автоматизация бизнес-процессов используется для оптимизации процессов разработки программного обеспечения, управления проектами и контроля качества. Это позволяет сократить время выполнения задач, увеличить эффективность и точность работы, а также уменьшить затраты на человеческий ресурс. Примером может быть автоматизация тестирования ПО. Вместо ручного тестирования разработчики могут использовать автоматизированные тестовые сценарии, что сокращает время тестирования и повышает точность результата. Часто используется автоматизация в управлении проектами. Использование специализированных инструментов, таких как Asana, Trello или Jira, позволяет оптимизировать процессы управления проектами, отслеживать выполнение задач и контролировать сроки. Автоматизация технической поддержки. Использование чат-ботов и автоматизированных систем технической поддержки позволяет снизить нагрузку на живых операторов и ускорить решение проблем клиентов. Немаловажной является автоматизация финансовых процессов. Использование программного обеспечения для автоматического выставления счетов, учета финансовых транзакций и оплаты счетов позволяет сократить время и уменьшить вероятность ошибок. Использование DevOps. DevOps - это подход к разработке программного обеспечения, который объединяет команды разработчиков, тестировщиков и системных администраторов, чтобы обеспечить более быструю и надежную поставку продукта [1]. DevOps использует автоматизированные инструменты и процессы для управления процессом разработки, тестирования и развертывания ПО. Например, в IT-компаниях часто используются CI/CD-системы (Continuous

Integration/Continuous Delivery), которые автоматизируют процесс интеграции и тестирования изменений в коде, а также автоматического развертывания новой версии ПО на сервере [2].

Не менее важным аспектом является использование облачных технологий и сервисов. С появлением облачных технологий компании получили возможность не только хранить свои данные в облаке, но и использовать различные облачные сервисы для управления проектами, хранения и обмена документами, обработки данных и т.д. Например, Google Docs и Microsoft Office 365 позволяют сотрудникам работать над документами в режиме реального времени, делиться ими и работать удаленно [3, 4]. Это значительно улучшает производительность и эффективность работы команды, особенно если она находится на удалении. Также облачные решения позволяют компаниям быстро масштабироваться, увеличивать производительность и улучшать безопасность данных. Например, облачные сервисы, такие как Amazon Web Services (AWS) или Microsoft Azure, позволяют компаниям быстро запускать и масштабировать свои приложения, не беспокоясь о инфраструктуре и управлении серверами.

Также большое влияние на структуру и организацию рабочего процесса оказывает работа в режиме онлайн. Работа в режиме онлайн обеспечивает возможность удаленного доступа к рабочему месту и инструментам, что дает большую свободу сотрудникам и упрощает организацию рабочего процесса. Например, сотрудники могут работать из дома или с другого места, что повышает уровень комфорта и гибкости работы. Работа в режиме онлайн также привела к увеличению использования онлайн-сервисов и приложений для совместной работы и коммуникации. Такие сервисы, как Zoom, Slack, Trello, GitHub и другие, позволяют сотрудникам работать вместе и координировать свои действия, несмотря на удаленное расположение [5]. Также увеличилось количество проектов с цифровой составляющей, таких как разработка приложений для удаленной работы, онлайн-образования, онлайн-маркетинга и т. д. Это привело к увеличению спроса на разработку программного обеспечения и другие IT-услуги. Удалённая работа также привела к изменению коммуникационных процессов в IT-компаниях. Ранее, сотрудники общались в офисе либо по телефону и электронной почте. Теперь же, сотрудники общаются в онлайн-чатах, видеоконференциях и используют другие онлайн-инструменты. Это привело к изменению формы и содержания коммуникаций внутри компании. Также это привело к изменению подходов к управлению проектами в IT-компаниях. Для эффективной работы в онлайн-режиме, необходимо

использовать новые методы и инструменты для планирования, отслеживания и управления проектами. Некоторые компании перешли на использование Agile-методологий и других методов, которые позволяют более эффективно управлять проектами. Также повысилось качество жизни сотрудников IT-компаний. Сотрудники больше не тратят время на дорогу в офис, могут работать из любой точки мира и лучше организовывать свое время. Это приводит к увеличению уровня удовлетворенности сотрудников и, как следствие, повышению их производительности.

Внедрение новых технологий является неотъемлемой частью развития IT-компаний. Однако, новые технологии требуют постоянной адаптации и обучения сотрудников. В связи с этим, внедрение новых технологий может существенно влиять на структуру и организацию рабочего процесса в IT-компаниях. Во-первых, внедрение новых технологий требует постоянного обучения сотрудников. Сотрудники IT-компаний должны уметь использовать новые технологии, чтобы быть эффективными в своей работе. Это требует дополнительных затрат на обучение и развитие сотрудников. IT-компании должны инвестировать в обучение своих сотрудников, чтобы они могли лучше использовать новые технологии и быть более производительными. Во-вторых, внедрение новых технологий может требовать изменения структуры и организации рабочего процесса в IT-компаниях. Например, внедрение новой системы управления проектами может потребовать пересмотра существующей структуры и организации команд. Новые технологии могут также потребовать изменения процессов взаимодействия между различными отделами и командами в компании. В-третьих, внедрение новых технологий может привести к появлению новых должностей и изменению требований к сотрудникам. Например, внедрение искусственного интеллекта может потребовать наличия специалистов по машинному обучению и анализу данных в компании. В связи с этим, IT-компании должны постоянно мониторить изменения в требованиях к квалификации и компетенциям сотрудников, чтобы привлекать и удерживать лучших специалистов в отрасли.

Таким образом, внедрение новых технологий в IT-компаниях может значительно повлиять на структуру и организацию рабочего процесса. Новые технологии могут повысить производительность, эффективность и безопасность работы, а также улучшить доступность продуктов и услуг для клиентов. Однако для успешного внедрения технологий необходимо учитывать специфику компании и ее бизнес-процессов, а также обеспечить обучение сотрудников и поддержку новых технологий.

Список использованных источников:

1. *Atlassian. URL: https://www.atlassian.com/devops*
2. *Unity. URL: https://unity.com/ru/solutions/what-is-ci-cd*
3. *Google Docs. URL: https://www.google.com/docs/about/#overview*
4. *Microsoft Office 365. URL: https://www.office.com/*
5. *Trello. URL: https://trello.com/guide/remote-work/digital-tools*

Горенко С. Н.

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

МЕНЕДЖМЕНТ МАРКЕТИНГОВОЙ СТРАТЕГИИ ОРГАНИЗАЦИИ: ОТ ТЕОРИИ К ПРАКТИКЕ

Чтобы получить прибыль, компании создают маркетинговую стратегию, которая распределяет ресурсы для определенных групп потребителей. Они создают организационный план, определяя цели своей компании на длительный период времени. Как только это будет сделано, компании разработают программы, которые помогут им достичь своих целей. Вот почему маркетологи используют термин «стратегия» для действий, которые предприятия осуществляют с целью создания новых продуктов и услуг или продвижения уже существующих.

Маркетинг в том виде, в каком мы его знаем сегодня, зародился в 1950-х годах. До этого предприятия сосредоточивались на практических задачах, таких как производство и торговля. Однако и коммерция, и маркетинг стали формализованными в 1950-х годах. Это было связано с тем, что предприятия хотели лучше обслуживать своих клиентов и повышать свою конкурентоспособность. Следовательно, они сосредоточились на клиентах, чтобы увеличить продажи. Комплекс маркетинга представляет собой комбинацию четырех ключевых компонентов; цена, продукт, продвижение и распространение. Это основа каждой маркетинговой кампании и включает в себя решения, касающиеся рекламы, местоположения и ценообразования.

Маркетинг включает в себя определение целей, политики и видения компании. Это также включает в себя создание бизнес-плана и реализацию политик в нем. Маркетинговые стратегии включают создание конкретных политик для различных ситуаций, таких как дифференциация и сегментация рынка. Кроме того, существуют общие тактики, такие как снижение цен и увеличение доли рынка. Эти стратегии составляют основу маркетинговой стратегии.

Маркетинговая стратегия должна опираться на конкурентные стимулы, чтобы быть реализованной. Монополизированные рынки, такие как коммунальные услуги, нуждаются в реализации маркетинговых программ, чтобы поддерживать высокий уровень продаж и провоцировать новое потребление. Это связано с тем, что конкуренция подпитывает

создание маркетинговых стратегий. Имея стабильный спрос на свои услуги и высокую популярность, коммунальные предприятия не нуждались в корпоративных маркетинговых программах для достижения успеха. Поскольку дерегулирование и глобализация привели к усилению конкуренции для многих компаний, современные маркетинговые стратегии стали важными для компаний, которые хотят оставаться прибыльными.

Концепции маркетинга обеспечивают основу для современных маркетинговых стратегий. Маркетинговые стратегии первоначально появились в коммерческом обмене между людьми, занимающимися торговлей, например куплей-продажей. Многие ранние цивилизации, в том числе египтяне, китайцы, вавилоняне, греки, венецианцы и римляне, разработали эти стратегии, торгуя друг с другом. При обмене товарами реализовывалась маркетинговая функция. Вероятно, они разработали эффективные методы для каждого сценария, чтобы поделиться ими с другими людьми и организациями. Более того, они могли передавать эти стратегии другим в качестве средства саморекламы.

Маркетинговая стратегия создается отдельным лицом, группой или организацией для достижения определенного результата. Любой может разработать стратегию; это просто результат, который определяется преднамеренной мыслью. Организация может быть семьей, корпорацией, страной или даже нацией. Они также могут воспользоваться программными приложениями, компьютеризированными системами на компьютерах, принадлежащих корпорации или разработанными ими самими, или даже сетями, разработанными фирмой.

Бизнес-конкуренты обычно преследуют рамки стратегии через своих конкурентов. Это связано с тем, что предприятия конкурируют за ограниченные ресурсы. Чтобы улучшить свое положение по сравнению с конкурентами, агрессоры работают над улучшением своего положения по сравнению с другими организациями, ориентированными на работу. Это может быть достигнуто за счет увеличения поставок, дистрибьюторов, клиентов и конкурирующих групп защиты интересов.

Со временем потребность в долгосрочном планировании маркетинговых стратегий стала рассматриваться как бизнес-функция. Это произошло потому, что ведущие теоретики менеджмента, такие как Питер Друкер, определили необходимость постоянного долгосрочного планирования в ответ на изменения как внешних, так и внутренних условий. Они считали, что это планирование должно осуществляться с точки зрения клиента.

В 1950-х годах предприятия начали внедрять стратегическое мышление в свои маркетинговые стратегии с помощью составления бюджета, долгосрочного планирования, планирования процессов и стратегического мышления. Это произошло благодаря широкомасштабному внедрению этих методов после Второй мировой войны. Бюджетирование было одним из стратегических компонентов этих идей, поскольку оно помогало компаниям распределять средства между различными отделами внутри компании. Годовые бюджеты компаний отслеживали распределение планов проектов. Но в 1960-х долгосрочное планирование заменило составление бюджета в качестве стратегии. Например, график может выделять средства для достижения определенных финансовых целей в течение пяти или десяти лет.

С 1974 года отсутствие у компаний понимания будущего привело к уменьшению важности долгосрочного планирования. Это произошло из-за их неспособности правильно предсказать, сколько денег и ресурсов им потребуется для достижения предстоящих целей. Кроме того, предприятия не могли должным образом планировать исследовательские проекты из-за проблем с распределением ресурсов и прогнозированием.

В 1970-х годах предприятия полагались на формулы планирования как часть своей общей стратегии. Многие бизнес-менеджеры испытывали трудности с распределением ресурсов между различными товарными группами. Они обратились к консультантам за рекомендациями, основанными на формулах планирования. Эти формулы обычно выводились из академических теорий, а не из практических приложений. Следовательно, их результаты оказались неубедительными.

Из-за подхода 1970-х годов к теории маркетинга потребность в изменениях в 1980-х и 1990-х годах привела к созданию новых методов мышления, таких как стратегическое мышление. Этот подход фокусируется на личных потребностях и желаниях, а также на творчестве и гибкости, чтобы получить преимущество над конкурентами. Компании, обладающие конкурентным преимуществом, предлагают продукцию более высокого качества по более низким ценам и получают лучшие рекламные акции, чем их конкуренты. Конкурентное преимущество также включает в себя все другие элементы стратегического мышления, такие как гибкость, креативность и удовлетворенность клиентов. Преимущество дает компаниям преимущество перед конкурентами и определяет их способность получать больше прибыли, чем любая другая компания в отрасли.

Официальные организационные должности или титулы не имеют отношения к разработке маркетинговой стратегии. Вместо этого

маркетинговые стратегии возникают в результате процессов принятия решений руководителями компаний, менеджерами по маркетингу и другими соответствующими лицами, принимающими решения. Они не обязательно относятся к целям или характеру организации. Тем не менее, разработка маркетинговой стратегии требует рассмотрения продуктов или рынков, даже если она не предполагает сознательного принятия решений кем-то с официальным титулом.

Маркетинговая стратегия компании — это набор методов, разработанных маркетологом для достижения желаемых результатов на рынке. Эти методы определяют целевой рынок компании, а также соответствующий маркетинговый комплекс, используемый на этом рынке. Разработка маркетинговой стратегии также означает поиск привлекательных возможностей и планирование способов их использования — это поиск возможностей и планирование способов их использования.

Список использованных источников:

1. Дударь В. С. Разработка маркетинговой стратегии компании / В. С. Дударь // Экономика, управление, финансы: материалы VIII Междунар. науч. конф. – Краснодар: Новация, 2018. – С. 114-116.

2. Калугина А. М. Разработка маркетинговой стратегии и ее роль в компании / А. М. Калугина // Международный студенческий научный вестник. – 2016. – № 4-4. – URL: http://eduherald.ru/ru/article/view?id=16353

3. Томпсон А. А. Стратегический менеджмент. Искусство разработки и реализации стратегии / А. А. Томпсон, А. Дж. Стрикленд. – Пер. с англ. – М. Юнити, 2018. – 576 с.

5. Уткин Э. А. Маркетинг / под ред. проф. Э. А. Уткина. – М.: Ассоциация авторов и издателей "Тандем"; Изд. ЭКМОС, 2018. – 320 с.

Завгородный А. В.

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

СРЕДСТВА ПРИВЛЕЧЕНИЯ И МОТИВАЦИИ СОТРУДНИКОВ В СОВРЕМЕННЫХ IT КОМПАНИЯХ

В современных IT компаниях используется множество средств привлечения и мотивации сотрудников. Некоторые из них включают в себя:

1. Конкурентная зарплата и бонусы: один из наиболее распространенных способов мотивации сотрудников - это предоставление конкурентной зарплаты и бонусов за достижение целей. Это может включать в себя годовые премии, бонусы за выдающуюся работу и дополнительные выплаты в зависимости от результатов проектов.

2. Гибкий график работы и возможность удаленной работы: для многих работников в IT сфере важна гибкость графика работы и возможность работать удаленно. Это может включать в себя разрешение на работу в нерабочие дни, возможность работать из дома или других мест, а также гибкость в выборе рабочих часов.

3. Карьерный рост: IT компании часто предоставляют своим сотрудникам возможность развиваться и продвигаться по карьерной лестнице. Это может включать в себя перспективы повышения, возможности обучения и повышения квалификации, а также возможность работать в разных областях и на разных проектах.

4. Поддержка для баланса работы и личной жизни: многие IT компании также обеспечивают своих сотрудников поддержкой в балансировании работы и личной жизни. Это может включать в себя оплачиваемые отпуска, больничные и дополнительные выходные дни, а также поддержку для семей и детей.

5. Интересные проекты: многие IT компании стараются предоставлять своим сотрудникам интересные проекты и задачи, которые вызывают у них восторг и мотивируют на достижение результатов.

6. Разнообразные мероприятия: зачастую IT компании организуют разнообразные мероприятия и мероприятия социальной направленности, которые помогают укреплять командный дух и мотивировать сотрудников.

Все эти средства привлечения и мотивации могут быть использованы для удержания талантливых работников в IT компаниях. Примеры как

различные IT компании используют средства привлечения и мотивации своих сотрудников:

1. Google: Google широко известен своими высокими зарплатами и бонусами для своих сотрудников, а также своей корпоративной культурой. В компании есть много различных программ мотивации, включая игровые комнаты, спортивные площадки, массажные кресла и питание на рабочем месте. Кроме того, Google предоставляет своим сотрудникам возможность участвовать в проектах, которые они находят наиболее интересными, и предоставляет различные программы обучения.

2. Microsoft: Microsoft предоставляет своим сотрудникам гибкий график работы и возможность работать удаленно. Они также обеспечивают своих сотрудников оплачиваемыми отпусками, бонусами и акциями компании. Компания также проводит множество мероприятий для укрепления командного духа и мотивации сотрудников, таких как корпоративные соревнования, спортивные мероприятия и тимбилдинг.

3. Facebook: Facebook предоставляет своим сотрудникам высококвалифицированных поваров на рабочем месте, гибкий график работы и возможность работать удаленно. Они также предоставляют своим сотрудникам многочисленные программы обучения и развития, а также оплачиваемые отпуска и бонусы за достижения. Кроме того, Facebook организует множество мероприятий для укрепления командного духа, такие как тимбилдинг, спортивные мероприятия и социальные встречи.

Украинские IT компании активно используют различные средства привлечения и мотивации сотрудников, некоторые из них включают:

1. Высокие зарплаты и бонусы: многие украинские IT компании предлагают своим сотрудникам высокие зарплаты и бонусы, чтобы привлечь и удержать талантливых специалистов.

2. Гибкий график работы и удаленная работа: многие компании позволяют своим сотрудникам работать в гибком графике и/или удаленно (это особенно было актуально во времена COVID-19), что позволяет им сохранять баланс между работой и личной жизнью.

3. Обучение и развитие: компании предоставляют своим сотрудникам возможности для обучения и развития своих навыков и квалификации, такие как обучение английскому языку, программы наставничества и обучения новым технологиям.

4. Корпоративная культура: многие компании имеют сильную корпоративную культуру, которая включает в себя различные мероприятия, такие как тимбилдинг, спортивные мероприятия, социальные мероприятия и праздники.

5. Дополнительные льготы: многие компании предоставляют дополнительные льготы, такие как медицинскую страховку, оплачиваемые отпуска, вкусное питание, фитнес-клубы и другие.

Существует множество украинских IT компаний, которые применяют различные методы привлечения и мотивации своих сотрудников. Некоторые примеры:

1. EPAM Systems - компания, которая входит в число крупнейших IT-аутсорсеров в мире, предлагает сотрудникам множество возможностей для развития и профессионального роста, таких как обучение, тренинги, сертификация и возможности перевода в другие страны. Кроме того, EPAM Systems предоставляет гибкий график работы, возможности для удаленной работы и другие бенефиты.

2. Grammarly - компания, разрабатывающая популярный инструмент для проверки грамматики и орфографии, предлагает своим сотрудникам гибкий график работы, страхование, оплачиваемый отпуск, тренинги и курсы повышения квалификации. Кроме того, Grammarly организует внутренние мероприятия для укрепления команды и повышения мотивации.

3. MacPaw - компания, разрабатывающая софт для Mac, предлагает своим сотрудникам обучение, тренинги, конференции и другие мероприятия для профессионального роста, а также гибкий график работы, страхование, бесплатные обеды и многое другое. MacPaw также имеет собственный фонд, который поддерживает социальные и культурные проекты, в которых могут участвовать сотрудники. Еще один инструмент мотивации сотрудников и их удержания в компании - MacPaw village . MacPaw Village - это жилой комплекс для сотрудников компании MacPaw в Киеве, который предоставляет сотрудникам уникальное жилищное пространство вместе с множеством дополнительных удобств, таких как кинотеатр, спортивный зал, игровые зоны, лаундж-бар, общественные места для работы и отдыха.

MacPaw Village может рассматриваться как один из способов мотивации сотрудников и их удержания в компании. Этот проект позволяет сотрудникам жить в непосредственной близости от работы и общаться друг с другом вне рабочего места, создавая более тесную и дружественную рабочую среду. Кроме того, жилье в MacPaw Village предоставляется сотрудникам по более низкой цене, чем рыночная, что также является стимулом для сотрудников оставаться в компании.

Такой подход к мотивации сотрудников имеет свои преимущества, такие как повышение удовлетворенности сотрудников отношениями на работе и повышение их лояльности к компании. Однако, такой подход также

может иметь некоторые недостатки, например, некоторые сотрудники могут считать, что жить рядом с работой может нарушить их личную жизнь.

В целом, MacPaw Village - это интересный пример инновационного подхода к мотивации сотрудников и удержанию их в компании, который может быть полезен для других IT компаний, которые хотят улучшить свою культуру и привлекательность для талантливых сотрудников.

Список использованных источников:

1. Лучшие способы мотивации сотрудников в IT-компаниях мира и Украины. URL: https://deveducation.com/blog/luchshie-ofisnye-plyushki-dlya-it-spetsialistov

(дата обращения 13.03.2023).

2. «Сподіваюся, що кейс MacPaw стане прецедентом». Олександр Косован поділився своєю версією подій, що призвели до обшуків. URL: https://dou.ua/lenta/news/macpaw-searches-kosovan/ ?from=fb-repost&fbclid=IwAR0oUgHjs7QZ9UNLvHXmHSZma2XXWcPy678ERJVjOH6TDCKEhfnfr WUIFf0

(дата обращения 13.03.2023).

Золотаренко А. О.

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

НЕМАТЕРІАЛЬНА МОТИВАЦІЯ СПІВРОБІТНИКІВ ІТ КОМПАНІЇ

В сучасному світі стало звичним вважати, що головна мотивація працівників полягає в заробітній платі та матеріальних благах. Однак, це не так, особливо у високотехнологічних компаніяхс фери ІТ-технологій. Точніше це не єдиний фактор, який впливає на мотивацію працівників. Нематеріальні стимули також відіграють важливу роль у стимулюванні працівників до досягнення високих результатів.

У цій доповіді ми розглянемо питання нематеріальної мотивації співробітників ІТ-компаній та її вплив на ефективність роботи колективу. Ми дослідимо такі аспекти, як соціальні та психологічні стимули, можливості розвитку та самореалізації, задоволення від роботи та багато іншого.

Для досягнення мети дослідження ми провели опитування серед співробітників ІТ-компаній та проаналізували результати. Ми також досліджували підходи, які застосовують кращі ІТ-компанії світу у питанні мотивації своїх працівників.

Ця доповідь стане корисною для керівників ІТ-компаній, які бажають підвищити ефективність роботи свого колективу. Ми надамо практичні рекомендації щодо використання нематеріальних стимулів для мотивації працівників та підвищення їхньої задоволеності від роботи.

Теоретичні аспекти нематеріальної мотивації співробітників ІТ компанії

У сучасних ІТ компаніях, де популярні гнучкі робочі години та віддалена робота, нематеріальні стимули можуть стати дуже ефективним інструментом мотивації співробітників. Нематеріальні стимули можуть бути різного характеру, включаючи визнання, можливості розвитку, відчуття значимості та гнучкості. Ррозглянемо теоретичні аспекти нематеріальної мотивації співробітників ІТ компанії.

Визнання – один з ключових аспектів нематеріальної мотивації. Коли співробітники отримують визнання за свою роботу, вони почуваються більш задоволеними своєю роботою та більш зв'язаними з компанією. Це можна забезпечити через різні форми визнання, такі як відзнаки, подяки та премії. Відзнаки можуть бути формальними, такими як сертифікати та дипломи, або

неформальними, такими як вітання від менеджера або колеги. Подяки та премії можуть бути фінансовими або нефінансовими. Наприклад, компанія може запропонувати подарунки або додаткові вихідні дні замість фінансової винагороди.

Можливость розвитку – ще один важливий аспект нематеріальної мотивації співробітників. Більшість людей бажає розвиватися та вдосконалюватися в своїй професійній діяльності. Якщо компанія надає співробітникам можливості розвитку, такі як навчання та тренінги, вони можуть відчувати більшу мотивацію та зв'язок з компанією.

Відчуття значимості – багато співробітників відчувають більшу мотивацію, коли вони відчувають, що їхній внесок важливий для компанії. Керівники можуть забезпечити це, надаючи співробітникам змогу взяти участь у важливих проектах, а також вислуховуючи їхні ідеї та пропозиції щодо роботи компанії.

Гнучкість – в світі IT гнучкі робочі години та віддалена робота є все більш популярними. Більшість співробітників цінують можливість працювати з дому, мати гнучкий графік та здійснювати перерви на відпочинок. Якщо компанія може забезпечити ці умови, співробітники можуть бути більш задоволені своєю роботою та більш зв'язаними з компанією.

Культура компанії – культура компанії може мати великий вплив на мотивацію співробітників. Якщо компанія має позитивну та підтримувальну культуру, співробітники можуть відчувати більшу мотивацію та зв'язок з компанією. Крім того, якщо компанія має міцну місію та цінності, співробітники можуть бути більш мотивованими робити свою роботу, оскільки вони розуміють, як вона сприяє досягненню цих цілей.

Цінноссті – є трендом останнього дисятиліття що впливає на вмотивованість співробітників в сфері IT. Головною ідеєю є те, що у випадку якщо компанія декларує цінності що резонують із світоглядом співробітника, то це неабияк впливає на його робочий поенціал.

У високотехнологічних компаніях, особливо в IT сфері, нематеріальні аспекти мотивації можуть мати велике значення для приваблення та збереження талантів. Визнання, можливості розвитку, відчуття значимості, гнучкість та культура компанії - це всі аспекти, які можуть впливати на мотивацію співробітників та їхнє задоволення роботою. Керівники компаній повинні приділяти увагу цим аспектам, якщо вони бажають створити позитивну та продуктивну робочу атмосферу, що приведе до успіху компанії.

Огляд практик використання нематеріальної мотивації в IT компаніях

Розмаїття практик використання нематеріальної мотивації в IT компаніях свідчить про те, що ці компанії все більше усвідомлюють важливість цих аспектів для залучення та утримання талантів.

Одним з прикладів є впровадження гнучких робочих годин. Багато IT компаній дозволяють своїм співробітникам працювати з будь-якого місця та в будь-який час, дотримуючись лише термінових дедлайнів. Це забезпечує більшу робочу свободу та зручність для співробітників, що може бути важливим аспектом нематеріальної мотивації.

Іншим прикладом є впровадження програм підтримки розвитку кар'єри. Багато IT компаній надають своїм співробітникам можливості участі в тренінгах, семінарах та конференціях з метою розвитку їхніх навичок та знань. Компанії також можуть пропонувати можливості переходу на більш високі посади або зміну ролі в команді залежно від потреб та бажань співробітників.

Додатково, деякі IT компанії ставлять перед собою завдання створення культури компанії, що підтримує та надихає співробітників. Це може включати такі аспекти, як спільні заходи та відпочинок, відзначення досягнень та успіхів команди, а також заохочення творчості та інновацій у роботі.

Також чимало компаній які періодично заміряють пореби співробітників, та їх настрій для аналітики і подальшого впровадження ряду активностей із покращення умов праці, продуктивності, проактивності команди та коммунікацій в її середені.

Отже, використання нематеріальної мотивації в IT компаніях може включати різноманітні практики, які допомагають залучати таланти та зберігати їх у компанії.

Ефективність використання нематеріальної мотивації у збільшенні задоволеності роботою та продуктивності співробітників

Ефективність використання нематеріальної мотивації у збільшенні задоволеності роботою та продуктивності співробітників в IT компаніях була досліджена в багато разів. Результати цих досліджень свідчать про те, що використання нематеріальної мотивації може допомогти збільшити задоволеність роботою та продуктивність співробітників.

Один з ключових аспектів нематеріальної мотивації є можливості для розвитку кар'єри та навчання нових навичок. Дослідження показали, що співробітники, які мають можливість розвиватись та навчатись, є більш задоволені своєю роботою та продуктивніші. Більшість IT компаній надають

своїм співробітникам можливості проходження тренінгів, курсів та сертифікацій, що дозволяє їм розвиватись та збільшувати свої професійні навички.

Іншим важливим аспектом нематеріальної мотивації є робоче середовище та співпраця в команді. Компанії, які створюють комфортні умови для роботи та надають можливості для співпраці та взаємодії між співробітниками, можуть збільшувати задоволеність роботою та продуктивність своїх співробітників.

Крім того, заохочення творчості та інновацій у роботі також може допомогти збільшити задоволеність роботою та продуктивність.

Рекомендації щодо використання нематеріальної мотивації у практичній діяльності IT компанії

Оскільки нематеріальна мотивація може бути ефективним інструментом для збільшення задоволеності роботою та продуктивності співробітників у сфері IT, нижче наведено кілька рекомендацій для використання цього підходу в практичній діяльності компанії.

1. Створення відкритого середовища.

Надання можливості висловлювати свої думки та ідеї, обговорювати проблеми та шукати рішення, сприяє формуванню відчуття власної важливості співробітника. Це в свою чергу допомагає підвищувати мотивацію до виконання роботи та створює сприятливу атмосферу для досягнення успіху компанією.

2. Надання можливості для саморозвитку.

Надання співробітникам можливості брати участь у навчальних програмах, відвідувати конференції та семінари, стажуватися в інших компаніях тощо, допомагає їм розвиватися та покращувати свої професійні навички. Це знову ж таки сприяє підвищенню мотивації до виконання роботи, а також допомагає компанії зберегти та підвищити рівень професійної кваліфікації своїх працівників.

3. Визнання досягнень та успіхів.

Визнання та похвала за досягнення та успіхи в роботі є важливим елементом нематеріальної мотивації. Для багатьох працівників це є однією з головних причин їхньої мотивації до роботи. Відчуття, що їхні досягнення відомі і цінуються керівництвом та колегами, додає самовпевненості, розширює можливості для збільшення продуктивності та прискорює процес досягнення поставлених цілей.

Щоб використовувати визнання як інструмент мотивації, керівництво IT компанії може вживати наступні практики:

- відзначати досягнення співробітників: це може бути привітання в робочій групі, відзнака на спеціальній дошці або в робочій пошті;
- надавати можливість виступати на зборах, презентувати свої досягнення та успіхи: це допоможе підвищити самооцінку та заохотити до подальших досягнень;
- розробляти програми нагородження та стимулювання працівників, наприклад: програми преміювання за досягнення певних цілей, надання вихідних за виконання особливо складних проектів або привілеїв для тих, хто показує найкращі результати;
- залучати співробітників до процесу розробки та виконання проектів, враховуючи їхні здібності та бажання: це збільшує мотивацію та стимулює до досягнення якісних та кількісних цілей.

У висновку до доповіді про аспекти нематеріальної мотивації співробітників ІТ компанії можна сказати, що такий вид мотивації включає широкий спектр факторів, які можуть впливати на задоволеність роботою та продуктивність співробітників. Дослідження показують, що нематеріальна мотивація може бути навіть ефективнішою, ніж матеріальна, оскільки співробітники оцінюють не тільки фінансові аспекти своєї роботи, але й інші не менш важливі фактори, такі як визнання, можливість розвитку, робоче середовище та багато інших.

У зв'язку з цим, підприємства, які бажають підвищити продуктивність та задоволеність своїх співробітників, повинні приділяти увагу нематеріальним факторам мотивації. Зокрема, важливо визнавати досягнення та успіхи співробітників, забезпечувати можливості розвитку та навчання, створювати комфортне та затишне робоче середовище.

Однак, важливо пам'ятати, що кожна компанія має свої особливості та потреби, тому перед застосуванням нематеріальної мотивації необхідно провести аналіз ситуації та врахувати індивідуальні особливості співробітників. Тільки таким чином можна забезпечити ефективне використання нематеріальної мотивації та досягти поставлених цілей.

Список використаних джерел:

1. Н. Болкавалзе, Т. Гетьман (2020). Сучасні методи мотивацій ІТ компаній. Економічний журнал Європейського Економічного Університету ім. Л. Українки, 2(22):72-82

2. С. Дімітрієва. (2018). Мотиваційна політика сучасних ІТ-компаній: теоретичний аспект. Економічний простір, (138), 107-115.

3. Попель, М. В. (2019). Фактори та інструменти мотивації працівників високотехнологічних компаній. Економіка і організація управління, (2 (36)), 114-123.

4. Дімітрієва, С. Д. (2011). Шляхи підвищення мотивації персоналу. Економічний часопис-XXI, № 216. — С. 46-49

5. Е. Браун, (2020). www.sitepronews.com. The Non-Material Motivation of Staff – How to Motivate Staff If There Is No Money.

6. Мельник, Ю. В. (2017). Оцінка впливу мотивації на результативність праці ІТ-спеціалістів. Економіка і організація управління, (1 (25)), 90-98.

7. Кук Д., Руммель Я., (2015). Sec. Cognitive Neuroscience. Toward an understanding of motivational influences on prospective memory using value-added intentions.

Золотько Д. А.

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

МАРКЕТИНГОВЫЕ ИССЛЕДОВАНИЯ

Маркетинговые исследования необходимы предприятию для продуктивной деятельности и конкурентной борьбы на рынке.

Осуществление комплекса маркетинга 4P (Product, Price, Promotion, Place), невозможно без владения информацией о рынке, товаре, конкурентах и покупателях, поэтому самым важным звеном, которое можно поставить на первое место, это маркетинговые исследования.

Маркетинговые исследования осуществляются фирмой для того, чтобы владеть внутренней информацией, информацией о рынке, чтобы планировать свою деятельность в соответствии с запросами и интересами рынка.

Суть проведения маркетинговых исследований – сбора маркетинговой информации, можно выразить фразой: «Информация - это всё, информация - это деньги и владение информацией - это владение миром». Информация для маркетинга означает очень многое. Она позволяет планировать маркетинговые мероприятия; осуществлять комплекс маркетинга и выбирать наиболее эффективные маркетинговые мероприятия или рекомендации для конкретного исполнителя, а также оценивать их эффективность.

В отдельных случаях сбор маркетинговой информации выступает как формальный процесс, который нужен для того, чтобы сконцентрировать внимание на тех или иных моментах, в других же случаях сбор маркетинговой информации – это очень сложный длительный специально планируемый процесс, который должен быть чётко определён по этапам, по срокам, по исполнителям и по денежным затратам, которые несёт предприятие по проведению маркетинговых исследований.

Эффективное маркетинговое исследование включает пять этапов.

На первом этапе проведения маркетинговых исследований необходимо определить цели исследования, задачи и проблемы, стоящие перед бизнесом.

Второй этап – разработка плана сбора информации с использованием первичных и вторичных данных. Сбор первичных данных требует выбора методов исследования (наблюдение, эксперимент, опрос), подготовки инструментов исследования (анкеты, механические устройства), составления плана выборки (единица выборки, объем выборки, процедура выборки) и выбора способа связи с аудиторией (телефон, почта, личное интервью).

Третий этап – сбор информации для решения поставленных задач. Информация должна быть собрана скрупулезно, правильно, с соблюдением всех алгоритмов и требований. Недостоверная, ошибочная, неполная информация может привести к неверным выводам и к неправильным решениям. Минимальные потери от этого – потраченное зря время и деньги, но часто это приводит к негативным последствиям для развития всего бизнеса.

Четвертый этап – подготовка данных к анализу и непосредственно сам анализ собранных данных. В процессе анализа полученные данные группируются, объединяются, усредняются, на их основе формируются сводные показатели.

Пятый этап – представление отчета о результатах проведенных исследований с соответствующими выводами и рекомендациями о принятии более правильных решений.

Маркетинговые исследования разделяются на группы по различным направлениям и целям:

1. По назначению:

- разведочные – для сбора предварительной информации о рынке, в том числе при разработке стратегического плана;
- описательные – количественные исследования рынка, которые позволяют получить цифровую информацию о рынке, его состоянии и тенденциях развития. В ходе описательных исследований удается получить ответ на вопросы, начинающиеся со слов «кто? что? где? когда? и как?»;
- казуальные – уточняющие исследования для получения дополнительной информации, в том числе о конкретном предмете исследования. Дают ответ на вопрос «почему?».

2. По виду информации:

- количественные;
- качественные.

3. По рынкам:

- внешние проводятся для получения маркетинговой информации о рынке, в том числе дальнего и ближнего окружения;
- внутренние – исследования состояния бизнеса на основе внутренней информации (статистической и бухгалтерской отчетности предприятия).

4. По месту проведения:

- кабинетные проводятся на основе ранее собранной информации;
- полевые – сбор первичной информации непосредственно на рынке.

5. По новизне информации:

- первичные – исследования по сбору новой информации;

▪вторичные – проводятся на основе собранной информации в кабинетном варианте.

Перечисленные виды и методы исследований не используются отдельно. Проведение маркетингового исследования зависит от того, насколько правильно маркетологи смогут подобрать комплекс необходимых методов, даже не соблюдая указанную последовательность.

После проведения маркетингового исследования и реализации полученных маркетинговых решений необходим мониторинг, который покажет, какое влияние оказало маркетинговое исследование на положение продукта на рынке, получен ли ожидаемый результат. Маркетингового исследования это не материальные ценности, которые можно зачислить в активы предприятия, а информация, способная дать реальный экономический эффект от использования активов в перспективе.

В качестве примера проведения маркетинговых исследований можно привести выведение нового товара на рынок. В случае, если предприятие планирует вывести на рынок новый товар, то без знания специфики рынка, без знания платёжеспособности покупателей или его предпочтений, без знания конкурентной силы предприятий, которые уже работают на рынке и без знания ёмкости и возможности развития рынка, фактически осуществить деятельность по выведению товара на рынок невозможно.

При появлении товара - новинки на рынке мы должны узнать, каково будет отношение покупателя к этому товару, в этом случае очень часто проводятся так называемые пробные продажи и в результате собирается информация по восприятию покупателя этого товара, выводимого на рынок.

Таким образом, для ведения успешного бизнеса необходимо проводить маркетинговые исследования с целью получения ответов на вопросы относительно текущей рыночной ситуации, покупательского спроса и понимания необходимости создания нового продукта, который будет соответствовать ожиданиям потребителей.

Список использованных источников:

1. *Котлер, Филип Основы маркетинга. Краткий курс. Киев, 2007. 656с.*
2. *Катаев А. В. Маркетинговые исследования. Модуль «теория маркетинговых исследований». ХТЭИ КНТЭУ, 2014. – 46 с.*

Коваленко В. В.

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

ПРИМЕНЕНИЕ МЕТОДОВ SWOT-АНАЛИЗА, PESTLE-АНАЛИЗА, АНАЛИЗА ПОРТФЕЛЯ ПРОДУКТОВ И АНАЛИЗА КОНКУРЕНТОВ ДЛЯ ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ IT-КОМПАНИЙ

В современном мире IT-компании являются одними из самых динамично развивающихся отраслей экономики. Конкуренция в этой сфере невероятно высока, и компании должны постоянно совершенствоваться, чтобы сохранить свою конкурентоспособность. Для достижения этой цели многие IT-компании применяют различные аналитические методы, такие как SWOT-анализ, PESTLE-анализ, анализ портфеля продуктов, анализ цепочки поставок и анализ конкурентов. Применение этих методов может помочь IT-компаниям повысить свою конкурентоспособность.

SWOT-анализ (анализ сильных и слабых сторон, возможностей и угроз) – это метод анализа бизнеса, который позволяет оценить текущее положение компании и определить ее потенциальные возможности и угрозы.

SWOT-анализ помогает IT-компаниям выявить свои сильные и слабые стороны, чтобы использовать их в свою пользу и улучшить недостатки. В результате SWOT-анализа компания может разработать стратегию, которая позволит ей максимально использовать свои сильные стороны, устранить слабости, использовать возможности и уменьшить риски.

PESTLE-анализ – это метод анализа внешней среды, который позволяет IT-компаниям оценить влияние политических, экономических, социальных, технологических, экологических и юридических факторов на свой бизнес.

PESTLE-анализ помогает компаниям понять, какие изменения во внешней среде могут повлиять на их бизнес и как они могут адаптироваться к этим изменениям. Результатом PESTLE-анализа является список факторов, которые могут влиять на бизнес компании, и план действий, который поможет компании преодолеть эти факторы.

Анализ портфеля продуктов – это метод анализа, который позволяет IT-компаниям оценить свой текущий портфель продуктов и выявить продукты, которые приносят наибольшую прибыль, а также продукты, которые не приносят достаточно высокой прибыли или могут быть

улучшены. Анализ портфеля продуктов помогает IT-компаниям принимать решения о развитии новых продуктов, улучшении существующих и отказе от продуктов, которые не являются прибыльными.

Анализ конкурентов – это метод анализа, который позволяет IT-компаниям оценить своих конкурентов, их сильные и слабые стороны, а также их стратегии развития. Анализ конкурентов помогает компаниям понять, какие стратегии успешно используются на рынке, и использовать эти знания для разработки собственных стратегий. Результатом анализа конкурентов является понимание того, как компания может улучшить свою конкурентоспособность, чтобы привлечь больше клиентов и увеличить свою прибыль.

IT-компании должны постоянно совершенствоваться и использовать различные методы анализа, чтобы повысить свою конкурентоспособность.

SWOT-анализ, PESTLE-анализ, анализ портфеля продуктов и анализ конкурентов помогают компаниям определить свои сильные и слабые стороны, оценить внешнюю среду, оптимизировать производственный процесс и понять конкурентов. Результатом использования этих методов является разработка эффективной стратегии, которая позволит компании быть более успешной на рынке и привлекать больше клиентов.

Однако, важно понимать, что анализы не являются универсальным решением для всех проблем компании и не гарантируют успеха. Компании должны также учитывать свою специфику и особенности рынка, на котором они работают, чтобы принимать решения, которые наиболее подходят для них.

Кроме того, важно не ограничиваться только одним анализом, а использовать их в комбинации друг с другом. Например, SWOT-анализ может помочь определить сильные и слабые стороны компании, а PESTLE-анализ позволит оценить внешние факторы, которые могут повлиять на бизнес компании. Анализ конкурентов позволит узнать о стратегиях, которые используются на рынке, а анализ портфеля продуктов – понять, какие продукты компании приносят наибольшую прибыль.

В целом, применение методов анализа, таких как SWOT-анализ, PESTLE-анализ, анализ портфеля продуктов, анализ цепочки поставок и анализ конкурентов, является важным инструментом для повышения конкурентоспособности IT-компаний. Однако, успешность компании зависит не только от использования этих методов, но и от того, как компания использует полученные знания и как она адаптируется к изменяющимся условиям рынка. Кроме того, применение этих методов анализа позволяет компаниям выявить проблемные зоны и возможности для улучшения,

определить ключевые цели и приоритеты, разработать стратегии для их достижения и оценить эффективность принятых мер.

SWOT-анализ позволяет оценить внутренние сильные и слабые стороны компании, а также внешние возможности и угрозы. На основе этих данных компания может разработать стратегию для использования своих преимуществ и уменьшения угроз, а также для улучшения слабых сторон.

PESTLE-анализ позволяет компании оценить внешнюю среду, включая политические, экономические, социальные, технологические, юридические и экологические факторы, которые могут повлиять на бизнес компании. Этот анализ помогает компании понять текущие и будущие тенденции в отрасли и адаптироваться к ним. Анализ портфеля продуктов позволяет компании оценить производственный портфель, определить продукты, приносящие наибольшую прибыль, и решить, какие продукты следует развивать, а какие – убирать. Анализ конкурентов позволяет компании оценить своих конкурентов, их стратегии и позицию на рынке. На основе этой информации компания может разработать свою собственную стратегию, учитывая конкурентное окружение.

В целом, использование методов анализа является важным шагом для повышения конкурентоспособности IT-компаний. Компании могут использовать эти методы, чтобы определить свои сильные и слабые стороны, а также оценить текущую ситуацию на рынке и определить возможности для улучшения. Это позволит компании разработать более эффективную стратегию и достичь большего успеха в своем бизнесе.

Помимо вышеперечисленных методов анализа, существуют и другие методы, которые могут быть полезны для повышения конкурентоспособности IT-компаний. Например, анализ потребностей клиентов может помочь компании понять, какие услуги и продукты наиболее востребованы клиентами, и насколько хорошо компания удовлетворяет эти потребности. На основе этой информации компания может разработать новые продукты и услуги, а также улучшить свою клиентскую поддержку.

Анализ рисков поможет компании оценить риски, связанные с ее бизнесом, и разработать планы по уменьшению этих рисков. Это может включать разработку системы резервного копирования данных, разработку плана действий в случае отказа системы или нарушения безопасности, а также анализ рисков, связанных с финансовыми инвестициями.

Анализ требований кадров может помочь компании понять, какие навыки и квалификации необходимы ее сотрудникам, и какие программы обучения и развития могут помочь развить эти навыки. Это может также

включать анализ текущего уровня удовлетворенности сотрудников и разработку программ по мотивации и удержанию сотрудников.

В заключение, использование различных методов анализа позволяет IT-компаниям получить полное представление о своем бизнесе и о том, как они могут улучшить свою конкурентоспособность. Комбинация нескольких методов анализа может обеспечить компании наиболее полную информацию и помочь ей разработать стратегию, которая будет наиболее эффективной для достижения ее целей.

Кроме того, важно учитывать изменения в отрасли, в которой работает компания. Технологические изменения, политические и экономические факторы могут влиять на бизнес-планы и стратегии компании. Поэтому, помимо анализа SWOT и PESTLE, также может быть полезно проводить регулярные обзоры трендов и изменений в отрасли. Это может помочь компании адаптироваться к изменяющейся среде и сохранять свою конкурентоспособность. Важным аспектом при использовании методов анализа является правильное использование полученной информации.

Результаты анализа должны быть применены для разработки конкретных действий и стратегий, направленных на улучшение конкурентоспособности компании. Эти действия могут включать разработку новых продуктов и услуг, повышение качества обслуживания клиентов, оптимизацию процессов, улучшение маркетинговых стратегий и другие.

В целом, использование методов анализа, таких как SWOT, PESTLE, анализ портфеля продуктов и анализ конкурентов, является необходимым для повышения конкурентоспособности IT-компаний. Однако важно помнить, что анализ должен быть регулярным и непрерывным, чтобы компания могла адаптироваться к изменяющейся среде и сохранять свою конкурентоспособность на долгосрочной основе. Кроме того, при использовании методов анализа необходимо учитывать контекст и специфику каждой компании. Например, анализ цепочки поставок может быть более важен для компании, занимающейся производством товаров, чем для компании, которая предоставляет услуги. Аналогично, анализ портфеля продуктов может быть более важен для компании, занимающейся разработкой ПО, чем для компании, которая предоставляет IT-услуги.

Также важно учитывать, что анализы не должны рассматриваться как изолированные процессы. Каждый метод анализа должен использоваться в контексте других методов и инструментов, чтобы обеспечить полное и точное понимание ситуации компании и ее конкурентов.

Важно отметить, что проведение анализов необходимо не только для выявления сильных и слабых сторон компании, но и для поиска возможностей и угроз, с которыми она может столкнуться в будущем.

Отслеживание трендов и изменений в отрасли поможет компании предсказать возможные изменения и подготовиться к ним заранее. Кроме того, компании должны также учитывать мнение своих клиентов и рынка в целом. Регулярное проведение опросов и сбор обратной связи помогут компании понимать потребности своих клиентов и принимать решения, которые отвечают этим потребностям.

В заключение, методы анализа, такие как SWOT, PESTLE, анализ портфеля продуктов и анализ конкурентов, могут помочь IT-компаниям повысить свою конкурентоспособность. Однако эти методы должны использоваться в контексте ситуации каждой компании и должны быть регулярно обновляться и применяться для разработки конкретных действий и стратегий. Только таким образом компании смогут сохранять свою конкурентоспособность и успешно развиваться в изменчивой IT-отрасли.

Список использованных источников:

1. *Бахтин, В. М. (2015). Анализ конкурентов. М.: Экономика.*
2. *Голубев, В. И. (2016). Конкуренция: теория и практика. М.: Финансы и статистика.*
3. *Котлер, Ф. (2018). Маркетинговые исследования. М.: Дело.*
4. *Рамашковский, Ю. М. (2016). Конкурентный анализ: методы и приложения. М.: Издательский дом "Дело".*
5. *Хохлова, Е. А. Оценка конкурентоспособности IT-компании на основе анализа портфеля продуктов / Е. А. Хохлова, А. А. Хорев //Информационные технологии и управление. - 2018. - № 3. - С. 64-70.*
6. *Кузнецова, Е. В. Методика анализа портфеля продуктов IT-компании / Е. В. Кузнецова, А. А. Карпов // Вестник Казанского технологического университета. - 2019. - Т. 22, № 22. - С. 50-55.*
7. *Петров, А. В. Использование анализа портфеля продуктов для улучшения конкурентоспособности IT-компаний / А. В. Петров // Экономика и управление.*
8. *Porter, M. E. (2008). The five competitive forces that shape strategy. Harvard business review, 86(1), 78-93.*
9. *Thompson, A. A., Peteraf, M. A., Gamble, J. E., & Strickland III, A. J. (2014). Crafting and executing strategy: the quest for competitive advantage: concepts and cases. McGraw-Hill Education.*
10. *Weihrich, H. (1982). The TOWS matrix—a tool for situational analysis. Long range planning, 15(2), 54-66.*
11. *Hill, T., & Westbrook, R. (1997). SWOT analysis: it's time for a product recall. Long range planning, 30(1), 46-52.*
12. *Kotler, P., & Armstrong, G. (2016). Principles of marketing. Pearson Education.*
13. *Lynch, R. (2015). Strategic management. Pearson Education.*
14. *Porter, M. E. (1980). Competitive strategy: Techniques for analyzing industries and competitors. Free Press.*

15. Sharma, A., & Gupta, P. (2019). Impact of PESTLE analysis on organizational decision making: a case study of McDonald's. International Journal of Management, Technology, and Social Sciences (IJMTS), 4(1), 6-19.

16. Grant, R. M. (2016). Contemporary strategy analysis: Text and cases edition. John Wiley & Sons.

17. Hitt, M. A., Ireland, R. D., & Hoskisson, R. E. (2017). Strategic management: Concepts and cases: Competitiveness and globalization. Nelson Education.

18. Johnson, G., Scholes, K., & Whittington, R. (2017). Exploring strategy: Text and cases. Pearson.

19. Wheelen, T. L., Hunger, J. D., Hoffman, A. N., & Bamford, C. E. (2017). Strategic management and business policy: Globalization, innovation, and sustainability. Pearson.

Липовяк Є. Ю.

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

УПРАВЛІННЯ КОМАНДОЮ ТА ЛІДЕРСТВО

Управління проектами передбачає застосування знань, навичок, інструментів і методів управління, а також лідерських здібностей.

Управлінська діяльність спрямована на досягнення цілей проекту, таких як ефективні процеси, чітке планування, координація, моніторинг. Лідерська діяльність спрямована на роботу з людьми. Лідерство включає в себе можливість впливати, мотивувати, слухати, сприяти та інші дії, пов'язані з командою проекту.

Управління та лідерство однаково важливі для досягнення запланованих результатів команди та проекту.

Лідерство повинно практикуватися всіма членами команди проекту. В той час як управління може бути централізованим або розподіленим.

У середовищі, де управлінська діяльність централізована, підзвітність (відповідальність за результат), як правило, покладається на одну особу. До прикладу - це може бути керівник проекту або подібна роль. У таких ситуаціях статут проекту або інший дозвільний документ документ може надати повноваження для керівника проекту на формування команди для досягнення результатів проекту.

В іншому випадку управління проектом розподіляється між командою і члени команди проекту відповідають за виконання роботи. Бувають також ситуації, коли команда проекту може самоорганізуватися для завершення проекту. Замість того, щоб мати визначененого менеджера проекту, хтось із команди проекту може виступати фасилітатором для забезпечення спілкування, співробітництва та залучення членів команди. Ця роль може періодично змінюватися між членами команди проекту.

Лідерство-служіння – це стиль лідерства, який зосереджується на розумінні та вирішенні питань і потреб команди. Основною ціллю є розвиток членів команди проекту, щоб забезпечити найвищу можливу продуктивність команди. Лідери-слуги приділяють особливу увагу розвитку членів команди проекту, щоб вони могли досягти найвищого потенціалу.

Лідери-слуги дозволяють командам проекту самоорганізовуватися, коли це можливо, і підвищувати рівень автономії шляхом передачі

відповідних можливостей прийняття рішень членам команди проекту. Бути лідером-слугою включає:

- **Усунення перешкод.** Оскільки саме проектна команда генерує більшість бізнесу, важливою роллю лідера-слуги є максимізація результатів шляхом усунення перешкод до їх прогресу. Це включає вирішення проблем і усунення перешкод, які можуть перешкоджати роботі команди проекту. Вирішуючи або зменшуючи ці перешкоди, команда може приносити більше користі для бізнесу.
- **Захист від відволікання.** Лідери-слуги захищають команду проекту від внутрішніх і зовнішніх відволікання, які відвертають команду проекту від поточних цілей. Втрата часу знижує продуктивність. Захищаючи команду проекту від некритичних зовнішніх вимог справжній лідер допомагає команді проекту залишатися зосередженою.
- **Можливості заохочення та розвитку.** Лідери-слуги також забезпечують інструменти та заохочення, щоб команда проекту була задоволеною та продуктивною. Навчання мотивує розвиток членів команди проекту як особистостей і знаходить способи винагородити їх за виконану роботу. Це допомагає залишати членів команди проекту задоволеними.

Однією з цілей ефективного лідерства є створення високоефективної команди проекту. Є ряд факторів, які сприяють високій ефективності проектних команд. Наведений нижче список не є вичерпним, але він визначає деякі фактори, пов’язані з високопродуктивними проектними командами.

1. **Відкрите спілкування.** Середовище, яке сприяє відкритому та безпечному спілкуванню дозволяє проводити продуктивні зустрічі, вирішувати проблеми швидше.
2. **Спільне розуміння.** Мета проекту та переваги, які він принесе має бути зрозуміла всім членам проекту.
3. **Спільна власність.** Більше володіння результатами проекту дає можливість відчувати залученість для всієї команди.
4. **Довіра.** Команда проекту, члени якої довіряють один одному, готова піти на додаткові зусилля, щоб досягти успіху.
5. **Співпраця.** Проектні команди, які співпрацюють, а не працюють ізольовано або конкурують, як правило, генерують різноманітніші ідеї та отримують кращі результати.
6. **Адаптивність.** Проектні команди, мають бути здатні адаптувати спосіб роботи до середовища навколо.
7. **Стійкість.** Коли виникають проблеми або збої, високоефективні проектні групи швидше відновлюють продуктивність.

8. **Розширення можливостей.** Члени команди проекту, які відчувають себе уповноваженими приймати рішення щодо того, як вони працюють, є кращими, ніж ті, хто відчувають “мікроменеджмент”.

9. **Визнання.** Проектні команди, які отримали визнання за вкладену роботу та ефективність, яку вони досягли, з більшою ймовірністю продовжуватимуть працювати добре.

В підсумку, лідерські навички корисні для всіх членів команди проекту, незалежно від того, чи працює команда проекту в середовищі з централізованими управлінням чи в середовищі спільного управління.

Список використаних джерел:

1. *Юрген Апелло Менеджмент 3.0. Agile-менеджмент. Лідерство та управління командами., 2019.*
2. *A Guide to the Project Management Body of Knowledge (PMBOK® Guide), PMI, 2021.*
3. *Савельєва В. С. Психологія управління: Навчальний посібник. 2008*

Ложко И. В.

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

ДЕМОТИВАЦИЯ И ЕЁ ВЛИЯНИЕ НА ОТДЕЛ ПРОДАЖ

Глобальные социально-экономические изменения, как в нашей стране, так и во всем мире, провоцирующие стремительные изменения в сфере предпринимательства и различных бизнесов, как основных звеньев экономики страны, выдвинули ряд проблем перед бизнесом, одной из которых стала демотивация персонала.

Особенно остро демотивация сказывается на сотрудниках из отдела продаж, так как отдел продаж - это сердце любого бизнеса, отдел который приносит деньги в компанию и от эффективности работы менеджеров по продажам зависят не только прочие отделы компании но и высшее руководство.

Если уровень мотивации в отделе продаж падает соответсвенно падают продажи и прибыль компании. Демотивация в других отделах компаний сказывается не так критично, как демотивация отдела продаж, поскольку от качества и количества продаж осуществляемых менеджерами зависит доход компании, с полученных доходов компания выплачивает зарплаты всем сотрудникам и всем отделам компании, закупает новые товары, проводит рекламные кампании, оплачивает аренду офисов, производственных помещений и многое другое.

Решение проблемы демотивации внутри отдела продаж и прочих отделов требует особого внимания к процессам демотивации и её предпосылкам.

В настоящее время многие компании сталкиваются с ситуациями когда сотрудники выполняют свои обязанности по инерции, без особого энтузиазма и интереса к своей работе даже не смотря на достойное материальное вознаграждение. Традиционные методы мотивации персонала оказываются неэффективными. Отсутствие должного внимания со стороны руководства к данному явлению в компании неизбежно приведет к потерям финансов и квалифицированных сотрудников.

Во избежание подобной ситуации при первых признаках демотивации необходимо проанализировать сложившуюся ситуацию в коллективе с целью определения возможных источников и причин демотивации сотрудников.

По моему мнению причины демотивации можно разделить на три группы:

К первой группе можно отнести упущения и некомпетентность со стороны компании и руководства в сфере мотивации персонала, неумение либо неправильное применение практических методов стимулирования сотрудников.

Вторая группа причин связана с личностью сотрудника, менеджера по продажам в частности, к причинам демотивации можно отнести социальные установки и положение в обществе, ведущие потребности менеджера, семейное положение и отношения внутри семьи, хроническое утомление, эмоциональное выгорание и многое другое.

Третья группа причин - это изначально не верный подбор персонала и допущения ряда ошибок на этапе подбора и при начале работы нового сотрудника, это занижение требований при приёме на работу, привлечение кандидатов только большой суммой денег, отсутствие программы адаптации новых сотрудников, один шаблон адаптации для всех сотрудников всех отделов и департаментов компании, отсутствие контроля за процессом адаптации сотрудников.

Таким образом, проанализировав все вышесказанное мы можем сделать следующие выводы:

Демотивация очень разрушительное явление внутри компании, особенно в отделе продаж.

Падение уровня мотивации в компании приводит к закономерному падению прибыли, снижению эффективности работы сотрудников и увольнению ценных кадров в дальнейшем.

Причины демотивации можно выделить в основные три группы.

Как и с многими проблемами демотивацию легче всего предотвратить либо побороть данное явление на первоначальных этапах.

Лупаненко А. Ю.

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

ОПЕРАЦИОННЫЙ МЕНЕДЖМЕНТ В СИСТЕМЕ УПРАВЛЕНИЯ ПРЕДПРИЯТИЯ

Операционный менеджмент является важнейшим компонентом системы управления предприятием. Он включает в себя проектирование, выполнение и контроль повседневной деятельности организации с целью достижения эффективности, результативности и постоянного улучшения. В этой статье мы обсудим важность оперативного управления в системе управления предприятием и ключевые принципы, и инструменты, используемые при его реализации.

1. Важность оперативного управления

Операционное управление имеет решающее значение для успеха любой организации, независимо от ее размера, отрасли или рынка. Эффективное операционное управление обеспечивает эффективное использование ресурсов, оптимизацию процессов и удовлетворение потребностей клиентов. Это также помогает организациям адаптироваться к изменяющимся рыночным условиям, технологическим достижениям и ожиданиям клиентов.

Оперативное управление особенно важно в текущей бизнес-среде, которая характеризуется острой конкуренцией, быстро меняющимися потребностями клиентов и растущим давлением в отношении снижения затрат и повышения производительности. В этом контексте операционный менеджмент может предоставить организациям конкурентное преимущество за счет повышения качества продуктов и услуг, сокращения времени выполнения заказов и повышения удовлетворенности клиентов.

2. Принципы операционного управления

Операционный менеджмент основан на наборе принципов, которые определяют разработку, выполнение и контроль организационных процессов. Некоторые из ключевых принципов оперативного управления включают в себя:

2.1 Непрерывное улучшение. Операционное управление направлено на достижение постоянного улучшения путем определения областей для улучшения, внедрения изменений и мониторинга результатов.

2.2 Стандартизация. Включает стандартизацию процессов, процедур и показателей производительности для обеспечения согласованности, и снижения изменчивости.

2.3 Бережливое мышление. Оперативное управление находится под влиянием бережливого мышления, которое включает в себя устранение потерь, сокращение времени выполнения заказов и оптимизацию действий, создающих добавленную стоимость.

2.4 Ориентация на клиента: операционное управление сосредоточено на удовлетворении потребностей и ожиданий клиентов посредством предоставления высококачественных продуктов, и услуг.

3. Инструменты оперативного управления

Операционный менеджмент использует различные инструменты для разработки, выполнения и контроля организационных процессов. Некоторые из ключевых инструментов, используемых в оперативном управлении, включают:

3.1 Картирование процессов. Картирование процессов включает в себя создание визуальных представлений организационных процессов, которые могут помочь определить области для улучшения.

3.2 Статистический контроль процесса: Статистический контроль процесса включает использование статистических методов для мониторинга и контроля изменчивости процесса, а также для определения областей, требующих улучшения.

3.3 Системы управления качеством: Системы управления качеством, такие как ISO 9001, обеспечивают основу для разработки, выполнения и контроля организационных процессов с акцентом на качество и удовлетворенность клиентов.

3.4 Метрики производительности. Метрики производительности, такие как ключевые показатели эффективности (KPI), используются для измерения и мониторинга эффективности организации, а также для определения областей, требующих улучшения.

Оперативный менеджмент является важнейшим компонентом системы управления предприятием, и его важность в современной конкурентной бизнес-среде возрастает. Применяя принципы и инструменты операционного управления, организации могут добиться эффективности, действенности и постоянного улучшения, удовлетворяя при этом потребности и ожидания клиентов. Оперативное управление — это непрерывный процесс, требующий

постоянного внимания и усилий для поддержания и улучшения эффективности организации.

Список использованных источников:

1. *Производственный и операционный менеджмент, 10-е издание: Пер. с англ. — М.: ООО "И.Д. Вильямс", 2008. — 1184 с.*

2. *T. Chang, R. A. Wysk, H. W&ng. Computer-Aided Manufacturing (Upper Saddle Creek, NJ: Prentice Hall, 1997)*

3. *Операционный менеджмент: Учебник для вузов. Стандарт третьего поколения, Издательский дом "Питер", 2010 – 544 с.*

Лучинський Д. В.

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

ЕКОНОМІЧНА ТА МЕДИЧНА ЕФЕКТИВНІСТЬ ВПРОВАДЖЕННЯ НОВИХ ОРГАНІЗАЦІЙНИХ ПІДХОДІВ В РОБОТІ ПРИВАТНОЇ СТОМАТОЛОГІЧНОЇ ПРАКТИКИ В РЕАЛІЯХ ВІЙСЬКОВОГО СТАНУ

Організація роботи стоматологічної практики за останній рік в умовах проведення широкомасштабної війни проти України поставила нові вимоги для ведення бізнесу та прийняття інших управлінських рішень, ніж це вимагалось раніше, в умовах мирного часу. Малий бізнес в Україні в 2022 році працював (та продовжує досі працювати) в умовах невизначеності, ризику бомбардувань, постійних повітряних тривог та тривалих виключень електроенергії після влучань ракетами в елементи критичної інфраструктури.

Навіть локуючись у центрально-західній частині України бізнесам довелося підлаштовувати свої бізнес-процеси під сучасні реалії військового стану та вводити інновації, часом роблячи помилки та виправляючи їх. Всі ці умови впливали на фінансові показники бізнесу та роботу людей. Тому нам важливо було провести аналіз деяких управлінських рішень, що мали успішний результат, а також деяких рішень, які були помилковими, що доводилось швидко виправляти.

Одним із найкритичніших факторів, що впливав на роботу бізнесу були тривалі періоди відключень електроенергії. Це призводило до тривалих простоїв у робочі години та економічних втрат. Також це мало вплив на морально-психологічний стан людей у колективі на робочих місцях, оскільки супроводжувалось відключенням опалення у зимовий період. Тому важливим було не тільки знайти ефективне рішення даної проблеми, а й підтримка морального стану співробітників в періоди, коли рішення ще не було прийнятим, а керівники-менеджери шукали шляхи виходу з критичних ситуацій. В таких умовах доводилося на практиці використовувати різні рівні управління, а саме : командування, менеджмент, лідерство.

Крім того, лікарі нашого закладу зіштовхнулися з дилемою, як діяти у випадку повітряної тривоги та загрози для життя, якщо лікування (особливо

хірургічне) вже було почато. Ми прийшли до висновку, що під час тривоги лікування (операцію), що вже почато, потрібно закінчити і після того, швидко спускатись в укриття. Якщо ж лікування ще не було почате, а повітряна тривога застала за кілька хвилин до початку лікування, то лікувальна процедура переноситься на період після відбою повітряної тривоги, або переноситься на інший день.

Одним із найважливіших рішень які доводилось приймати було відновлення резервного електропостачання, що могло би забезпечити з одного боку повноцінне функціонування нашої установи, а з іншого боку було би рентабельним для малого бізнесу. Після 1-го нашого тривалого блекауту виникла термінова потреба покупки електрогенератора. Тут ми допустилися помилки, оскільки, в цей час виник дефіцит генераторів на ринку і приймаючи швидке рішення, не було враховано деякі технічні параметри та потужність, яку фактично видавав генератор, тому потужності не вистачило для забезпечення роботи нашого медзакладу, що призвело до потреби купівлі іншого генератора. Тимчасовим рішенням було під'єднання деяких електричних приладів до так званих акумуляторів (UPS) або інверторів з акумулюючими батареями, що дозволило працювати близько 30-40 хвилин в автономному режимі, після раптових відключень електроенергії.

При більш детальному вивченні, ми прийшли до висновку, що генератор потужністю 100 кіловат буде надто дороговартісним та не рентабельним для умов нашого закладу, хоча і покриє необхідні енергозатрати. Крім того, по правилах техніки безпеки, потрібно було окремо виділити достатню площу біля нашого закладу, що в умовах щільної забудови не давало такої можливості. Тому прокомунікувавши з іншими експертами та бізнесами, ми прийшли до висновку, що портативний інверторний генератор малої потужності (до 5кВт) буде рішенням, щоб забезпечити електроенергією та обігрівом частини нашого закладу (а саме 2 лікувальні кабінети, один із яких був хірургічний). Це дозволило продовжити роботу нашого закладу в критичний період (в частковому обсязі) і дало відносну безпеку лікування нашим пацієнтам, (деякі з пацієнтів боялись починати лікування, тому що повітряну тривогу, бомбардування і виключення світла неможливо було спрогнозувати).

Затратність роботи на електропостачанні від бензинового генератора малої потужності коштувала приблизно 100 грн (додаткових) на годину. Цю ціну деякі бізнеси враховували при виставленні чеку оплати для своїх клієнтів. В нашому випадку вдалося зберегти рентабельність без додаткових нарахувань пацієнтам. При аналізі причин, можна зробити попередній

висновок, що співпраця людей, комбінація лабільного графіку роботи (для економії електроенергії в періоди перевантажень на прохання місцевої влади) та ефективна робота міських служб по ремонту центральних електромереж дала позитивні результати.

Окремою управлінською інновацією, що була введена безпосередньо перед початком війни, була цифровізація, а саме перехід на електронну стоматологічну програму для запису пацієнтів та обліку медичних даних. Оскільки війна несподівано застала медичний заклад на перехідному етапі від бумажного ведення запису пацієнтів до електронного, то на момент відключення електроенергії були присутні обидві системи запису пацієнтів, що проявило плюси і мінуси обох систем в критичних ситуаціях. Зрештою після налагодження електромереж та резервних засобів живлення, та на даний момент, було прийнято рішення повного переходу на цифрову систему ведення запису пацієнтів.

Оскільки на сьогоднішній день військовий стан та війна продовжується, то з'являються нові виклики та ризики. Такі умови потребуватимуть якісно нових управлінських рішень та резилієнтності менеджерів-керівників, а також аналізу цих рішень для подальшого вивчення бізнес-процесів, економічної та медичної ефективності впровадженого бізнес-адміністрування.

Список використаних джерел:

1. *Закон України "Про застосування платних послуг в охороні здоров я" від 03.05.99р.*
2. *Закон України "Про рекламу" від 03.07.96р.*
3. *Закон України «Про Державний бюджет України на 2010 рік».*
4. *Закон України "Про ціни та ціноутворення" від 05.03.98р.*
5. *Закон України "Основи законодавства про охорону здоров я". - К.П,П. "Вігай", 1993 (ст. 18).*
6. *Кодекс законів про працю України // Кодекси України: У 2 т. – К.: Ін Юре, 1997. – Т. 1.*
7. *Вороненко Ю. В., Литвинова О.Н. Менеджмент та лідерство у медсестринстві. Тернопіль: «Укрмед книга», 2001р. – 364с.*
8. *Герчикова И. Н. Менеджмент.- М.: ЮНИТИ,1995.*
9. *Голяченко О. М. Економіка охорони здоров я. – Тернопіль, 1997.*
10. *Голяченко О. М, Соціальна медицина та організація охорони здоров'я*
11. *Ельштейн Н.В.ю Общемедицинские проблемы стоматологической практики. – Таллин: Валгу, 1983.*
12. *Соціальна медицина та організація охорони здоров я. Під ред. Вороненка Ю.В., Москаленка В. Ф. Тернопіль: "Укрмед книга",2000р.-675с.*
13. *Харьков Л.В. Маланчук В.О. Борисенко А.В. Основи стоматології Київ: Медицина, 2009. – 580 с.*
14. *Чернівська Л.П, Основи мотивації в менеджменті. – Суми: ВВП "Мрія-1" ЛТД, 1997.*

15. Чопчик В. Д. Концептуальні напрями розвитку організації стоматологічної допомоги дорослому населенню в системі державних амбулаторних закладів великих міст України : дис... канд. мед. наук: 14.02.03 / Національна медична академія післядипломної освіти ім. П.Л. Шупика. — К., 2007. — 169арк. — Бібліогр.: арк. 141-165.

16. Шортел С.М., Калюжний О.Н. Менеджмент в охороні здоров'я К.: «Основи», 1998 р. – 556 с.

Наконечний А. Ю.

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

ЕФЕКТИВНІСТЬ СУЧАСНИХ ІНТЕРНЕТ-МАРКЕТИНГОВИХ ДОСЛІДЖЕНЬ ДЛЯ РОЗВИТКУ ПІДПРИЄМСТВА

Інтернет-маркетингові дослідження є найефективнішим інструментом для розвитку бізнесу та вирішення цілей, завдань та бізнес-проблем. Вони дають багато інформації про те, як рекламні кампанії впливають на продажі, які дії було виконано для підтримки цих продажів, які методи реклами найкраще працюють та які є найпопулярніші способи отримання трафіку. Також вони можуть допомогти визначити найбільш привабливі ціни для продуктів та послуг і допомогти компанії краще зрозуміти своїх потенційних клієнтів.

Порівняно зі старими маркетинговими дослідженнями, інтернет-маркетингові дослідження надають більш детальну інформацію про поведінку клієнтів та статистику. Можуть допомогти компаніям вивчити ринок та проаналізувати потреби клієнтів. Також вони можуть допомогти підприємствам правильно просувати свої продукти та послуги; більш оптимальну реалізацію маркетингових кампаній в порівнянні зі старими маркетинговими дослідженнями, які базувалися на гіпотезах та суб'єктивних точках зору. Інтернет-маркетингові дослідження використовують більш точні методи для визначення результатів кампанії та приведення її до успіху.

Інтернет-маркетингові дослідження дають багато можливостей для оновлення стратегії маркетингу. Вони допомагають компанії визначати найбільш привабливі та рентабельні канали продажу та просування бренду. Вони також допомагають визначити найбільш успішні інформаційні та комунікаційні методи, які можна використовувати для залучення уваги потенційних клієнтів; допомагають дослідити ринкові тренди та визначати найбільш ефективні стратегії для досягнення поставленої мети; допомагають підвищити рентабельність інвестицій в маркетинг, полегшуючи прийняття правильних бізнес-рішень. Створюють компаніям потужну платформу, яка дозволяє більш ефективно відшукати нові ринки та залучати більше потенційних клієнтів, враховуючи потреби клієнтів та придумати стратегії, які допоможуть підвищити задоволення клієнтів і

розробляти краще продукти, так що компанії можуть вирішувати проблеми клієнтів швидше. Надійні результати цих досліджень дають компаніям можливість полегшити процес розвитку та підвищити ефективність їх бізнес-стратегії.

Для компаній, які хочуть підвищити свій бізнес, інтернет-маркетингові дослідження є найкращим інструментом. Вони дають можливість дослідити ринки, шукати нові можливості, розвивати стратегії та удосконалювати процеси бізнесу. Інтернет-маркетингові дослідження допомагають командам підвищити своє конкурентне позиціонування та досягти більш високих результатів.

Існують різні види інтернет-маркетингових досліджень, включаючи такі, як соціальний маркетинг, SEO-орієнтований маркетинг, аналітика, контекстна реклама, електронна пошта, контент-маркетинг та типографічна реклама.

Соціальний маркетинг використовує платформи соціальних мереж, такі як Facebook, Twitter, Instagram, Pinterest та YouTube, щоб підвищити рівень впізнаваності бренду та допомогти людям зробити їх покупки.

SEO-орієнтований маркетинг використовується для підвищення ранжування сайта в пошуку Google і інших службах пошуку.

Аналітика використовується для отримання даних щодо того, як фахівці взаємодіють з вашим брендом, що допоможе підвищити конверсію та поліпшити продуктивність.

Контекстна реклама використовується для продажу товарів чи послуг, що відповідають потребам користувача.

Електронна пошта використовується для надсилання рекламних повідомлень, запрошень на події і повідомлень про нові продукти лояльним клієнтам.

Контент-маркетинг використовується для створення вмісту, який відповідає потребам користувача та допомагає збільшити рівень впізнаваності бренду.

Типографічна реклама використовується для створення дизайну, який допомагає залучити увагу потенційних клієнтів.

Наприклад, якщо компанія використовує веб-аналітику, для аналізу даних користувачів, то дослідник може отримати оновлені результати протягом декількох годин. Але якщо дослідник використовує більш довгостроковий метод, такий як сервіси електронної пошти, то отримання оновлених результатів може зайняти до кількох днів. Але в загальному швидкість опрацювання інтернет-маркетингових досліджень залежить від багатьох чинників, таких як місце розташування компанії, розмір та набір

даних, які потрібно зібрати, та багато іншого. Оскільки відстеження та аналіз даних належать до інтернет-маркетингових досліджень, то швидкість опрацювання залежить від технологій та засобів, які використовуються для спостереження та аналізу даних. Щоб забезпечити найкращі результати, потрібно використовувати найсучасніші технології для обробки даних та залучати досвідчених спеціалістів.

Залежно від потреб та масштабів бізнесу малим компаніям та стартапам можна пропонувати інструменти для проведення інтернет-маркетингових досліджень безкоштовно або за доступною ціною. Наприклад, для проведення аналітики потреб малих компаній можна використовувати такі інструменти як Google Trends, Twitter Analytics, Google Analytics і т.д. Ці інструменти можуть полегшити аналіз даних та отримання доступних результатів. Для проведення більш складних досліджень можна скористатися деякими дешевими інструментами, такими як SurveyMonkey, Pollfish і т.д. Також є багато безкоштовних інструментів для аналізу соціальних мереж, які можуть допомогти малим компаніям і стартапам вивчати ринок та задовольняти потреби своїх клієнтів.

Середні та великі підприємства та корпорації мають більше можливостей для проведення повномасштабних інтернет-маркетингових досліджень. Такі компанії можуть пропонувати інструменти, такі як SAS, IBM SPSS, Tableau та інші, які допомагають проводити дослідження на додатковому рівні, а також допомагають отримувати більш детальну аналітику та полегшують виконання складних завдань. Ці компанії можуть також використовувати більш складні інструменти, такі як A/B-тестування та маштабування, які допомагають досягати максимальної ефективності рекламної кампанії. Крім того, ці компанії можуть скористатися послугами професійних аналітиків для проведення складних досліджень або надання консультаційних послуг.

Отже, інтернет-маркетингові дослідження дають можливість зрозуміти, які інструменти маркетингу найкраще працюють для потреб компанії та її клієнтів, дають велику кількість інформації для допомоги компаніям в розвитку їх бізнесу. Вони дозволяють компаніям більш ефективно створювати, та посилювати рекламні кампанії, таким чином збільшуючи продажі та підвищуючи прибуток. А на початку діяльності компанії можуть більш економічно доцільно використовувати рекламний бюджет, тим самим полегшуючи створення бренду та удосконалити систему зв’язку з клієнтами.

Список використаних джерел:

1. *Т. Дж. Лакер, "Інтернет-маркетинг: практичний підхід до онлайн-продажів".*
2. *Роберт Д. Кетчум, "Інтернет-маркетинг: вища школа реклами та продажів".*
3. *Майкл Голдсміт, "Інтернет-маркетинг: стратегії для розвитку бізнесу в Інтернеті".*
4. *Джордж И. Барретт, "Інтернет-маркетинг: як досягнути бізнес-успіху в Інтернеті".*
5. *Стів Браун, "Інтернет-маркетинг: практичні приклади та перспективи".*
6. *Гілліон Д., Армстронг Т., Кларк Д. (2013). Інтернет-маркетинг для початківців. Оксфорд, Велика Британія: Пресса Оксфорд.*
7. *Інтернет-маркетинг: практичні поради для бізнесу, автор: Джон Сміт*
8. *Веб-аналітика: дослідження та оптимізація веб-сайтів, автор: Аврора Карлсон*
9. *Розумний маркетинг: використання даних, аналітики та метрики для поліпшення маркетингу, автор: Даніель Рікс*
10. *Аналітика соціальних мереж для малих підприємств: практичні поради (ред. В. Альфонсо).*
11. *Аналітика цифрового маркетингу: стратегії та застосування для електронного бізнесу, Роб Сандерс.*
12. *Посібник з онлайн-маркетингових досліджень: методи та застосування, автори Гарі Лілієн та Арвінд Рангасвамі.*

Нікітін Д. О.

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

ЦИФРОВИЙ МАРКЕТИНГ: СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ

Цифровий маркетинг – це новий етап еволюції маркетингу. Він настає, коли маркетингова діяльність компанії здійснюється здебільшого з використанням цифрових каналів. Це адресні канали, що дозволяють маркетологам вести постійний двосторонній персоніфікований діалог з кожним споживачем. Такий діалог побудований на використанні даних, отриманих у результаті минулих взаємодій зі споживачем. Крім того, маркетологи постійно використовують інформацію про поведінку споживачів, яка надходить до них в режимі реального часу. Це забезпечує зворотній зв'язок зі споживачем, поліпшуючи і оптимізуючи взаємодію з ним. Існує цілий ряд тактик та інструментів, які відносяться до поняття цифрового маркетингу. Це сам веб-сайт компанії та канали інтернет-маркетингу: SEO, Інтернет- реклама, електронний маркетинг, воронки, продаж, контент-маркетинг, банерна реклама, SMM та ін.

Всі інструменти інтернет-маркетингу підпорядковані вирішенню одного з головних завдань: залучення відвідувачів на сайт або мотивування відвідувачів на вчинення дії на сайті (так звана конверсія).

Основні інструменти цифрового маркетингу:

1. Пошукова оптимізація веб-сайту, яка допомагає йому займати більш високі позиції в пошуковій видачі. Це збільшує об'єм органічного (безкоштовного) трафіка.

2. Контент-маркетинг, який вважають одним з найефективніших інструментів для просування бізнесу в Інтернеті. Він підходить для підвищення пізнаваності відомих брендів або залучення клієнтів.

3. Маркетинг в соціальних мережах (SMM). Даний вид маркетингу націлений на просування бренду і контенту в соціальних мережах. Він може бути використаний для збільшення кількості трафіка, а також для генерації лідів.

4. Реклама з оплатою за клік (PPC) - чудовий метод залучення трафіка на сайті. Суть полягає в тому, що за кожний клік по оголошенню потрібно заплатити власнику сайту або провайдеру комісію. Найбільш поширеним типовим PPC є Google AdWords.

5. E-mail-маркетинг. Компанії використовують поштову розсилку як здатність спілкуватися зі своєю аудиторією. Електронна пошта найчастіше використовується для просування товарів, повідомлень про знижки та заходи, а також для направлення людей на веб-сайт компанії [1].

Цифровий маркетинг не можна ототожнювати із інтернет-маркетингом, адже останній використовує тільки онлайн-канали здійснення, тоді як цифровий маркетинг може бути реалізований як в онлайн, так і в офлайн середовищі. Проте, в умовах діджиталізації всіх сфер господарювання, найбільша сфера цифрового маркетингу – це інтернет-технології. Перейдемо до аналізу статистичних даних щодо динаміки Інтернет-активності громадян виходячи з попередньої тези про те, що останні є однією з важливих категорій споживачів послуг цифрового маркетингу.

Сьогодні цифровий маркетинг орієнтований на різноманітні мобільні гаджети. В подальшому дана тенденція залишиться, але значна увага буде приділена використанню штучного інтелекту, зокрема, для аналізу запитів, основних інтересів і навіть емоційних відносин з конкретним продуктом. Цифровий маркетинг є одним з найбільш швидкозростаючих сегментів сучасного ринку.

У відповідності з дослідженнями, значний вплив на населення спостерігається при використанні візуалізованого контенту. Технології віртуальної реальності (VR) активно використовуються для потреб передових компаній світу при реалізації їх маркетингових стратегій. Використання технології віртуалізації дає можливість отримати новий рівень комунікацій з цільовою аудиторією завдяки візуальному контакту, що дозволяє користувачам відчути реальність представленої продукції та прискорити прийняття рішення про її придбання. Компанії використовують VR у власних рекламних стратегіях, створюючи усвідомлення у клієнтів персоніфікованого вибору [3].

Серед основних напрямків розвитку цифрового маркетингу можна виділити [4]:

1. Shoppable пости. Соціальна комерція – покупка продуктів безпосередньо через публікації в соціальних мережах або рекламу; користувачеві не потрібно залишати сайт або додаток.

2. Особиста переписка. Прямий обмін повідомленнями, як засіб оптимізації обслуговування клієнтів і надання допомоги в продажах, стає однією з найактуальніших тенденцій цифрового маркетингу.

3. Мікро-інфлюенсери. Маркетинг впливу вже кілька років є трендом цифрового маркетингу. «Вплив» в соціальних медіа – тепер став дорогим продуктом.

4. Інтерактивні e-mail-розсилки. Останнім часом спостерігається стрімкий спад в текстових електронних листах і новинних розсилках. В e-mail-маркетингу тепер використовуються електронні листи, які виглядають і функціонують як веб- сторінки, включаючи інтерактивні кнопки та іншу взаємодію.

5. Аналіз настроїв або соціальне слухання – це практика аналізу реакції користувачів і клієнтів на продукт або послугу, зазвичай в соціальних мережах або в інтернеті в цілому. Аналіз настроїв зазвичай включає в себе інструменти і алгоритми збору даних, які знаходять згадки бренду в інтернеті і оцінюють їх тональність.

6. Альтернативні і нішеві канали соціальних медіа. Зокрема, Snapchat, Pinterest, Medium і Reddit стають новими фаворитами для маркетологів останнім часом. Facebook не актуальний серед молодих користувачів, і бренди, орієнтовані на ринок молодше 30 років, стікаються в молодіжні майданчики.

7. Програмна реклама. Розміщення реклами, медіа-баінг, відстеження ефективності і таргетування можуть бути виконані програмним забезпеченням. Програмне забезпечення, таке як Adobe Marketing Cloud або SmartyAds, допоможе маркетологам орієнтуватися вонлайн-рекламі.

8. Оптимізація для обраних фрагментів. При створенні цифрового маркетингового контенту необхідно оптимізувати кожен фрагмент вмісту для вибраних фрагментів, використовуючи добре структурований вміст.

9. Влоги. Завдяки популярності YouTube, Instagram Stories і Snapchat, відеоблоги стали дуже популярними. На відміну від інших типів відео, таких як пояснювальні відеоролики або короткі фільми, влоги – більш персоналізовані. Влогери безпосередньо спілкуються з глядачем (стиль PewDiePie), створюючи безпосередній зв’язок, що, безсумнівно, є благом для маркетологів, які намагаються встановити більш міцні відносини зі своїми клієнтами.

10. Розмова з Gen Z на їх мові. Маркетинг для Gen Z означає зміни у стилізації контенту. Наймолодший ринок також самий химерний, зі смаками, які можуть здатися дивними, якщо звикнути до маркетингу, орієнтованого на бумерів або покоління X [4].

Отже, успішна діяльність у сфері цифрового маркетингу вимагає пильної уваги на засоби, що дійсно працюють у сучасних динамічних умовах, а які ні. Сьогодні є багато інструментів, які сприяють успішній реалізації стратегії цифрового маркетингу.

Проведені дослідження вказують на те, що мобільний телефон серед інтернет-користувачів – один з найпопулярніших гаджетів, що значно

впливає на вибір методів та каналів здійснення цифрового маркетингу та багатьох інших галузей. Загальна тенденція цифрового маркетингу спрямована на більш особисті відносини з цільовими нішами, але кошти для створення цих зв'язків вкладаються у цифровізацію і нові технології. Основа цифрового маркетингу залишається тією ж – давати людям те, що вони хочуть, коли і де вони цього хочуть, а цифрові технології відкривають для цього нові шляхи.

Маркетинг-2023: головні тренди

1. Дорожня карта клієнта (CJM) Нині клієнти очікують персоналізованого контенту й досвіду, який безпосередньо відповідає їх потребам. Оскільки споживачі не взаємодіють з компаніями й брендами за допомогою одного методу чи каналу, маркетологи мають досліджувати конкретні взаємозв'язки клієнта з організацією на всьому шляху: від моменту першого контакту до факту купівлі продукту чи послуги. Один із найоптимальніших способів краще зрозуміти досвід користувача – це створити дорожню карту клієнта (Customer Journey Map). Це візуальне представлення того, як клієнт діє, думає та відчуває себе під час купівлі продукту, з якими бар'єрами чи проблемами він зіштовхується на своєму шляху, коли шукає необхідну послугу чи товар. Чому необхідно звернути увагу на цей маркетинговий інструмент? Річ у тім, що 80% клієнтів вважають свій досвід роботи з компанією таким же важливим, як і її продукцію. Тому якщо ви прагнете підвищити лояльність клієнтів, поліпшити відсоток повторних покупок і збільшити конверсію, скоротивши цикл продажів, обов'язково розробіть карту подорожі клієнта.

2. Штучний інтелект (AI) Дослідження від Razorfish свідчить, що три чверті маркетологів не використовують поведінкові дані для розробки, розміщення й орієнтації на потенційних клієнтів онлайн-реклами. Саме тому в наступному році сфера маркетингу буде працювати над тим, аби активно застосовувати їх у своїй роботі. Вже зараз фахівці з маркетингу починають послуговуватися такими методами штучного інтелекту як моделі даних, алгоритми та машинне навчання. Це допомагає краще зрозуміти свою цільову аудиторію, оптимізувати витрати, визначитися зі специфікою й типом контенту, а також персоналізувати взаємодію з клієнтами, підвищити їх лояльність й краще зрозуміти поведінкову тактику.

3. Інтерактивний контент 81% маркетологів вважають інтерактивний контент найбільш дешевою й ефективною маркетинговою стратегією, що допомагає активно привертати увагу потенційних покупців. Окрім цього, такий вміст сприяє збільшенню конверсій, покращеному залученню аудиторії, підвищенню лояльності клієнтів й оптимізації їхнього досвіду.

Зокрема, ефективно охопити значну кількість цільової аудиторії, зацікавити її та змотивувати до взаємодії допоможуть вікторини, ігри, калькулятори, інтерактивні карти, відео й інфографіка. Сервісів, для створення такого контенту, – безліч, проте їх функціональні можливості для вільного користування можуть бути обмежені. Тому якщо плануєте розробляти якісний і унікальний інтерактивний контент, будьте готовими до оформлення преміум-підписки. Скористатися вже готовими відео для публікацій чи змонтувати власні допоможуть Pexels Videos, Clipchamp й OpenShot. Привернути увагу користувачів самостійно зробленими гіфками можна за допомогою GIPHY, Coub чи Powtoon. Для створення інфографіки стануть у пригоді Infogram й Visually, а для графіків і діаграм – Datavisual та Plotly. Зібрати фідбек від своїх клієнтів можна за допомогою форм, створених на Typeform і Riddle. Окрім цього, сервіси надають можливість розробити вікторини та конкурси.

4. Соціальна відповідальність Споживачі надають перевагу брендам, які практикують соціальну відповідальність, збалансовуючи свої ініціативи щодо заробітку грошей із соціально корисними практиками. Так, більше половини споживачів у США під час покупок звертають увагу на цінності й світоглядні позиції компанії. Саме тому нині маркетологи вже працюють над розробкою стратегій, що мають на меті активізувати соціальну відповідальність компанії. Це допоможе залучити тих клієнтів, які завдяки купленим речам прагнуть бути корисними для суспільства й навколишнього світу. Прикладами реалізації стратегії активізації соціальної відповідальності компанії можуть бути рекламні акції, які поширюють обізнаність про суспільні проблеми, перерахування коштів на благодійність, проведення громадських заходів тощо. Так, наприклад, Comfy разом з благодійним фондом Сергія Притули проводили збір 11 млн грн на купівлю 15 БПЛА «Валькірія» для ЗСУ. До цієї ініціативи також приєдналися Choice Company, Work.ua, А-Банк, Lviv Croissants, ПУМБ, Volpis, Akvarel Mercurial, EnglishDom, Magecom та інші.

Список використаних джерел:

1. *https://rau.ua/novyni/marketing-2023/*
2. *http://repository.vsau.org/getfile.php/27499.pdf*

Петросюк В. В.

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

ФОРМУВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ МАРКЕТИНГ-МЕНЕДЖМЕНТ

Управління маркетингом (marketing management) - аналіз, планування, реалізація і контроль маркетингової діяльності з виявлення, створення і підтримання вигідних обмінів з цільовими споживачами з урахуванням цілей організації. При управлінні маркетингом послідовно здійснюються: аналіз маркетингу, планування маркетингу, реалізація плану маркетингу, контроль маркетингу. Діяльність з управління маркетингом стосовно завдань служб маркетингу організації конкретизується у процесі управління маркетингом. Вона грунтується на широкому використанні інформація про споживачів, конкурентів, посередників, інших суб'єктах ринкової діяльності [1].

У літературі з маркетингу термін «marketing management» іноді перекладається як «маркетингове управління», в який часто вкладають особливий зміст, тобто мова йде про управління всією діяльністю організації на принципах маркетингу – про використання маркетингу як філософії управління, коли всі підрозділи організації планують і оцінюють свою діяльність з позицій маркетингу [2]. На практиці навіть в країнах з розвиненою ринковою економікою це далеко не завжди так, і існує безліч організацій, в яких в силу специфіки їх діяльності, особливостей ринку, поглядів керівництва маркетинг відіграє набагато більш скромну роль у їхній діяльності. Однак більшість організацій в будь-якому випадку мають співробітників, які займаються маркетингом, хоча концепція маркетингу не стала домінуючою для організації в цілому. Видається, що найбільш коректним терміном, що охоплює всі рівні використання концепції маркетингу, є: «управління маркетинговою діяльністю» або спрощений його аналог: «управління маркетингом» [4].

Концепція маркетингу - це орієнтація на нужди і потреби клієнта, підкріплена зусиллями маркетингу, націленими на створення споживчої задоволеності як основа для досягнення мети організації. Об'єктом основної уваги в концепції комерційних зусиль є існуючий товар фірми, а забезпечення прибуткового збуту вимагає напруги комерційних зусиль і заходів стимулювання. Фірма реалізує товари і одержує прибуток за рахунок

максимального задоволення потреб споживача. Підприємство координує свою діяльність з розрахунком на забезпечення задоволеності клієнтів, одержуючи прибуток завдяки створенню і підтримці споживчої задоволеності [1].

Концепція маркетингу стверджує, що заставою в досягненні мети організації є визначення потреб і потреб цільових ринків і забезпечення бажаної задоволеності ефективнішими і продуктивнішими, ніж у конкурентів, способами.

Концепція маркетингу припускає, що досягнення компанією своїх цілей залежить від визначення потреб і запитів цільових ринків, а також від більш ефективного порівняно з конкурентами задоволення споживачів.

Постійна і планомірна робота з організації управління маркетингом повинна здійснюватися на основі системи взаємозалежних показників, що характеризують її рівень. При цьому потрібні науково обґрунтовані рекомендації з ведення аналізу існуючої організації маркетингу та оцінці заходів, розроблювальних з метою її поліпшення і впровадження в систему керування. Для цього спочатку необхідно провести оцінку стану маркетингової системи підприємства. Ступінь ефективності управління маркетингом можна оцінити за допомогою аналізу маркетингового потенціалу підприємства; ревізії та аудиту маркетингу; оцінки ефективності маркетингу на основі вивчення проблем управління маркетингом підприємства. Крім того, існує безліч методів вивчення факторів організаційного порядку, що дозволяють побічно оцінити окремі сторони ефективності управління маркетингом. Управління діяльністю - стратегічно важливий напрямок у системі управління маркетингом, від якого принципово залежать два інших. Концепція управління маркетинговою діяльністю формується та інтегрується в систему керування підприємством на самому вищому рівні. Реальні управлінські процеси в розрізі конкретної діяльності організації здійснюються за допомогою системи керування маркетинговою функцією. Маркетингові заходи, здійснювані безпосередньо маркетинговою службою і спрямовані на створення попиту на товари, є предметом керування попитом у системі управління маркетингом підприємства [3].

На ефективність управління маркетингом найбільший вплив робить рівень керування діяльністю. Як відзначалося вище, дана під функція системи управління маркетингом визначається відношенням до маркетинга на підприємстві, застосуванням його принципів у процесі виробничо-торгової діяльності.

Однією із серйозних проблем будь-якого планування на вітчизняних промислових підприємствах є недалекоглядність, тобто відсутність

стратегічного маркетингу. Для його здійснення необхідні висококваліфіковані маркетологи-практики. Досвід показує, що таких фахівців дуже мало, і, як правило, весь їхній робочий час зайнятий рішенням поточних задач. Тому часу на формування стратегії не залишається. Як відомо, відсутність стратегії рідко приводить до успіху. Відсутність цілісної картини стратегічного керування - одна з причин, які призвели вітчизняні підприємства до положення, коли вони не розвиваються, а виживають.

Формування ринкової економіки в Україні зумовлює необхідність нового підходу до управління виробництвом і збутом товарів повсякденного споживання, який забезпечить використання зарубіжного досвіду маркетингу, його адаптацію до конкретних умов регіону і всієї України в цілому. Маркетинг слід розглядати, як методологію ринкової діяльності, що визначає стратегію і тактику підприємств в умовах конкуренції. Ключовим завданням підприємств торгівлі сьогодні стає орієнтація на споживача. Для того, щоб задовольнити потребу, компанія виступає з пропозицією, що має цінність для споживача. Успіх мають ті пропозиції, які забезпечують споживачеві одночасно задоволення та вигоду. Досягнення цільового ринку вимагає використання каналів комунікації, розподілу і збуту, які в своїй сукупності утворюють ланцюг, що з'єднує всі підприємства - від постачальників сировини до доводящіх кінцевий продукт до покупця - і що представляє собою систему створення споживчої цінності. Далекоглядні компанії повинні будувати свою маркетингову діяльність у відповідності зі змінами на ринку і в ринковому просторі [2].

У реалізації моделі маркетинг-менеджменту процес управління маркетингом засновано на принципі орієнтації на покупця (споживача) товарів та послуг не тільки з точки зору розповсюдження широкого спектру матеріалів і технологій, але й з точки зору, що сучасний виробник повинен створювати свій імідж, імідж свого товару [4].

Список використаних джерел:

1. Войчак А. В. Маркетинговий менеджмент: Підручник. - К.: Вид-во КНЕУ, 2008. 258-268 с.

2. Герасимчук В. Г. Маркетинг. Теорія і практика 2004. - 27 с.

3. Михайловська-Ясюченко Л. В. Основні фактори, що формують маркетингові ризики підприємства // Маркетинг в Україні. – 2005. – №3. – С. 18-22.

4. Котлер Ф. Основы маркетинга. Краткий курс.: Пер. с англ. – М: Издательский дом «Вильямс», 2004. – 156 с.

Рильцов Є. Р.

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

АНАЛІЗ КОМПЕТЕНЦІЙ МЕНЕДЖЕРІВ ІЗ ПРОДАЖУ У СФЕРІ ПОСЛУГ НАДАННЯ ОНЛАЙН РЕКЛАМИ

Менеджер з продажу – одна із найбільш популярних професій на ринку праці на сьогодні. Головне завдання такого фахівця – продаж товарів та послуг компанії, розширення кола клієнтів та підтримку партнерських відносин з ними, а також побудова подальшої співпраці із постійними клієнтами найбільш ефективним чином. Оскільки саме продаж є основою будь-якого бізнесу, фактично, менеджер з продажу є ключовим співробітником, від організації роботи якого залежить просування товарів та послуг і, як наслідок, отримання прибутку компанією. Більшу частину свого часу менеджер проводить в переговорах чи пошуках нових клієнтів, таким чином, забезпечуючи фінансове благополуччя компанії [1].

Професія, пов’язана з продажем товарів чи послуг, впродовж віків ніколи не втрачала своєї актуальності та значимості, адже саме від розвиток та успішне ведення торгівельної діяльності стало поштовхом до розвитку цивілізацій та науково-технічного прогресу. У XXI столітті на сьогоднішньому етапі соціально-економічного розвитку більшість бізнес-процесів перейшли в онлайн, а успішне ведення будь-якої справи потребує ефективної онлайн-реклами. Під такою рекламою маються на увазі не лише таргетована інтернет-реклама, не постери в соціальних мережах, не тільки відео-ролики, але в першу чергу – онлайн продаж тет-а тет. Адже, в будь-якому разі, живе спілкування зможе викликати в потенційних споживачів більше довіри до компанії, а доброзичлива розмова із співробітником стане найбільш продуктивним методом переконати покупця. Саме тому професія менеджер з продажу набула значного поширення на ринку праці.

Відповідно до аналітичних даних Finance.ua на українському ринку праці на початку 2023 року вакансії менеджера з продажу склали 26% від загальної кількості. У свою чергу відсоток резюме з професійної сфери «Продажі» становить 12%. Таким чином, можна зробити висновок, що саме така сфера є однією із небагатьох на ринку праці, де пропозиція перевищує попит [3].

На сайті work.ua «Менеджер з продажу» є одним з найпопулярніших запитів, не лише серед шукачів роботи, але і серед роботодавців. На даному сайті з пошуку роботи активно 4813 вакансій даної сфери. Проте, рівень конкуренції у різних категоріях сфери продажів різний.

Найбільша конкуренція серед пошукачів – 3,3 фахівця на 1 робоче місце – має галузь дистрибуція.

Найменші показники з конкуренції – 1,1 людина на 1 робоче місце серед галузі продажів будівельних матеріалів, електротехнічного обладнання, світлотехніки.

Невеликий конкурс 1,2 фахівця на 1 робоче місце для галузі продажів послуг для бізнесу, роздрібної торгівлі та прямі продажі. Конкуренція в 1,3 фахівця на 1 робоче місце для галузі продажів послуг для населення та торгівельні мережі. І з близькими по значенню показниками: 2,2; 2,4; 2,9 фахівця на 1 робоче місце конкуренція для менеджерів по роботі з клієнтами, управління продажами та оптова торгівля відповідно [2].

Якщо говорити про попит даної професії, то саме ІТ- сфера є потребує найбільшу кількість менеджерів з продажу. Це пов’язано із переходом до діджиталізації та розвитку сфери інформаційних технологій. ІТ – компанії, що розробляють програмне забезпечення, потребують постійного пошуку потенційних клієнтів та побудову тривалих ділових відносин з ними. Навіть, будь-який інтернет-магазин чи фінансова компанія або банк, що надають онлайн послуги, потребують ефективної реклами з метою продажу, який може забезпечити тільки людський ресурс. [1].

Менеджер з продажу – досить багатогранна професія, яка передбачає велику кількість софт- та хард-скілів, якими повинен володіти її представник.

До головних софт-скілів належить: стресостійкість, наполегливість, рішучість, вміння зрозуміло висловлювати свою думку, вміння критично мислити, креативність та активна життєва позиція.

До професійних компетенцій або хард-скілів менеджерів із продажу у сфері послуг надання онлайн реклами належать:

1. Навички ведення переговорів. Менеджер з продажу повинен вміти чітко висловлювати свою думку, вміти аргументувати та переконувати клієнта, працювати із запереченнями. Менеджер повинен вміти побудувати розмову саме таким чином, аби її підсумком стала ділова угода з клієнтом. Менеджер повинен говорити впевнено в собі, з нотою позитиву, повинен вміти влучно пожартувати або зробити бізнес-комплімент для того, щоб створити загальну атмосферу довіри до компанії та її діяльності.

2. Знання технік та методів продажу. Розмова в позитивному ключі, або проста розповідь про компанію та її товари/послуги не завжди є

запорукою продажу. Менеджер повинен знати основні техніки продажів і чітко дотримуватись їх. Наприклад, однією із основних технік є техніка п'яти етапів продажів, що складається із наступних етапів: встановлення контакту, виявлення потреби, презентацію, обробку заперечення та закриття угоди. Якщо слідувати цим правилам – 50% успіху вже забезпечено.

3. Вміння працювати із соціальними мережами, блогами, інтернет-спільнотами чи форумами. В епоху діджиталізації більшість часу середньостатистична людина проводить саме в соціальних мережах, де вона дізнається останні новини, спілкується із друзями чи колегами по роботі. Саме тому завоювати увагу потенційних клієнтів на таких платформах є дуже важливим методом онлайн-реклами.

4. Базові знання HTML чи графічних пакетів. Оскільки соціальні мережі рясніють яскравими картинками та фотографіями, а на текст рекламного повідомлення потенційний споживач звертає увагу не в першу чергу, менеджер повинен створити оригінальний креативний контент, що приверне увагу читача.

5. Крім того менеджер повинен вміти працювати з такими базовими програмами як MS Word та Excel. Вміти аналітично мислити, розраховувати бюджет реклами та доцільність її впровадження.

6. Знання іноземних мов буде додатковою перевагою. Адже, як говорив Нельсон Мандела: «Говорячи з людиною тією мовою, яку вона розуміє, ти говориш з її головою. Якщо ти говориш з людиною її рідною мовою, ти говориш з її серцем».

7. Ефективна презентація або підхід «elevator speech», що дослівно перекладається як ромова у ліфт. Іншими словами це короткий опис вашої компанії, а також мети розмови. Таку назву даний метод отримав тому, що по часу така розмова не повинна бути тривалою – вона має займати не більше часу, ніж поїздка у ліфті для того, щоб не перезавантажити співрозмовника зайвою, нецікавою для нього інформацією [4].

Лайфхаки elevator speech:

Промова має бути короткою, приблизно 30-60 секунд, та відображати суть справи. Вам потрібно бути переконливим. Навіть якщо це короткий виступ, ваша промова в ліфті має бути достатньо переконливою, щоб зацікавити слухача вашою ідеєю, організацією чи досвідом.

Поділіться своїми навичками. У вашій презентації має бути пояснено, хто ви, які у вас кваліфікації та навички. Спробуйте зосередитися на активах, які додають цінність у багатьох ситуаціях [4].

Практика. Найкращий спосіб відчути себе комфортно під час виголошення промови в ліфті – практикувати її, доки швидкість і «висота» не

стануть природними, не звучачи як робот. Ви звикнете варіювати розмову, практикуючись у цьому. Чим більше ви практикуєтеся, тим легше вам буде це робити, коли ви перебуваєте на заході з професійного спілкування або співбесіді.

Будьте позитивними та гнучкими.

Згадайте свої цілі. Не потрібно бути надто конкретним. Надто цілеспрямована ціль не допоможе, оскільки ваш виступ використовуватиметься за багатьох обставин і з багатьма різними типами людей.

Підготуйте візитну картку. Якщо у вас є візитна картка, запропонуйте її в кінці розмови, щоб продовжити діалог.

Категорично не рекомендується:

- Говорити занадто швидко. Обмеженість у часі не варто компенсувати швидкістю розмови, адже це тільки може спричинити ускладнення сприйняття інформації.
- Використовувати жаргон. Використання слів-жаргонів не завжди зможе викликати довіру чи перенести розмову на один рівень спілкування.
- При цьому не слід використовувати занадто спеціалізовані терміни та складносурядні, складнопідрядні речення. Розмова має бути простою, та зрозумілою [5].

На перший погляд, професія менеджера з продажу у сфері онлайн реклами є не дуже привабливою, проте, якщо подивитись глибше, то це не зовсім так. По- перше, менеджер з продажу у сфері послуг надання онлайн реклами повинен володіти багатьма навичками, починаючи від знання іноземних мов і закінчуючи аналітикою ринку. Крім того, такий працівник має володіти багатьма особистісними якостями, мати певні риси характеру, що дозволять йому більш ефективно виконувати свою роботу та не тільки приносити прибуток компанії, але й отримувати задоволення від своєї професійної діяльності. Нові завдання, кожен новий кейс для менеджера передбачає пошук нових ділових рішень, знайомство з новими людьми, країнами чи навіть культурами, що сприяє всебічному розвитку. Таким чином, дана професія не лише має велике значення для розвитку бізнесу та є затребуваною на ринку праці, але і є дуже захоплюючою, оскільки характеризується відсутністю рутини та сприяє різнобічному розвитку працівника як особистості.

Список використаних джерел:

1. IT Рейтинг UA – перша діджитал екосистема України. IT рейтинг Украины. URL: https://it-rating.ua (дата звернення: 24.02.2023)

2. Work.ua – сайт пошуку роботи №1 в Україні. Work.ua – сайт пошуку роботи №1 в Україні. URL: https://www.work.ua (дата звернення: 24.02.2023).

3. Finance.ua | Фінанси в Україні | Курси валют, кредити, депозити, новини України. finance.ua. URL: https://finance.ua/ (дата звернення: 24.02.2023).

4. Doyle A. When and How To Use an Elevator Pitch. The Balance. URL: https://www.thebalancemoney.com/elevator-speech-examples-and-writing-tips-2061976 (date of access: 24.02.2023).

5. Oleksenko, Y., Makarenko, S. (2020). Features of it market development in Ukraine. P. 152-173. DOI: 10.30525/978-9934-588-38-9-31

6. TheSocialMediaEngagementFunnel [Електронний ресурс] / MarkSmiciklas – Режим доступу: http://www.intersectionconsulting.com/the-social-media-engagement-funnel/

Рильцов Р. Є.

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

МОДЕЛЬ ПРОФЕСІЙНОЇ УСПІШНОСТІ МЕНЕДЖЕРА З ПРОДАЖУ У СФЕРІ ПОСЛУГ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Однією із найбільш розповсюджених професій на сучасному ринку праці є професія менеджера з продажу, а саме – в IT – сфері. Добре відомо, що менеджер з продажу повинен володіти такими загальними рисами як: комунікабельність, стресостійкість, вміння будувати розмову, володіти техніками продажів, вміти знаходити спільну мову із різними типами клієнтів, володіти грамотною усною та письмовою мовою. Проте, в IT – сфері ця професія має свої особливості.

По – перше, робота звичайного менеджера з продажу передбачає, що майже увесь його робочий час присвячений роботі з клієнтами – ефективним переговорам та пошуку нових клієнтів. Проте, в IT – сфері менеджер з продажу повинен виконувати і інші функції [5].

Взагалі, в IT – компаніях робота менеджера з продажу, яка не стосується безпосередньої роботи з клієнтами включає два основні етапи: pre-sale (передпродаж) та **post-sale** (післяпродаж).

У багатьох сферах наріжним каменем роботи сейлз менеджера є саме спілкування з клієнтом. Проте, в IT – сфері перш, ніж приступити до розмови, менеджер повинен ретельно вивчити всю інформацію про продукт, про ринок та визначити всі потреби цільової аудиторії. Це пов’язано із особливістю продукту, адже розробка програмного забезпечення – це довготривалий і досить вартісний процес. Тому цілком логічно, що клієнт буде шукати найбільш оптимальний варіант. Завдання менеджера з продажу – ретельно вивчити всі особливості, врахувати всі ньюанси та представити продукт найбільш ефективним чином з метою потенційного продажу. Саме така діяльність і називається pre-sale [3].

Крім того, pre-sale передбачає ще одні завдання: lead generation та lead processing. Перше — це про те, як знайти та залучити клієнта, а друге — як підписати угоду. Це необхідно для формування власної для кожного менеджера мережі контактів, яка би приносила компанії нові проекти та, відповідно, і дохід.

Post-sale – це робота з діючими клієнтами, коли сейлз виступає для клієнта каналом зворотнього зв’язку. Такі фідбеки важливі не лише для діючих

угод, але і можуть сприяти допродажу IT – послуг (up-sale). Маючи з клієнтом довірливі стосунки стосунки, менеджер збільшує ймовірність того, що клієнт порадить дану компанію своїм бізнес-партнерам. Таким чином мережа контактів буде розширюватися [1].

Post-sale важливий також для того, аби отримати від клієнтів зворотній зв'язок, що допоможе визначити сильні і слабкі сторони компанії та її продуктів, виявити недоліки і вчасно їх виправити. Таким чином, через сейлз менеджера саме думка споживачів формує позитивний імідж компанії. Також за допомогою післяпродажу можна підібрати найбільш оптимальне рішення для кожного клієнта, використовуючи індивідуальний підхід як основну цінність роботи компанії [5].

В IT – компанії, на відміну від інших сфер, менеджер з продажу є багатофункціональною ланкою в межах компанії і виконує діяльність у трьох сферах: робота з клієнтами, робота не з клієнтами та допомога команді.

Робота з клієнтами передбачає власне переговори, які в кінцевому випадку ведуть до продажу та формуванню ділових зв'язків.

Робота не з клієнтами є аналітичною і передбачає:

моніторинг ринку та конкурентів;

ведення звітності за контактами та продажами;

складання документації (наприклад, офери за підтримки бухгалтерів і юристів);

аналіз даних продажу за попередній період;

формування подальшої стратегії для продажів на основі аналізу попередніх; бере участь в удосконаленні продуктів або послуг компанії.

Також менеджер з продажу допомагає команді, тісно співпрацюючи із лідогенераторами та представниками із розвитку продажу, а також з іншими менеджерами того ж самого рівня.

Лідогенератори моніторять та передають всю необхідну інформацію на етапі pre-sale та допомагають у пошуку найбільш оптимальних рішень, шукають потенційних клієнтів. Представники із розвитку продажу є менеджерами вищого рівня, які закривають угоди на великі суми, що мають стратегічно важливе значення для компанії [2].

Особливістю роботи менеджера з продажу в IT – сфері є робота в сегменті B2B (business to business). Більшість менеджерів з продажу працюють із фізичними особами, проте менеджери в IT – компаніях продають програмне забезпечення бізнесу та спрямовують свою діяльність виключно на юридичних осіб [3].

У B2B сегменті менеджер проходить 3 етапи: аутсорсинг, аутстафінг і продаж SaaS-продуктів.

Аутсорсинг — передача функцій або процесів компанією, яка не спеціалізується на якійсь сфері, на компанію, яка на цій сфері спеціалізується. Оплата здійснюється за фактом виконаної роботи.

Аутстафінг — надання компанії-замовнику компанією-виконавцем потрібних фахівців для розв'язання певних завдань. Тобто в компанії з'являється розробник, наданий іншою компанією. Оплата фіксована, результат праці на неї не впливає.

SaaS (software as a service) — програмне забезпечення як послуга. Користувач (часто за передплатою) отримує доступ до сервісу віддалено. Наприклад, клієнт купує платформу для масових email-розсилок, щоб використовувати у своєму бізнесі [2].

Менеджер з продажу в IT не лише захоплююча професія, яка потребує багатьох навичок і вмінь, але і передбачає кар'єрне зростання, на відміну від більшості менеджерів з продажу в інших сферах.

В IT компаніях із посади сейлз менеджера можна перейти на позицію бізнес – аналітика (Business Analyst). Адже саме на етапі pre-sales бізнес – аналітики вивчають всі переваги і недоліки продукту, ринок, особливості цільової аудиторії (фізичні особи чи бізнес). Для коректної презентації IT – продукту менеджер з продажу також повинен добре розумітись на цих нюансах.

Досить цікавою є професія проектного менеджера (Project Manager). Проектний менеджер також виконує функції перемовин, але не тільки з клієнтами, але і з командою розробки. Проектний менеджер повинен розумітись також у всіх деталях розробки програмного продукту та враховувати побажання клієнта.

Лідогенератор (Lead Generator / Researcher) має багато суміжних моментів із роботою менеджера з продажу. Це фахівець, який шукає клієнтів, налаштовує рекламу, моніторить соціальні мережі [4].

Таким чином, професія менеджера з продажу в IT – компанії є не лише перспективною та високооплачуваною, але і захоплюючою та надзвичайно цікавою. Особливостями цієї роботи є отримання безцінного досвіду у сфері B2B продажів та знань в IT сфері. Крім того, менеджер з продажу в даній сфері навіть передбачає професійне зростання чи зміну діяльності.

Список використаних джерел:

1. IT Рейтинг UA – перша діджитал екосистема України. IT рейтинг Украины. URL: https://it-rating.ua (дата звернення: 24.02.2023)

2. Work.ua – сайт пошуку роботи №1 в Україні. Work.ua – сайт пошуку роботи №1 в Україні. URL: https://www.work.ua (дата звернення: 24.02.2023).

3. Finance.ua | Фінанси в Україні | Курси валют, кредити, депозити, новини України. finance.ua. URL: https://finance.ua/ (дата звернення: 24.02.2023).

4. Li Guo, Chao-Lu Wu, Li Guo (2016). The Importance of Factors Influencing the Brain Drain of IT Employee. Series: Advances in Economics, Business and Management Research. Proceedings of the 2016 International Conference on Management Science and Management Innovation. DOI: 10.2991/msmi-16.2016.86

5. Oleksenko, Y., Makarenko, S. (2020). Features of it market development in Ukraine. P. 152-173. DOI: 10.30525/978-9934-588-38-9-31

Самойленко Н. В.

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

КРОСС-КУЛЬТУРНАЯ КОМПЕТЕНТНОСТЬ МЕНЕДЖЕРОВ

Сегодня количество кросс-культурных взаимодействий в деловой и личной жизни резко увеличилось. Это связано с открытием границ, активизацией внешнеэкономической деятельности Украины, глобализацией. Для украинских компаний, особенно для тех, которые ведут свою деятельность на международном и межрегиональном уровне, количество кросс-культурных рисков и возможностей постоянно растёт, что определяется самим ходом развития человечества.

Взаимодействие и столкновение разных культур встречается чаще, чем большинство менеджеров обращают на это внимание. Для того, чтобы соответствовать требованиям времени, современному руководителю целесообразно развиваться в вопросах кросс-культурного менеджмента. Изучение кросс-культурной темы помогает лучше узнать себя, идентифицировать свой культурный профиль, а значит, сделать менеджеров более успешными в бизнесе (увеличить потенциал компании, её стоимость), избежать нежелательных последствий для личной жизни, карьеры и бизнеса (предотвратить ситуации, ведущие к потере прибыли).

Что такое кросс-культура? Словосочетание «кросс-культура» состоит из двух слов: «cross» и «culture»; в переводе с английского языка - «пересечение культур». Существуют различные трактовки словосочетания «кросс-культура» - это общение, взаимодействие представителей различных культур, сотрудничество и коммуникация «на стыке культур», «на пересечении культур», «на столкновении культур». Это многообразие показывает деликатность, проблематичность темы. Сложность кросс-культурного взаимодействия ещё обуславливается частой неосознанностью своей культурной специфики многих вступающих в него людей. Аксиомы кросс-культурного взаимодействия гласят: культура видна в сравнении; плохих культур не бывает, бывают просто разные культуры; все культуры разные, но равные.

Предлагаю выделить бизнес-ситуации, в которых проявляется, формируется, создается кросс-культура. Так, наиболее характерными областями социально-экономической деятельности бизнес-организаций, где

происходит пересечение, взаимодействие, столкновение разных культур, являются: управление международным и межрегиональным бизнесом; взаимодействие профессиональных субкультур в бизнесе; управление ценностями компании; коммуникация с внешней средой компании; маркетинг; управление человеческими ресурсами; переезд, трудоустройство и карьерный рост в другом регионе, стране. Логично, что деятельность в кросс-культурных условиях создает для участников одновременно специфические возможности и риски, а управлять такими ситуациями призван кросс-культурный менеджмент.

Кросс-культурный менеджмент - новая область знания для Украины, это менеджмент, осуществляемый на стыке культур, подразделяющийся на:

1) макроуровень - управление на стыке национальных и региональных культур;

2) микроуровень – управление на стыке локально-территориальных, возрастных, профессиональных, организационных, иных культур.

Предмет кросс-культурного менеджмента - это управление деловыми отношениями, возникающими на стыке разных культур, включающее:

1) создание толерантного взаимодействия и коммуникаций, условий плодотворного труда и успешного бизнеса на пересечении разных деловых культур;

2) регулирование межкультурных конфликтов в бизнес-среде;

3) развитие кросс-культурной компетенции собственников бизнеса, менеджеров, персонала.

Украинские компании, ведущие внешнеэкономическую деятельность, постоянно сталкиваются с трудностями в области кросс-культуры и понимают всю значимость информации о менталитете, ценностях и национальных традициях клиентов, партнеров, потенциальных сотрудников, которые являются носителями иных культур.

Взаимодействие профессиональных субкультур в бизнесе. Выделяется большое разнообразие профессиональных субкультур в одной социально-экономической среде. Например, многие могут вспомнить особую атмосферу внутри компании бухгалтеров или отдела продаж, особый колорит общения обслуживающего персонала между собой, социально-культурное отличие бывших работников силовых органов от представителей творческих профессий и науки.

Перечисленные здесь субкультуры контактируют между собой, как правило, только по формальным вопросам, что обуславливается самой принадлежностью к разным профессиональным субкультурам. Говоря о ситуациях взаимодействия профессиональных субкультур, важно отметить,

что при их пересечении риск возникновения неблагоприятных последствий бывает довольно высоким.

Кстати, трудности могут возникнуть и внутри одной субкультуры, если во взаимодействие вступают представители разных поколений (фактически – также представители разных культур). Например, сложно договориться, понять друг друга менеджерам разного поколения. Так, при переговорах между «красным директором» и молодым топ-менеджером, выпускником MBA, высок риск недоговоренности по вопросам стратегического менеджмента, HR и PR-менеджмента. Причина – в разнице образования, управленческого мировоззрения и управленческого мышления, профессиональном и жизненном опыте, стереотипах, возрасте. В таком случае, при подготовке к переговорам целесообразно тщательно продумать коммуникацию с представителем другого поколения, другой культуры (национальной, религиозной, локальной, и т. п.) и субкультуры.

Столкновения различных культур и субкультур ведут к конфликтам, понижению потенциала компании, отрицательной синергии организации. Противостояние между профессиональными субкультурами в одной компании может и должна нивелировать корпоративная культура.

Создание и управление кросс-культурным капиталом, на мой взгляд, включает такие характеристики:

1. культурный и кросс-культурный подход введён в идеологию, миссию, стратегию бизнеса компании, во все сферы деятельности организации: управление международным и межрегиональным бизнесом; коммуникация с внешней средой компании; управление человеческими ресурсами; маркетинг; управление ценностями компании; взаимодействие профессиональных субкультур в бизнесе (в т.ч. взаимодействие разных поколений);

2. планомерная, целенаправленная, регулярная работа со «сходствами» и «различиями» в областях, наиболее «уязвимых» для кросс-культурных рисков: для некоторых компаний – это HR-менеджмент, для других – маркетинг, а для третьих – PR-менеджмент, и т.д.;

3. разработка и реализация системы адаптации корпоративной культуры компании к национальным, региональным, локально-территориальным особенностям базирования филиалов, подразделений, отдельных проектов;

4. создание и управление уникальной для организации системой смягчения кросс-культурного шока, вызванного действиями компании во внутренней среде (персонал, экспаты и их семьи) и во внешней среде (потребители, клиенты, местное общество);

5. введение в HR-менеджмент кросс-культурного подхода, в т.ч. разработка и реализация кросс-культурной компетенции персонала компании, обучение и развитие персонала по межкультурной теме с привлечением внутренних и внешних ресурсов организации, включение кросс-культурного элемента в процесс подбора, оценки, ротации персонала;

6. создание, поддержание и интенсивное использование корпоративной информационной базы на кросс-культурную тему:

- накопление специальных кейсов, необходимых компании в разных ситуациях;
- организация корпоративной библиотеки со специальной литературой, справочными материалами, словарями иностранных языков;
- введение специального раздела на внутрикорпоративном сайте компании с целью создания базы данных по межкультурной теме и обменом опыта персонала по прошлым и текущим сложным кросс-культурным ситуациями (например, выход из межкультурного конфликта, создание многонациональной команды, продвижение на межрегиональном и международном рынке, коммуникация с клиентами и партнерами из иной культурной среды, др.);
- регулярные групповые фасилитационные сессии по актуальным кросс-кульутрным вопросам, проблемам, ситуациям.

Создание кросс-культурного капитала способствует интенсивному развитию руководителя в межкультурной теме, однако требует вложения всех возможных ресурсов, т. к. помогает избежать рисков - потери прибыли, репутации компании и её менеджмента.

Список использованных источников:

1. Мясоедов С. П. Управление бизнесом в различных деловых культурах. М., Издательство: Вершина, 2009. С.284.

2. Триандис Г. Культура и социальное поведение. – М.: Форум, 2007. – 384 с.

3. Gesteland, Richard R. Cross-Cultural Business Behavior. Copenhagen: Copenhagen Business School Press, 1996

Сладецький Р. А.

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

ОРГАНІЗАЦІЯ РОБОТИ КОМАНДИ ДЛЯ СТВОРЕННЯ НОВОГО ІТ ПРОДУКТУ

Більшість розробників стартап проектів вважають наявність оригінальної ідеї своїм ключовим фактором успіху. Проте, відсутність поруч людей, які здатні не лише повністю зрозуміти сутність ідеї автора, а й максимально ефективно реалізувати її, незважаючи на наявність різного роду перепон та несприятливих факторів, загрожує тим, що стартап проект взагалі не відбудеться. Команда стартапу на початкових етапах, зазвичай складається з друзів та однодумців, але з розвитком проекту та зростанням масштабів його реалізації постає потреба у залученні професіоналів у різних сферах (маркетинг, фінанси, продажі, операційна діяльність, залучення інвестицій тощо). Тому формування злагодженої команди є чи не найголовнішим питанням для успішного розвитку стартап проекту [2].

Команда проекту створюється керівником проекту — юридичною особою, якій замовник делегує права по управлінню проектом в обсязі, визначеному контрактом.

Задачею керівника проекту при формуванні команди є підбір членів команди, які забезпечували б:

- відповідність кількісного і якісного складу команди цілям і вимогам проекту;
- ефективну групову роботу по управлінню проектом;
- психологічну сумісність членів команди і створення активної стимулюючої «внутрішньопроектної» культури;
- розгорнуте внутрішньогрупове спілкування і вироблення оптимальних групових розв'язань проблем, що виникають під час реалізації проекту.

Керівник проекту призначає проект-менеджера, що здійснює загальне керівництво проектом, контролює його основні параметри і координує діяльність членів команди. Менеджер проекту визначає необхідну кількість фахівців членів команди, їх кваліфікацію, проводить відбір і найм працівників [4].

Формуючи команду, проект-менеджер збирає разом групу людей, намагаючись об’єднати їх загальною ціллю і єдиними задачами. Новизна,

унікальність, ризик і швидкоплинність — всі ці риси притаманні новому проекту, вони ж і визначають труднощі при формуванні команди. Створення команди для нового проекту ускладнено ще й тим, що ці люди не працювали разом, не мають загальних цінностей і норм, але повинні працювати ефективно і синхронно. Необхідний тривалий час, щоб всередині групи виникло командне почуття, щоб встановились загальні норми, стандарти і цінності. Щоб проект був успішним, згрупування людей повинно відбутися до того, як команда почне працювати на повну потужність.

За формою команда проекту відображає існуючу організаційну структуру управління проектом, розділення функцій, обов'язків і відповідальності за рішення, що приймаються в процесі його реалізації. На верхньому рівні структури знаходиться менеджер проекту, а на нижніх — виконавці, відділи і фахівці, що відповідають за окремі функціональні сфери.

За змістом команда проекту є групою фахівців високої кваліфікації, що володіють знаннями і навичками, необхідними для ефективного досягнення цілей проекту.

Розуміння, скільки і яких людей потрібно проекту, складається на момент завершення роботи над передпроектною аналітикою. Коли відомий масштаб робіт та ключові завдання, легше спрогнозувати кількість майбутніх працівників. Наймати програмістів та інших IT-працівників мають IT-директор та начальник відділу управління. Перший зможе оцінити інструментарій та рівень володіння ним, другий – зрозуміти, чи спрацюється новий співробітник із командою IT-фахівців [5, с. 66].

Звичайно ж, усі компанії різні: у них різні бізнес-мети, вони стикаються з різними проблемами та, відповідно, впроваджують різні технології. Все це відбивається на структурі та розмірі їх IT-відділів. Вони можуть дуже відрізнятися один від одного. Проте можна простежити деякі закономірності. Як правило, команди формуються навколо певних функцій. У цій статті ми поговоримо про найбільш поширені типи IT-команд, їх ролі та обов'язки.

Те, які у компанії є підрозділи в IT-команді, залежить від завдань, які потрібно виконувати. Як правило, йдеться про такі функції:

- Обслуговування IT-систем. IT-команди стежать за тим, щоб IT системи компанії працювали належним чином, а також займаються їх оновленням у разі потреби.
- Автоматизація процесів. IT-команди впроваджують технології, що найбільш підходять для автоматизації тих чи інших бізнес-операцій.
- Інтеграція систем. IT-команди відповідають за коректну спільну роботу всіх систем, що використовуються в компанії.

- Управління даними. IT-команди організовують збирання, зберігання, захист та обробку даних.
- Забезпечення кібербезпеки. IT-команди відповідають за захист систем, мереж, пристроїв та даних у компанії.
- Надання технічної підтримки. IT-команди допомагають користувачам вирішувати питання щодо роботи програмного забезпечення або пристроїв [1, с. 318].

Більшість людей уявляє IT-відділ як групу експертів у технологіях. Проте в IT-командах є різні посади і багато хто з них вимагає більше творчих талантів або бізнес-навичок, ніж технічних знань. Розглянемо найбільш поширені професії:

- Менеджер проекту відповідає за планування та виконання всіх завдань щодо проекту. Він чи вона координує роботу різних команд, спостерігає за всіма процесами та стежить за тим, щоб усе виконувалось у встановлені терміни та проект залишався в рамках бюджету.
- IT-аналітики аналізують усі організаційні процеси у компанії, вивчають вже існуючі інформаційні системи та займаються пошуком можливостей для оптимізації роботи.
- Розробники — це ті люди, які пишуть код. Вони створюють програмне забезпечення, використовуючи різні мови програмування. Back-end розробники будують внутрішню логіку і функціональність продукту, а front-end розробники, своєю чергою, працюють над елементами, із якими взаємодіють користувачі.
- QA-фахівці стежать за якістю продукту, тестують його та виявляють недоліки, які необхідно усунути.
- UI та UX дизайнери зосереджені на ефективній взаємодії між кінцевими користувачами та додатком. Вони проектують інтерфейс таким чином, що продукт виглядає привабливо і зручно ним користуватися.
- Фахівці з аналізу даних займаються збором, перевіркою та аналізом даних, дозволяючи цим підприємствам приймати рішення на їх основі.
- Solution архітектори проектують IT-системи і стежать за тим, щоб нове рішення добре працювало спільно з застосовуваними в компанії.
- Фахівці з кібербезпеки захищають організації від кіберзагроз та атак. Їхнє завдання — передбачати та запобігати можливим проблемам.
- IT-адміністратори відповідають за встановлення, обслуговування та налаштування обладнання, програмного забезпечення та мереж у компанії.

В організаціях, де застосовуються сучасні підходи (Agile, Scrum), посадові обов'язки деяких фахівців, наприклад, розробників, адміністраторів та фахівців із забезпечення якості, можуть перетинатися [3, с. 65].

Отже, ІТ-команди можуть складатися із різних підрозділів, а назви посад варіюються від компанії до компанії. Але доки робота кожного фахівця узгоджується із загальною стратегією та бізнес-цілями організації, структура ІТ-відділу не така важлива. Однак, необхідно, щоб кожен підрозділ мав чітке розуміння своїх обов'язків та зони відповідальності. Тільки так можна домогтися того, щоб компанія процвітала в сучасному швидко змінюваному світі технологій.

Список використаних джерел:

1. Виноградський М. Д., Бєляєва С. В., Шкапова О. М. Управління персоналом: Навчальний посібник. – К.: Центр навчальної літератури, 2021. – 504 с.

2. Копішинська К. А. Ключові засади формування команди стартап проекту. Спільнота. Економіко-правові дискусії. 2017. 27 травня. URL: http://www.spilnota.net.ua/ua/article/id-1875

3. Кучеренко В. Р., Маркітан О.С. Управління діловими проектами: Навчальний посібник. – К.: Центр навчальної літератури, 2020. – 280 с.

4. Ладика І. Що таке стартап-інкубатор і як туди потрапити? Studway. 2017. 13 березня. URL: https://studway.com.ua/startapinkubator

5. Ситник Н. І. Концептуальні основи стартапів: їх сутність і класифікація. Бізнес Інформ. 2016. №8. С. 64-68.

Топчій О. Д.

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

ЗАСТОСУВАННЯ СУЧАСНИХ ІНСТРУМЕНТІВ ІНТЕРНЕТ-МАРКЕТИНГУ ДЛЯ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА НА РИНКУ НЕРУХОМОСТІ

Інтернет-маркетинг на ринку нерухомості може бути дуже вигідним та ефективним. За допомогою цифрового маркетингу компанії можуть охопити цільову аудиторію, одночасно створюючи тривалий вплив на них. Оскільки більшість потенційних покупців шукають квартири та будинки онлайн, інтернет-інструменти стали рішенням як для продажу вторинної нерухомості між фізичними особами, так і для великих забудовників первинної нерухомості. У порівнянні з друкованими та ефірними ЗМІ інтернет-маркетинг виявляється одним із найефективніших. Він робить майже однакову роботу менш ніж у половині загальних витрат, при цьому отримуючи швидкі доходи.

Ефективність використання інтернет-простору для продажу нерухомості підтверджується опитуванням 2019 року компанією ResearchMe 3000 користувачів, які мали досвід придбання житла за останні 3 роки та тих, хто планує покупку найближчим часом. За даними опитування, половина покупців планує шукати квартиру за допомогою сайтів-агрегаторів оголошень, 38% на офіційних сайтах забудовників, 23% у мобільних додатках та близько 16% звернуться до соціальних мереж. Ті, хто вже зробив свій вибір, найчастіше зверталися до ріелтора, але після самостійного вивчення пропозицій забудовників [1].

Розглянемо найбільш актуальні інструменти сучасного маркетингу, які спираються на інноваційний потенціал інтернет-технологій та можуть бути використані для підвищення конкурентоспроможності підприємства на рінку нерухомості.

1. Онлайн-управління репутацією та крауд-маркетинг

Нерухомість – це бізнес, у якому імідж та репутація є критичними. Інтернет-огляди безпосередньо впливають на те, як люди витрачають свої гроші. Перетворення відгуків на продажі важливе в більшості галузей, але для нерухомості це важливо з двох причин:

Купівля чи продаж будинку – це складний процес фінансово та юридично. Нерухомість має великий життєвий цикл покупки.

Отримання відгуків допомагає збільшити лояльність себе. Якщо клієнт залишився задоволений – компанії використовують усі можливості та методи стимулювання, щоб зафіксувати його позитивний досвід та використовувати його для покращення іміджу [2].

Для цього можна використовувати крауд-маркетинг – аналіз цільової аудиторії, позиціонування в соціальних мережах, блогах, форумах певної тематики.

2. VR-маркетинг та 3D-тури

Демонстрація майбутньої квартири – ще один спосіб втримати увагу користувача та відпрацювати частину заперечень. Можна показати різні планування та варіанти ремонту, тому клієнтам буде простіше прийняти рішення про купівлю [3].

Згідно з дослідженням VRARA, 40,4% покупців квартир підтвердили, що панорамні тури відіграють важливу роль у прийнятих рішеннях про покупку. 72,7% клієнтів, яким забудовники запропонували панорамні тури, позитивно оцінюють цей інструмент. А також 45,2% покупців квартир підтверджують, що 3D- та VR-контент допомагають прийняти рішення про купівлю швидше, ніж тільки 2D-планування [4].

Віртуальні інструменти збільшують свою популярність у багатьох сферах, зокрема на ринку нерухомості. Про це також свідчить дослідження, згідно з результатами якого, у 2016-2021 роках обсяг світового ринку обладнання AR та VR збільшувався в середньому на 58% щорічно та досягнув 99,4 млн. одиниць за цей період. Як результат - до 2021 ринку збільшився майже в 10 разів [5].

Однак, віртуальна прогулянка квартирою - це не інструмент прямих продажів. Вона не відповідає на найважливіші питання, які цікавлять клієнта: ціна, підстави для укладення угод, договірні відносини, права компаній на земельну ділянку. Існує величезний блок технічних та юридичних питань, який неможливо виключити з процесу. Ніякі демонстраційні та іміджеві рішення не можуть на 100% впливати на вибір людини. Але вони можуть допомогти зробити його у користь компанії, що їх використовує.

3. Відео-маркетинг

Відео-маркетинг у сфері нерухомості – один із найкращих способів отримати більш якісні потенційні ліди. Це тому, що потенційних покупців легше переконує візуальний рівень. Нерухомість сьогодні також покладається на візуальну привабливість - відео допоможе виглядати об'єкту

більш привабливим, що може збільшити довіру клієнта до компанії-забудовника [2].

Завдяки смартфонам сьогодні простіше, ніж будь-коли ділитися та поширювати відео. Саме тому дедалі більше фахівців схиляються до відео-маркетингу як інструмент збільшення ROI бізнесу [7].

4. Маркетинг у соціальних мережах

Звіт національної асоціації ріелторів свідчить, що 77% ріелторів активно використовують соціальні мережі для нерухомості у тій чи іншій формі. Компанії використовують сервіси, такі як Facebook, LinkedIn, Instagram, YouTube, Twitter та Snapchat, щоб залучати та спілкуватися з існуючими клієнтами та потенційними покупцями.

Типи маркетингу у соціальних мережах:

Органічний. Це обмін неоплаченими публікаціями та оновленнями на сторінках компанії у соціальних мережах. Вони включають текстові, графічні та відео повідомлення, повідомлення з хештегами, посиланнями тощо.

Платний. Цей вид маркетингу у соціальних мережах передбачає окремий бюджет на просування та включає спонсорські публікації, текстові, графічні та відеореклами тощо [2].

Нерухомість - одна з найскладніших категорій з точки зору ухвалення рішення про покупку. Потенційні покупці вивчають і порівнюють безліч варіантів, що, у свою чергу, сприяє розвитку онлайн-агрегаторів, що збирають масив пропозицій в одному місці. На висококонкурентному ринку складно виділитися, тому рекламодавці активно переходять у digital. Зростає інтерес компаній до найбільш конверсійних форматів – відеореклами, просування в соціальних мережах та ремаркетингу. Сучасні онлайн-інструменти дозволяють побудувати ефективну тривалу комунікацію з цільовою аудиторією та провести користувача через весь шлях – від першого контакту з рекламою до покупки.

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. Стратегії цифрового маркетингу нерухомості [Електронний ресурс] – Режим доступу: https://www.innoservdigital.com/blog/

3. Digital-інструменти для ринку нерухомості у 2020 році [Електронний ресурс] - promedia.io/blog

4. Міжнародна корпорація даних (IDC): Використання технологій віртуальної та доповненої реальності у бізнесі [Електронний ресурс] – Режим доступу: https://www.idc.com/

5. *Офіційна сторінка Асоціації VR/AR технологій [Електронний ресурс] – Режим доступу: https://www.thevrara.com/*

6. *Ефективне використання VR на ринку нерухомості [Електронний ресурс] – Режим доступу: www.cossa.ru/special/realty/*

7. *Статистика інтернет-маркетингу [Електронний ресурс] – Режим доступу: www.sostav.ru*

Чернявский В. И.

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

КАК НАЧАТЬ РАБОТУ С EMAIL МАРКЕТИНГОМ

Email маркетинг – один из самых надежных маркетинговых каналов. Несмотря на огромное количество появляющихся социальных сетей, email маркетинг обеспечивает наилучшие результаты. Email маркетинг одинаково хорошо работает для крупного, среднего и малого бизнеса.

Сегодня мы рассмотрим, как спланировать работу с email маркетингом, и как создать email маркетинговую стратегию.

Вот что вы сегодня узнаете:

- Почему вам нужен email маркетинг
- Как создать стратегию email маркетинга и подготовить базу email адресов для рассылки
- Какие показатели необходимо отслеживать в email маркетинге

Почему вам нужен email маркетинг

Email маркетинг имеет один из самых больших показателей рентабельности инвестиции среди всех маркетинговых каналов. Помимо этого, для 60% потребителей email коммуникация остаётся предпочтительным каналом связи.

Email маркетинг позволяет достигать различных бизнес целей, например:

- Увеличение объёма продаж
- Управление интернет-траффиком сайта
- Информирование и обучение клиентов
- Повышение узнаваемости бренда

Так же огромным плюсом email маркетинга является возможность комбинировать его с другими маркетинговыми каналами, такими как социальные сети, web сайт, реклама и т.д.

Подготовка к email маркетингу

Первый шаг подготовки к email маркетингу – это выбор email провайдера (ESP). Email провайдеры помогают создавать и рассылать email маркетинговые кампании. Сейчас на рынке очень много различных email провайдеров. Все они имеют плюс-минус схожий функционал. Выбирайте тот, с которым вам будет удобно работать.

Ключом к успешному email маркетингу является постоянный рост подписчиков на email рассылку. Каждый подписчик — это возможный будущий покупатель. Для роста базы подписчиков необходимо разместить у себя на сайте форму подписки на рассылку. Для обеспечения попадания в лист рассылки только проверенных email адресов, форма подписки должна быть с подтверждением контактной информации на email.

По мере роста базы подписчиков, целесообразно поделить базу на сегменты. Вот пример признаков, подходящих для сегментирования:

- Географический
- Демографический
- Взаимодействие с прошлыми email письмами (например, переход по ссылке)
- Информация о прошлых покупках

Сегментирование базы позволяет подготавливать более релевантный контент для каждого сегмента, что в свою очередь ведет к повышению конверсии на всех этапах маркетинговой воронки.

Зачастую для достижения результата маркетинговой кампании мало отправить одно письмо. Для email маркетинга используются цепочки писем. Письмо 1, письмо 2 и т.д. Важно сразу создать контент календарь, который включает для каждого запланированного письма следующее:

- Цель письма (например, повышение вовлеченности, промоакция)
- Дата и время отправки
- Тема письма
- Содержимое письма
- Призыв к действию
- Список получателей
- Автор письма

На основе такого календаря создается автоматическая рассылка.

Тестирование и отслеживание результатов

К сожалению, невозможно раз и навсегда настроить email маркетинг. Какой-то контент в рассылке получает лучший отклик, какой-то, наоборот. Поэтому важно экспериментировать с контентом, стратегией, сегментацией базы и отслеживать результаты.

Для этого используется A/B тестирование. Разным частям аудитории отправляется разный контент и потом сравниваются результаты. На основании этого выбирается тот подход, который показывает лучшие результаты и применяется на всю аудиторию. Вот основные характеристики email маркетинга, которые важно отслеживать:

- Процент доставки писем
- Процент открытия писем
- Процент перехода по ссылкам в письмах
- Процент попадания писем в спам
- Процент отписавшихся от рассылки
- Возврат инвестиций от рассылки
- Средняя прибыль от письма

Комбинация данных характеристик позволит определить успешность маркетинговой кампании, а также даст необходимую информацию для дальнейших улучшений. Например, низкий процент открытия писем может свидетельствовать о неправильно подобранной теме письма. Или низкий процент перехода по ссылкам в теле письма может говорить о слабом контенте или невыраженному призыву к действию.

Email маркетинг является одним из основных инструментов современного бизнеса. И хоть он не приносит мгновенных результатов, но в долгосрочной перспективе позволяет достигать ошеломительных результатов и обеспечивать конкурентоспособность любого бизнеса. Email маркетинг долгий процесс, с лихвой окупающий затраченные усилия.

Mykyta Bobniev

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

DIGITALISATION OF BUSINESS PROCESSES

1. Digitalisation of Business Processes is a key driver for increased efficiency and productivity in modern business.

In the modern world with a new economy, when modern life is completely connected with technology, the need for digitalization of business processes is obvious.

All modern business is closely connected with technologies and computer solutions. The effectiveness of modern technologies has long been proven by society and large market demand. Thus, we can say that for the effective development of modern business and its business processes, digitalization of all business processes is an absolutely necessary component. After all, this is an important component of business efficiency.

2. The use of digital technologies for automating and streamlining business processes can lead to reduced costs, increased revenue, and enhanced customer experience.

It is obvious that the use of digital customer registration systems, task tracking, calculation of the time spent on tasks, a missed call control system, electronic calendars and other digital tools will improve the efficiency of working with clients. It is also clear that the use of digital documents, e-mails, and signing documents with an electronic signature significantly reduces costs.

3. The integration of digital technologies into business processes requires a clear understanding of the benefits and challenges associated with the adoption of new technologies.

Every founder, CEO and other change agent who will introduce digital solutions into the company's business processes must clearly understand why he is doing it. What is the main goal? But what problems will be encountered in this way?

All these questions should be clearly spelled out in the plan for digitization of the company's business processes. It should be a clearly structured document (road map) in which all the steps on the way to digitization should be written.

4. The development of effective digital strategies is essential for businesses seeking to leverage the potential of digitalisation in their operations.

The digitization plan (road map) should be detailed and approximated to the type of strategy.

The most precise, detailed strategy for the digitization of business processes is the key to the successful implementation of this strategy

5. Successful digital transformation initiatives require strong leadership, effective change management, and a commitment to ongoing learning and development.

Initiatives regarding the digital transformation of business processes should come from the company's founders or CEO. They should be visionaries, initiators and implementers of these transformations.

For this, founders or CEOs must constantly acquire new knowledge. The process of learning and studying new market and business trends should be a common skill of such managers.

Through these changes, they must communicate the importance of transformation to their team.

6. The digitalisation of business processes presents both opportunities and risks, requiring careful assessment and management to ensure optimal outcomes.

In order for the digital transformation process to be successful, founders or CEOs must consider all possible risks when developing a strategy and carefully write a plan for dealing with these risks.

One of the main risks may be the team's lack of support for these changes, and sabotage on the way to transformation.

In order to prevent negative consequences in the process of perception of the transformation by the work team, it is necessary to build the most transparent and regular communication with the staff, where the importance of the necessary changes should be consistently and easily communicated.

7. Digitalisation can enable businesses to innovate and create new products and services, opening up new markets and opportunities for growth.

The importance of digital transformation also lies in the fact that it creates a platform for further innovation in the company, which is so necessary for the future development of the business.

A digital platform built as a result of digitization will provide an opportunity to quickly implement, test, analyze, correct and deploy new business and innovative solutions.

8. The digitisation of business processes also requires investment in infrastructure, including hardware, software, and networking capabilities.

It should also be noted that the digital transformation strategy should include detailed calculations of all costs necessary for successful digitization.

It may seem that the costs of digitization can be unreasonably high, but it should be remembered that such costs are a contribution to the readiness to cope with irreversible market changes.

9. As the pace of technological innovation continues to accelerate, businesses must continually reassess their digitalisation strategies to stay ahead of the curve.

The ideal interval for reviewing and adjusting the transformation strategy is 3 years.

But founders and CEO must constantly monitor trends and changes in the market in order to quickly react to such changes and make timely changes to the transformation strategy.

11. The increasing adoption of digital technologies in business processes requires a shift in mindset, from a focus on traditional, hierarchical structures to more agile, collaborative models.

The transformation strategy should include regular work with the team, which should be aimed at conveying the importance of the digital transformation of the company's business processes, as well as the transformation of the team's vision and understanding of the business.

Maksym Bondarchuk

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

BRIEF OVERVIEW OF MANAGEMENT IN ANCIENT ROME LIFE

Management in ancient Rome refers to the methods and practices used by Roman leaders and administrators to govern and manage the vast empire that Rome controlled during its peak. The Roman Empire was one of the largest and most complex political entities in human history, encompassing much of Europe, North Africa, and the Near East. Given the size and complexity of the empire, effective management was essential to maintain order and stability.

One of the key features of Roman management was the hierarchical system of government, with a clear chain of command and well-defined roles and responsibilities. At the top of the hierarchy was the emperor, who held ultimate authority over the empire. The emperor was supported by a council of advisors, as well as a vast bureaucracy of officials and administrators, who were responsible for implementing the emperor's decisions and carrying out the day-to-day operations of government.

Another important aspect of Roman management was the use of legal and administrative institutions to maintain order and control. The Roman legal system, which was based on a complex set of laws and regulations, was used to enforce the emperor's will and maintain order throughout the empire. Additionally, the Roman army, which was one of the largest and most powerful military forces in the world at the time, was used to enforce the emperor's authority and protect the empire from external threats [1].

Despite the many successes of Roman management, there were also challenges and limitations. For example, the vast size of the empire and the diversity of its population made it difficult to impose a uniform system of governance and administration. Additionally, the lack of effective communication and transportation systems made it difficult to maintain control over distant regions.

The Roman management system was highly centralized, with power and authority concentrated in the hands of the emperor and his top officials. The emperor was the ultimate decision-maker and had the power to appoint and dismiss officials, as well as to pass laws and regulations. The emperor was also responsible for leading the army and ensuring the security of the empire [2].

One of the key institutions in Roman management was the Senate, which was a body of elite citizens who advised the emperor on matters of governance and policy. The Senate also played a role in the administration of justice, as senators often served as judges in legal cases.

Another important aspect of Roman management was the use of provinces and governors to govern the empire's territories. Provinces were large geographical areas within the empire, and each province was governed by a governor appointed by the emperor. Governors were responsible for maintaining order, collecting taxes, and carrying out the emperor's policies within their provinces.

One of the challenges of Roman management was the task of maintaining order and control over such a vast and diverse empire. To address this challenge, the Romans developed a highly organized and efficient military system, which was used to maintain order and defend the empire against external threats. The Roman army was composed of professional soldiers and was highly disciplined and well-trained [3].

Another challenge of Roman management was communication and transportation. To address this challenge, the Romans built a network of roads and highways that connected the various regions of the empire, making it easier for troops, officials, and goods to move from one place to another. Additionally, the Romans developed a system of couriers and messengers to carry messages and news across the empire.

Despite these challenges, Roman management was highly effective in maintaining order and stability throughout the empire. The legacy of Roman management can be seen in the many institutions and practices that continue to influence modern systems of government and administration, such as the hierarchical system of government, the use of legal and administrative institutions, and the importance of efficient communication and transportation systems.

The success of Roman management was also due in large part to the administrative skills of Roman officials and administrators. The Roman bureaucracy was well-organized and efficient, and officials were trained in the tasks of governance and administration. Additionally, the Romans had a strong tradition of record-keeping, which helped to ensure that information was accurate and up to date [4].

Another important feature of Roman management was the use of law and order to maintain stability and control. The Roman legal system was based on a set of written laws and regulations, which were applied uniformly throughout the empire. This helped to ensure that everyone, regardless of their status or position,

was subject to the same laws and regulations. Additionally, the Roman courts were impartial and just, and provided a means for citizens to seek justice and resolve disputes.

The Roman Empire also placed a great emphasis on public works and infrastructure, which were key to the success of its management system. For example, the Romans built a vast network of roads, aqueducts, and public buildings that served the needs of the empire's population. These public works projects helped to promote commerce and communication, and also served to enhance the prestige of the Roman state.

It is also worth noting that the Roman management system was highly adaptable and flexible, which allowed the empire to respond effectively to changing circumstances. For example, when the empire faced internal or external challenges, the Romans were able to adjust their policies and practices to meet the needs of the moment. This flexibility and adaptability helped to ensure the long-term success of the Roman Empire [5].

In conclusion, the success of Roman management was due to a combination of factors, including a well-organized and efficient bureaucracy, a strong tradition of record-keeping, a commitment to law and order, a focus on public works and infrastructure, and an adaptable and flexible approach to governance. The legacy of Roman management continues to influence modern systems of government and administration and provides important lessons for contemporary leaders and managers.

References:

1. *Kelly, C. (2006). The Roman Empire: A Very Short Introduction. Oxford University Press, pp. 45-60.*

2. *Grant, M. (1978). A History of Rome. Charles Scribner's Sons, pp. 120-140.*

3. *Bowman, A. K., & Wilson, A. (2010). The Oxford Handbook of Roman Studies. Oxford University Press, pp. 210-230.*

4. *Johnston, D. (1999). Roman Law in Context. Cambridge University Press, pp. 150-165.*

5. *Gwynn, D. M. (2007). The Roman Republic: A Very Short Introduction. Oxford University Press, pp. 70-85.*

Vitalii Ivanov

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

MODERN ASPECTS OF REMOTE MANAGEMENT OF A SOFTWARE DEVELOPMENT TEAM

Remote software development is not a new phenomenon and has been around since the moment of software as such. It is a process of creating software products that is carried out remotely using various technologies. The development of computers and computer networks, in particular, the global prevalence of the Internet (over 5 billion users in 2022) [1], data transfer rates [2], cloud solutions, and video conference technologists (VoIP) ensured, firstly, an increase of the technical quality of remote software development. Moreover, remote work can be more efficient than traditional office work, as developers can work most productively in their own environment. In addition, remote work gives you the opportunity to work with different clients, which gives you the opportunity to gain experience and improve your professional skills. The majority of software developers work from home, with 86 % currently working entirely remotely. Since the pandemic, the number of remote software engineer job roles has soared, and at least two-thirds of developers want it to continue that way in the future. Work-from-home culture is here to stay and is flourishing in the development community. [3].

Platforms for freelancers (Upwork, Weblancer, Freelancehunt and others) began to provide connections between the owner of the software and its developers based on their own view of the process organization [4]. For the most part, they are aimed at building, executing and guaranteeing the financial side of the process and do not provide a command workflow. The growing requirements for the quality, complexity and speed of software development require the involvement of not individual developers, but a team or teams, which makes freelancing very limited in terms of the scope of services.

In turn, scaled software products and enterprise-level solutions already use practices involving a large geography of engineers, sharing responsibility between representative offices in different countries, cities or districts. But there always exists an indivisible cell of software developers working together within the same office [5, 6]. This approach allows the team to maintain the necessary high level of communication to coordinate development.

It is important to mention that the Coronavirus pandemic contributed to the search for new organizational solutions and the separation of previously indivisible cells of developers.

In the management of fully remote team work, the following issues can be identified [6]:

1) communication - requires online communication as a skill for all team members;

2) organizational - as a new workflow approach to organize the software delivery process;

3) leadership - remote leadership goes beyond the usual view of this concept and requires additions;

4) coordination of working hours time zones;

5) intercultural - increases the requirements for tolerance of participants;

6) language - expects one common language of communication within one development process;

7) legalization - within labor laws of the country or countries.

To solve organizational problems, the usage of tools already widely spread in software development is great. In particular, project management systems - special programs that allow you to organize work on projects, set deadlines and tasks, assign responsibilities and track progress. They can also be used to share documents and discuss tasks. The next well-known systems, such as JIRA, Trello, Asana, are used [7]. The most popular - JIRA - stands out for its versatility, customization and integration with other tools.

Version control systems - GIT and remote repositories providing UI control: GitHub, BitBucket, GitLab - solve both organizational and communication problems. JIRA integration is recommended to help link versions, commits, and pull requests to specific ticket IDs in JIRA, thereby gaining more resources to manage the development process [8].

At first glance, powerful development of video conference tools (ZOOM, Slack, Google meet, Microsoft Teams) decreased communication problems, and they do not look so blocking remote work, but the practice has shown that even these tools must be used correctly. Moreover, additional skills are required for participants in organizing, taking part, listening and speaking in a video conference. Chats and instant messengers, such as Slack, are another effective tool for communication when working remotely. They allow you to exchange messages and files, as well as create group chats to communicate and discuss tasks. Chats and messengers can also be used to collaborate on documents and projects. The organization of the process according to Scrum/Kanban helps to solve the problem only partially and provides only a minimum set of activities to achieve the result.

The introduction of regular one-to-one meetings between cell members, as well as additional meetings in small groups, contributes to the growth of distributed communication in the development team and, as a result, the consistency of technical decisions made, which directly affects the quality of the developed software.

Remote work can lead to employee motivation problems. The lack of direct contact with colleagues and managers, as well as the lack of an office atmosphere, can lead to the fact that employees begin to lose interest in work and patience. It is also important that managers cannot control the work of their employees directly. This can lead to employees spending a lot of time on unnecessary tasks, which negatively affects productivity and quality of work. To solve such problems, the leader needs not only to effectively use modern advanced management tools, but also to learn remote empathy [9].

Forming a remote development team, time zones of its participants are very important, in the context of the intersection of working hours [6]. It is recommended to ensure that at least half of the working hours of the members of an indivisible development team overlap.

The development of tolerance and business ethics also plays an important role in the formation of a multi-team with a wide geography [10]. It is recommended to manage off-top communication and direct it to neutral, interesting topics.

Obviously, in modern software development, the first non-local universal language of communication is English. The level of English is a critical skill in the recruitment and formation of a remote team in different countries. The introduction of additional meetings described above also contributes to the improvement of understanding between the participants through the synchronization of vocabulary.

The problem of legalizing the work of team members located in different countries with different labor legislation and tax policies should be taken into account as well. It is recommended to consider this during planning the geography of the workforce and focusing only on certain countries or regions.

Despite the impediments, the following advantages can be distinguished:

1) reducing dependence on the local labor market - expanded geography allows you to attract more technically relevant candidates, as well as diversify human resources;

2) reduction of office operating costs - remote work does not require an office and providing employees with a workplace;

3) saving the mental and emotional resources of software developers, which could be spent on travel to and from the office, as well as on related

communication within the office, which in turn contributes to a better focus on the task.

The list of advantages can be expanded individually, however, it is obvious that the problems and advantages of remote software development come from the same features. The correct use of modern tools and adaptation of management will allow you to get more benefits by organizing remote software development for all stakeholders of this process.

References:

1. Global number of internet users 2005-2022. 2023. URL: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide.

2. Median Country Speeds December 2022. 2023. URL: https://www.speedtest.net/global-index.

3. Do Software Engineers Prefer to Work Remotely in 2023? A Deep Dive. 2023. URL: https://www.turing.com/kb/do-software-engineers-prefer-to-work-remotely.

4. Upwork Review- Why You Should Use it in 2023. 2023. URL: https://apploye.com/upwork-review.

5. Understanding the Role That Outsourcing and Globalization Has on Software Development. 2022. URL: https://apploye.com/upwork-review.

6. M. Rita Thissen, Susan K. Myers, R. Nathan Sikes, Jean P. Robinson and Valentina Grouverman. Globalization of Software Development Teams. 2011. URL: https://www.intechopen.com/chapters/17415.

7. Project management software and tools: Your best picks for 2023. 2023. URLt: https://asana.com/ru/resources/best-project-management-software.

8. Comparing Git Workflows: What You Should Know. 2018. URL: https://www.atlassian.com/git/tutorials/comparing-workflows.

9. 8 Tips for Empathy in Remote Workplaces. 2021. URL: https://twentyonetoys.com/blogs/future-of-work/empathy-tips-remote-workplaces.

10. Resolving Online Conflict: Dispute Resolution for Remote Workers. 2021. URL: https://www.stkate.edu/academics/women-in-leadership-degrees/dispute-resolution-for-remote-work-environments.

Artem Kozlov

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

PECULIARITIES OF TEAMWORK

In general, the effectiveness of the team is determined by the manager's ability to clearly outline the tasks, ensure their implementation with the necessary resources, encourage and control the activities of people and, if necessary, correct their actions. Group work has its own characteristics. First of all, it is effective when you need to quickly find the right solution to a problem that has arisen in the organization. Therefore, the team's ability to identify possible alternatives, choose the best one, agree on the method of its implementation, etc., is of great importance. For this, appropriate conditions should be created, taking into account that the process of identifying alternatives takes place by discussing the situation, arguing positions, and exchanging opinions between team members. Therefore, when determining the factors that affect the effectiveness of the team, in this section, you should pay attention to those that accompany the decision-making process. Such factors include:

- team size;
- team composition;
- group norms;
- cohesion of team members;

Team size. Management theorists have devoted much attention to determining the ideal number of team members. They established that a group consisting of seven plus - minus two people is optimal for management and interpersonal communication in the process of the activity. Such a team is the least conflictual and the most operational. In a group of fewer than five people, the creative potential decreases, not only due to a decrease in the number of ideas put forward but also due to the fact that the responsibility for the decisions made becomes more personalized and this forces to abandon some decisions that seem too risky[1]. A larger team is able to solve more complex and diverse tasks since its members have greater collective experience and knowledge, but a group of more than 9-10 people becomes difficult to coordinate, and its members may experience difficulties in declaring and justifying their opinions in front of others, which plays a particularly negative role when studying problems that do not have a clear solution. In addition, the increase in team size increases the tendency to avoid

work, and informal groups appear, the actions and intentions of which are often contradictory.

Team composition. In this context, the composition of the team takes into account the degree of similarity of its members in terms of points of view, and the approaches they show when solving problems. Experience shows that a group should consist of dissimilar people with different positions, ideas, ways of thinking, etc. Such a group will be able to work more efficiently, put forward and consider more alternatives, and therefore make more informed decisions.

Group norms. The norms adopted by the group significantly affect the behavior of an individual and the direction in which the group will work: to achieve the goals of the organization or to the contrary. Norms tell team members what behavior and what work is expected of them. Only compliance with the norms allows an individual to count on involvement in the team, its recognition, and support. But, if we consider the norms from the organization's point of view, then they can have not only a positive but also a negative character, i.e. hinder the achievement of its goals. The latter include theft, absenteeism, and destructive criticism of the company's activities. [2] Therefore, the manager should form such group norms that would create a motivational environment favorable to the company's goals and objectives (devotion to the company, protection of its interests, concern for product quality and customer service, teamwork, etc.). At the same time, it is worth noting that those norms that correspond to the mentality of employees are well-established and cultivated, and those that contradict them are not. So, for example, devotion to the company and orientation to collective work is extremely developed in Japanese management (which corresponds mainly to the communal nature of relations among Japanese people) and is weakly manifested in American management. Individual work is more encouraged there, as it provides higher results, which is the basis for the development of any firm. Therefore, an American worker changes his place of work if he sees that he cannot realize himself sufficiently in the old one. [3] Group norms and rules can play a decisive role in a person's decision to join a group. If they are recognized by all team members unconditionally, they speak of high team cohesion.

Team cohesion. This is a measure of the attraction of team members to each other and to the team. A high level of team cohesion increases the efficiency of the entire organization if the goals of both are aligned with each other. In cohesive groups, there are fewer communication problems, fewer misunderstandings, tension, mistrust, and higher productivity. The leader should do everything to unite the group and align its goals with the goals of the organization. At the same time, care should be taken to ensure that cohesion does not become group unanimity

when the pressure of the team on its individual members becomes excessive. [4] Group pressure is perhaps the strongest way to influence the behavior of a person within the collective, who, even if he is right, is forced to give way to him, in order to prevent conflicts from having a negative impact on the team's activities, it is necessary to direct them in a functional direction.

References:

1. *Warren Bennis , On Becoming a Leader, 1989, p. 101.*
2. *Stephen R. Covey, The 7 Habits of Highly Effective People: Powerful Lessons in Personal Change, 1989, p. 240.*
3. *Daniel Kahneman Thinking, Fast and Slow. 2002, p.375.*
4. *W._Chan_Kim, Blue Ocean Strategy, 2005. P.71.*

Artem Loktionov

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

THE USE OF AI-POWERED TOOLS FOR ENHANCING DAY-TO-DAY BUSINESS OPERATIONS: BENEFITS AND RISKS

The topic of AI-powered tools for enhancing day-to-day operations is a rapidly growing field in today's business world. The term AI - artificial intelligence - was coined in 1955 by John McCarthy, a math professor at Dartmouth who organized the seminal conference on the topic the following year (Brynjolfsson and McAfee). With the advancement of technology, AI has become an integral part of our lives, and various industries are embracing it to improve their operational efficiency. AI-powered tools are now being used to automate tedious and repetitive tasks, analyze data to generate valuable insights, and improve decision-making processes. This paper explores the benefits and risks of AI-powered tools usage in business operational activities, providing the theoretical justification along with the real-world examples and case studies.

There are several benefits of using AI-powered tools in day-to-day operations. Some of these benefits include increased work efficiency, improved accuracy, cost savings, enhanced customer experience, improved work safety, and improved scalability. The following paragraphs will concentrate on examples of how AI-powered tools have translated into tangible improvements in company operations.

Increased efficiency is one of the most significant benefits of using AI-powered tools in business operations. One area where AI-powered tools have made a significant impact is the banking industry. Chatbots and virtual assistants have been implemented by many banks to automate customer service interactions and provide customers with instant assistance without having to wait on hold for a human representative. According to a report by Juniper Research, chatbots and virtual assistants in the banking industry will save an estimated 862 million hours of customer service time by 2023, representing a significant improvement in efficiency (Gohil).

A recent article by Gohil in Forbes highlights how banks are leveraging AI-powered tools like chatbots and virtual assistants to improve their customer service and streamline their operations. For example, Bank of America's virtual assistant, Erica, has helped the bank process more than 160 million requests since its launch

in 2018. Similarly, Capital One's chatbot, Eno, has helped the bank automate routine tasks like checking account balances and paying bills, allowing human representatives to focus on more complex tasks (Gohil).

Improved accuracy is one of the other key benefits of using AI in company operations, particularly in the healthcare industry. AI-powered tools can analyze medical images and provide accurate diagnoses, helping to reduce human error and improve patient outcomes. For example, a study conducted by Google found that an AI algorithm was able to accurately detect breast cancer in mammograms with a lower false-positive rate than human radiologists (McCarthy).

According to a recent article by McCarthy in The Guardian, AI-powered tools are transforming the field of radiology by improving the accuracy of diagnoses and reducing the time it takes to analyze medical images. For example, researchers at Stanford University have developed an AI algorithm that can diagnose pneumonia with a higher accuracy rate than human radiologists. Another example is the use of AI to analyze MRI scans, which can help identify early signs of Alzheimer's disease (McCarthy).

Cost savings is another major advantage of using AI-powered tools in business operations. One example of how AI-powered tools have enabled cost savings is in the retail industry. Amazon has implemented AI-powered robots in its warehouses to automate the picking and packing of orders, which has reduced labor costs and increased order fulfillment speed (Albanesius).

According to a recent article by Albanesius in PCMag, Amazon has been using AI-powered robots in its warehouses since 2012. These robots are equipped with sensors and cameras that allow them to navigate the warehouse and pick up items to fulfill customer orders. By automating this process, Amazon has been able to significantly reduce its labor costs and increase its order fulfillment speed, enabling the company to deliver products to customers more quickly and efficiently (Albanesius).

As AI technology continues to develop and become more accessible, we can expect to see even more benefits and improvements across various industries. However, while there are many benefits to using AI-powered tools in day-to-day operations, there are also several challenges and potential risks associated with their use. Some of the most significant challenges and risks include data bias, cybersecurity risks, ethical concerns, lack of transparency, and integration challenges.

A recent article by Ross in Wired highlights the issue of data bias in AI algorithms. The article explains how biased data can lead to discriminatory outcomes, citing examples such as facial recognition software that misidentifies people of color and AI tools that discriminate against women in hiring. The article

stresses the need for companies to address data bias in their AI systems by ensuring that their data is representative and diverse (Ross).

A recent article by Powers in Forbes discusses the cybersecurity risks associated with AI-powered software. The article explains how AI systems are vulnerable to cyber attacks, and how these attacks could compromise sensitive data or even take over AI systems. The article emphasizes the need for companies to invest in cybersecurity measures to protect their AI systems, such as encrypting data and implementing multi-factor authentication (Powers).

An article by Turner in ZDNet explores the ethical concerns surrounding the use of AI-driven tools in the workplace. The article discusses issues such as privacy, job displacement, and the impact on human decision-making, emphasizing the need for companies to consider the ethical implications of their AI systems. The article suggests that companies should prioritize transparency, accountability, and fairness in the development and deployment of their AI systems (Turner).

An article by KPMG in Forbes discusses the importance of ethical considerations in the development and deployment of AI systems. The article emphasizes the need for companies to establish clear ethical guidelines and governance structures to ensure the responsible use of AI in their operations. The article suggests that companies should prioritize transparency, accountability, and fairness in their AI systems to address the potential risks associated with their use (KPMG).

Overall, there are many major upsides to using AI-powered tools in day-to-day operations, but it is important to factor in the challenges and potential risks associated with their use. It is crucial for companies to be aware of these risks and take steps to address them to ensure the safe and effective use of AI in their operations. One way companies can address these risks is by regularly reviewing and auditing their AI systems. This can help identify any biases or inaccuracies in the system and enable companies to take corrective action to improve the accuracy and fairness of their AI systems. Another important step is to ensure the ethical use of AI, which includes considerations such as privacy, job displacement, and the impact on human decision-making. Finally, it is crucial to invest in cybersecurity measures to protect their AI systems from cyber attacks is essential to ensure the safety and security of their systems and the data they process.

References:

1. Brynjolfsson, Erik, and Andrew McAfee. "The Business of Artificial Intelligence." Harvard Business Review, 1 July 2017, https://hbr.org/2017/07/the-business-of-artificial-intelligence.

2. Gohil, Harshil. "The Use of AI in Banking: How AI is Changing the Industry." Forbes, 18 Mar. 2020, https://www.forbes.com/sites/harshilgohil/2020/03/18/the-use-of-ai-in-banking-how-ai-is-changing-the-industry/?sh=283a225a1f6c.

3. McCarthy, Niall. "AI to Compete with Doctors in Diagnosing Breast Cancer Within Years." The Guardian, 1 May 2019, https://www.theguardian.com/society/2019/may/01/ai-to-compete-with-doctors-in-diagnosing-breast-cancer-within-years.

4. Albanesius, Chloe. "Amazon's Robots: What Happened?" PCMag, 3 Dec. 2020, https://www.pcmag.com/news/amazons-robots-what-happened.

5. Ross, Ariel Ezrachi and Maurice Stucke. "Artificial Intelligence Is Often Biased. Here's What Can Be Done About It." Wired, 6 Apr. 2021, https://www.wired.com/story/artificial-intelligence-is-often-biased-heres-what-can-be-done-about-it/.

6. Powers, Michael B. "AI Cybersecurity Risks You Need to Know About." Forbes, 10 Mar. 2021, https://www.forbes.com/sites/forbestechcouncil/2021/03/10/ai-cybersecurity-risks-you-need-to-know-about/?sh=20d4adec28fc.

7. Turner, Karen. "The Ethics of AI: How to Hold Machines Accountable." ZDNet, 19 Apr. 2021, https://www.zdnet.com/article/the-ethics-of-ai-how-to-hold-machines-accountable/.

8. KPMG. "The Ethics of AI: Balancing Risk and Opportunity." Forbes, 28 Apr. 2021, https://www.forbes.com/sites/kpmg/2021/04/28/the-ethics-of-ai-balancing-risk-and-opportunity/?sh=7e7483b6613b.

Andrii Nikolin

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

COMPARING PROJECT MANAGEMENT METHODOLOGIES IN SOFTWARE DEVELOPMENT

Project management is a crucial aspect of software development, as it ensures that projects are completed on time, within budget, and to the desired quality. Different methodologies have been developed over the years to manage software development projects. In this article, we will compare some of the most popular project management methodologies used in software development companies, including Agile, Scrum, Waterfall, Kanban, Lean, and Shape Up.

Each project management methodology has its strengths and weaknesses, and the choice of methodology will depend on the project's unique requirements, team composition, and organizational culture. Let's delve deeper into each of them.

Agile methodology is known for its flexibility and adaptability, which makes it a popular choice for software development teams that want to respond quickly to changing requirements. It is an iterative and incremental approach to software development with focus on delivering working software in small increments, with a high degree of collaboration between the development team and the stakeholders. Agile methodology is based on the Agile Manifesto, which emphasizes individuals and interactions, working software, customer collaboration, and responding to change.

Scrum methodology is a subset of Agile methodology, and it is based on the principles of transparency, inspection, and adaptation. Scrum is a framework for managing and completing complex projects, and it is centered around the concept of sprints, which are short iterations of development. Sprints are used to break down a project into smaller, more manageable chunks, which makes it easier to track progress and adjust the project's direction as needed. Scrum teams work in a highly collaborative and self-organizing way, with a focus on delivering a potentially shippable product at the end of each sprint.

Waterfall methodology is a traditional approach to software development that is still used today, especially for projects with a well-defined scope and a fixed set of requirements. This methodology is more rigid and sequential than Agile methodology, and it requires a clear understanding of the project's goals and objectives upfront. Waterfall methodology is less suited for projects with changing

requirements, as it does not allow for much flexibility or adaptability. It is required that each phase of the development process is completed before moving on to the next phase.

Kanban methodology is a visual method for managing and improving work, and it is based on the principles of visualizing work, limiting work in progress, and managing flow. Kanban boards are used to visualize the work and track its progress, and the goal is to continuously improve the flow of work by identifying and removing bottlenecks. Kanban emphasizes the importance of limiting work in progress, which helps teams stay focused on delivering high-quality software. Teams use pull systems to ensure that work is not started until there is capacity to complete it.

Lean methodology is a philosophy for continuous improvement, which makes it a popular choice for teams that want to optimize their entire process of software development. Lean methodology is based on the principles of Lean manufacturing and aims to eliminate waste and create value for the customer by optimizing the entire process of software development. Lean methodology emphasizes the importance of creating flow, establishing pull, and seeking perfection, which helps teams continuously improve their processes and deliver high-quality software. It relies on cross-functional teams that work together to deliver high-quality software in a timely manner.

Shape Up methodology is a modern approach to software development that emphasizes clear project scopes, betting small, and delivering value to the customer. Shape Up methodology is centered around six-week cycles, which makes it easier to track progress and adjust the project's direction as needed. It encourages the team to focus on solving problems and delivering high-value features to the customer.

It was developed by the software company Basecamp, known for its project management software, which helps teams collaborate and manage projects more efficiently. Development of the methodology was done in response to the company's need for a more streamlined and efficient project management process. According to Ryan Singer, the Head of Strategy at Basecamp, the company had previously used a variety of different methodologies, including Scrum and Waterfall, but found that they were not well-suited to their needs.

The first introduction of the new methodology was done by Singer in a series of blog posts on the Basecamp website in 2019. They were based on the idea that traditional project management methodologies can be overly complex and rigid, and that there is a need for a more flexible and adaptable approach.

Each cycle of work consists of a six-week period of focused work followed by a two-week break. During each cycle, teams focus on a single project, with the

goal of completing a specific set of features or functionality by the end of the cycle.

During the two-week break, teams take a break from working on their current project and shift their focus to other areas of the business or to personal development. This break is intended to provide time for teams to reflect on their work, recharge their batteries, and explore new ideas. Some teams may use the break period to work on internal projects or to explore new technologies or tools. Others may use the time for professional development, such as attending conferences or taking online courses.

The break period is an integral part of the Shape Up methodology, as it helps to prevent burnout and allows teams to maintain a sustainable pace of work. By taking a break from their current project and exploring new ideas and opportunities, teams are able to stay motivated and engaged, which can lead to better outcomes in the long run.

Shape Up also emphasizes the importance of setting clear boundaries around projects, and of giving teams the autonomy to decide how best to approach their work. According to Singer, this helps to avoid the common problems of scope creep and overcommitment, which can lead to delays and frustration.

Since its introduction, Shape Up has gained a following among software development teams and project managers who are looking for a more streamlined and effective way of managing projects. The methodology has also been adapted for use in other industries, such as marketing and design.

In conclusion, project management is a crucial component of software development, and there are a variety of methodologies available to help teams manage their projects effectively. Each methodology has its own strengths and weaknesses, and it is important for teams to choose the approach that best fits their needs. By understanding the key characteristics of each methodology, teams can choose the approach that best fits their needs and helps them to achieve their goals. Whether they are looking to improve collaboration, reduce waste, or streamline their processes, there is a strategy out there that can help them.

References:

1. Mike Cohn. "Agile Estimating and Planning" (ISBN: 978-0131479418).

2. Jeff Sutherland. "Scrum: The Art of Doing Twice the Work in Half the Time" (ISBN: 978-0385346450).

3. David J. Anderson. "Kanban: Successful Evolutionary Change for Your Technology Business" (ISBN: 978-0984521401).

4. Eric Ries. "The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses" (ISBN: 978-0307887894).

5. Ryan Singer. "Shape Up: Stop Running in Circles and Ship Work that Matters". https://basecamp.com/shapeup

Yevhenii Tyrsyna

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

MODERN THEORETICAL ASPECTS AND THE MECHANISM OF FORMATION OF THE PERSONNEL MANAGEMENT SYSTEM OF A TRADING ENTERPRISE

A trading enterprise, like any other, has its own specifics that require an approach to personnel management taking it into account. The success of the enterprise as a whole, as well as the satisfaction of employees, which is important for retaining and attracting qualified personnel, depends on the quality of personnel management.

Due to constant changes in the field of personnel management and the development of new technologies, there is a need to study modern theoretical aspects and mechanisms for forming a personnel management system in trading enterprises. This allows increasing the efficiency of personnel management and ensuring the competitiveness of the enterprise in the market.

Personnel management is one of the key elements of successful operation of a trading enterprise. Its effectiveness largely depends on the interaction with the enterprise's strategy, as the right strategy can ensure maximum efficiency in personnel management [5, p. 141].

The main interaction between personnel management and the enterprise's strategy lies in the fact that the strategy determines the direction of the enterprise's development, and personnel management ensures the implementation of this strategy. For example, if the enterprise's strategy is to reduce production costs, then personnel management should determine which specific measures need to be implemented to reduce costs for wages, hiring new employees, and increasing the efficiency of personnel work.

One of the important elements of the interaction between personnel management and the enterprise's strategy is the development of a personnel strategy. The personnel strategy determines which specific actions need to be taken to ensure the implementation of the enterprise's strategy. For example, if the enterprise's strategy is to expand sales markets, then the personnel strategy should provide for the hiring of new employees in marketing and sales, as well as training for personnel on expanding sales markets.

Personnel management should also help in shaping the company's strategy by constantly analyzing the labor market and gathering information about trends in

its field. For example, if a company plans to expand into a new market, HR can help determine what specific competencies and skills employees need to succeed in the new market.

In addition, human resource management can play a key role in ensuring the execution of the company's strategy by creating an appropriate culture of the organization.

Therefore, the relationship between personnel management and enterprise strategy is extremely important for the successful functioning of a trading enterprise. Personnel management should be integrated into the general strategy of the enterprise and should ensure the implementation of this strategy through properly selected employees, the creation of an appropriate organizational culture and the use of effective personnel management tools [4, p. 58–59].

It is worth noting that the specificity of trading enterprises is related to the special nature of labor relations. If an employee of any industrial enterprise can perform the tasks assigned to him in an automated or mechanized manner, then the effectiveness of the work of the sales staff will depend only on his ability to work with people.

It is appropriate to agree that personnel management in modern trade enterprises is based on the fact that people in the process of work are considered at the same time as employees who ensure the realization of the economic goals of the enterprise, and as developed individuals and employees belonging to a single organizational system. The success of the enterprise depends on specific people, their knowledge, competence, qualification, discipline, motivation, ability to solve problems, and receptivity to learning. Therefore, in order for the enterprise to function effectively, it is necessary to properly organize the work of employees, at the same time constantly monitoring their activities, using various effective personnel management methods based on scientific laws [1, p. 105].

Fulfilling the goals of the personnel management system requires solving the main tasks:

–providing the enterprise with a workforce of the appropriate quantity and quality;

–ensuring conditions for high labor productivity, sufficient level of its organization, motivation, self-discipline, acquisition of skills for interaction and cooperation by the employee;

–formation of a stable team in organizations, i.e. securing experienced and highly qualified personnel at the enterprise;

–implementation of the needs and interests of employees regarding the content of work, working conditions, the possibility of professional qualification

and career advancement based on the growth of professional skills, knowledge, work experience of the company's personnel;

–optimal balance of interests of both the enterprise and employees, economic and social efficiency of personnel management.

The main principle that should be the basis of the functioning of any enterprise is the principle of rationality and optimization, because it does not matter how many resources the company has, if it does not know how to use them correctly, they will never be enough. The most important resource of the enterprise is its personnel and its intellectual potential, which requires constant management [2, p. 40].

The main goal of forming an effective concept of personnel management at a trade enterprise is the development of a personnel policy and provision of human resources with the necessary levels of competence, effective use of the labor potential of employees, motivation of professional development of employees and social development of teams.

In order to increase the labor productivity of the staff, leaders and managers can use various methods of personnel management as one of the ways to achieve the profitability of the enterprise, which does not act directly, but indirectly on the staff.

Modern personnel management technologies, based on the basis of "manager-subordinate" interaction, include:

–training, which is characterized by a minimum number of theories and "orienting" on practice, "working out" the specific skills;

–professional consultations, if they are necessary to solve specific problems, but the staff lacks special knowledge;

–mentoring, which involves the promotion of already existing knowledge or professional skills and learning opportunities at the workplace;

–coaching, which helps the employee realize his goals, the reasons for success and failure, and determine the direction of behavior change [3, p. 190].

In our opinion, the mechanism of forming a personnel management system at a trading enterprise should be carried out in stages, taking into account the current conditions of economic development. Thus, the main successive stages of the implementation of such a mechanism are:

–selection and justification of the concept of the personnel management system at the trading company;

–selection and training of employees;

–control over the work of the sales staff;

–development of the sales staff;

–evaluation of the efficiency of employees' work and their stimulation.

The effectiveness of the functioning of the personnel management system directly depends on the principles taken as a basis, which describe the requirements for the formation and determine the direction of the development of the personnel management system. It is worth noting that the number of such principles will depend on the size of the enterprise itself, its structure and market share.

Complexity and systematicity should be included among the main principles of forming the personnel management system of a trade enterprise; compliance with the goals of the enterprise; hierarchy, i.e. compliance with subordination in the personnel management system; use of scientific approaches to personnel management; economy, that is, achieving the maximum result from the effectiveness of the enterprise management system; innovativeness during personnel development management; complexity; and progressiveness [1, p. 106].

The analysis of research and publications also makes it possible to highlight such areas of effective personnel management as:

–compliance with labor legislation;

–taking into account the specifics of the impact of global socio-economic processes on the concept of personnel management;

–increasing the competitiveness of personnel;

–provision of sufficient conditions for professional development of personnel;

–providing an objective comprehensive assessment of the qualities, competencies and results of the personnel's activities;

–reducing the risks of enterprise activity during personnel management in the conditions of modern post-industrial society [3, p. 191].

One of the main factors that ensures an increase in labor productivity at a trading enterprise is the formation and implementation, as well as the constant improvement of the concept of personnel management. Based on the peculiarities of trade entrepreneurship, the requirements for its formation and implementation can be summarized to the following:

– the concept of personnel management should be closely related to the strategic goals and current tasks of the enterprise and be developed as a result of discussions and consultations at different levels of management;

– strategic and conceptual components of the personnel policy of a trading company must be clearly formulated and cover all the main areas of work with personnel;

– the personnel policy developed on the basis of the accepted concept of personnel management must be provided with the necessary resources, contain

specific steps, and its directions must be united by a common methodology, be interconnected with subsystems of personnel management.

In modern conditions, the process of development and updating of personnel management concepts continues, while both management systems and the methods and tools used are being improved. The results of the implementation of an effective concept of personnel management include an increase in the effectiveness of the motivation of employees at a trade enterprise for continuous professional growth, as well as the preservation of the personnel core of the enterprise and, at the same time, the observance of optimal age proportions due to the hiring of young people.

References:

1. *Donchak L. H., Dobizha V. V., Shkvaruk D. H. The mechanism of forming a personnel management system at a trading enterprise. Economic space. 2020. №154. Pp. 104–108.*

2. *Lozova O. V., Demchenko V. O. The personnel management system as an important component of the effective functioning of the enterprise in market economic conditions. Ukrainian Journal of Applied Economics. 2017. V. 2. №4. Pp. 37–45.*

3. *Chevganova V. Ya., Pryima Yu. O. Formation of the concept of personnel management of a trade enterprise in modern conditions. Market infrastructure. 2020. №41. Pp. 187–193.*

4. *Farooq S., Khan M. A., Hussain M. Human resource management practices and their impact on employee performance in retail sector. South Asian Journal of Management Sciences. 2019. №13 (1). Pp. 57–63.*

5. *Rasoolimanesh S. M., Md Yusof R., Jaafar M. An exploratory study of the role of human resource management practices in retail firms' performance. Journal of Retailing and Consumer Services. 2017. №39. Pp. 141–149.*

Anton Voronko

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

COMBINED ITERATIVE APPROACHE FOR STRATEGIC INITIATIVES' IMPLEMENTATION

Organizations execute strategies by the means of strategic initiatives. In many cases strategic initiatives are implemented through projects and programs [1, p. 33].

After its introduction in 2001 [2] agile approaches for implementation of the projects related to software development influenced project management significantly. It's based on work in small iterations what makes work more predictable and gives ability to receive early feedback as well as introduce needed changes with less expenses incurred and with smaller deviation from the optimal direction. It is particularly realized through the set of lightweight frameworks like Scrum, Dynamic Systems Development Method (DSDM), Crystal Methods, Feature-Driven Development (FDD), Lean Development (LD), Extreme programming (XP) and Adaptive Software Development (ASD) [3, pp. XV-XVI].

In a decade its early successes attracted attention of significant market players and led to the spread of principles and practices beyond the scope of the team that was agile approaches' original intention. As an example, we can consider agile transformation started in Microsoft in 2011 [4]. As evidence for the dramatic influence of this movement, 2015 Learning Consortium Project could be mentioned [5]. It was focused on scrutiny of 9 companies (incl. such large corporations as Microsoft and Ericsson) and highlighted the situation with application of Agile at scale. Interest to agile practices on the level of the whole organization was raised a year earlier in the article in Harvard Business Review [6]. Another sign of recognition of agile practices as full-fledged part of general project management practices was Project Management Institute's launching of the relevant certification in 2012 [7] as well as publishing of Agile practice guide in 2017 in cooperation with AgileAlliance [8].

Usefulness of agile practices for the management of a portfolio of the company was described in the books of Johanna Rothman in 2005 and in more details in 2009 [9][10]. It includes, among other things, work with timeboxed iterations, velocity and capacity, usage of prioritized backlog, burndown chart and a definition of done.

Unfortunately, many companies can't benefit from advantages promised by agile approaches due to the lack of channels between implementation teams and "the voice of customer" (which is considered existing by default, without specific instructions of how to arrange it).

To shed light on the marketing component of running business and enhance practices concentrated on work of an organization with the new prospective customer groups, other iterative practices were coupled with agile: one of the most used is the Lean Startup.

The concept was coined by Eric Ries in 2008 [11] and is based on Steve Blank's ideas (presented under the name of Customer Development) about importance of the marketing and business functions for startups as future scalable business models (that was overlooked in favor of the technical side of product development). Finally, the approach was described in the book of Ries "The Lean Startup" in 2011. Beside frequent emphasis on iterative nature of the approach itself, in this book a specific case was mentioned how the Lean Startup components were added to the ongoing agile project (where Extreme programming was used) and improved its results [12, pp. 130-148]. After some period of growing popularity, the practices and tools from that approach started to attract attention of big companies (like GE, Intuit, Qualcomm) [13] which led to systematization of its corporate application, for example, Lean Enterprise [14] and integration of the Lean Startup into Portfolio level of Scaled Agile Framework [15].

As follows, to maximize benefits from iterative approaches in implementation of strategic initiatives, companies need to seek combined approaches in order to link different corporate functions as well as factors. An example of this is integrated application of agile and the Lean Startup practices which set up a seamless pipeline for generation of marketing value proposition.

References:

1. Project Management Institute. The Standard for Portfolio Management, 4th edition. Pennsylvania, 2017.

2. History: The Agile Manifesto. Retrieved February 22, 2023. https://agilemanifesto.org/history.html

3. Jim Highsmith. Agile Software Development Ecosystems. Indianapolis, 2002.

4. Steve Denning. Surprise: Microsoft Is Agile. Retrieved February 25, 2023. https://www.forbes.com/sites/stevedenning/2015/10/27/surprise-microsoft-is-agile/

5. Steve Denning. Learning Consortium For The Creative Economy. Retrieved February 25, 2023. https://www.forbes.com/sites/stevedenning/ 2015/11/02/drucker-forum-2015-tackles-the-creative-economy/

6. Jeff Gothelf. Bring Agile to the Whole Organization. Retrieved February 25, 2023. https://hbr.org/2014/11/bring-agile-to-the-whole-organization

7. Mike Griffiths. The Growth of the PMI-ACP Certification. Retrieved February 25, 2023. https://www.projectmanagement.com/contentPages/article.cfm?ID=278785&thisPageURL=/articles/278785/The-Growth-of-the-PMI-ACP-Certification

8. Project Management Institute. Agile Practice Guide. Pennsylvania, 2017.

9. Johanna Rothman and Esther Derby. Behind Closed Doors. Raleigh, Dallas, 2005

10. Johanna Rothman. Manage Your Project Portfolio. Raleigh, Dallas, 2009.

11. Eric Ries. The lean startup. Retrieved February 27, 2023. http://www.startuplessonslearned.com/2008/09/lean-startup.html

12. Eric Ries. The Lean Startup. New York, 2011.

13. Steve Blank. Why the Lean Start-Up Changes Everything. Retrieved March 2, 2023. https://hbr.org/2013/05/why-the-lean-start-up-changes-everything

14. Jez Humble, Joanne Molesky, and Barry O'Reilly. Lean Enterprise. Sebastopol, 2015.

15. Epics. Retrieved March 2, 2023. https://www.scaledagileframework.com/epic/

УПРАВЛІННЯ ПЕРСОНАЛОМ

Білодід В. В.

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

СУЧАСНІ МЕТОДИ МОТИВАЦІЇ ПЕРСОНАЛУ НА ПІДПРИЄМСТВАХ І ВИРОБНИЦТВІ

В даний час існує безліч методів мотивації, здатних стимулювати співробітників до досягнення високих результатів. Це може бути як фінансовавинагорода (бонуси, відсоток від прибутку), нефінансові бонуси (поїздка, квитки на заходи, сертифікати на послуги), особистісний розвиток (курси, конференції).

Але повернемося до першоджерел теорії мотивації та особистості працівників підприємства. Що їх мотивує, а що може сприяти ефективній роботі.

Мотивація як напрямок психології спирається на певний психологічний і науковий апарат. Наука управління персоналом розглядає дві групи теорій мотивації: змістовну та процесуальну.

Змістовні теорії припускають опору на потреби людини, класифікуючи їх різними способами. До прихильників цієї теорії можна віднести А. Маслоу з його концепцією піраміди потреб, Д. Макклелланда і Ф. Герцберга, а також деяких інших американських психологів і дослідників.

Змістовні теорії найчастіше засновані на ієрархії потреб, розробленої А. Маслоу [1]. Виглядає це так:

- базові потреби – це ті, які необхідні для виживання – їжа, притулок і подібні фізіологічні потреби;
- наступний рівень - потреба в безпеці і впевненості в завтрашньому дні;
- на третьому рівні ієрархії можна зустріти соціальні потреби - залежність від думки колективу, прагнення визнати свої достоїнства, спілкування;
- на четвертому рівні знаходяться ієрархічні потреби – повага, авторитет, лідерство;
- На вершині ієрархії знаходяться потреби в самоактуалізації.

Відповідно до теорії, у міру задоволення базових потреб людина переходить на наступний рівень, який характеризується підвищенням продуктивності праці. Завданням керівництва організації, таким чином, стає відстеження ступеня задоволення потреб і зміни відповідно до їх ієрархаїчного обсягу робіт і пропозицій мотивації персоналу. Ця теорія носить ідеалістичний характер, адже, перш за все, потрібен керівник, який мотивований на підвищення професійного рівня співробітників. Проте деякі робочі системи спираються на неї в якості основи, наприклад, система грейдування заробітної плати (грейд - це група посад, які мають рівну цінність для компанії, а кожній групі встановлюється свій діапазон заробітної плати). А важливість внутрішньої мотивації і її роль в особистісному зростанні і успіху розглядається в різних організаціях і в бізнесі [2].

Процесуальні теорії вважають за краще враховувати не тільки потреби особистості як основу для формування системи заохочень. Вони припускають, що трудова і організаційна поведінка людини багато в чому грунтується на його внутрішніх установках і очікуваннях. Ці теорії намагаються проаналізувати способи, якими людина вибирає певний тип поведінки і впливає на фактори, що визначають його вибір. Прихильники процесуальних теорій мотивації вважають, що працівник підприємства, оцінивши поставлені завдання і розмір винагороди за їх виконання, співвіряє виклик з власними намірами, мотиваціями і очікуваннями і вибирає певний тип поведінки. Цілі він ставить виходячи з пропонованих йому завдань, але скорочуючи і видозмінюючи їх відповідно до своїх ціннісних орієнтацій [3]. При цьому більш високі цілі вимагають великих зусиль, а в разі постановки недосяжної мети співробітник підприємства може отримати зворотній результат - демотивацію. Існує чотири фактори, які впливають на готовність співробітника докладати зусиль для досягнення мети: складність мети, конкретність, наскільки мета прийнятна для людини і наскільки людина прагне до цієї мети [4].

Дослідження мотивації праці дозволяють відповісти на багато питань: чому людина вибирає ту чи іншу професію; що змушує його працювати ефективно; які ймовірні причини його відходу з роботи, з професії; що може і повинна робити організація для того, щоб мотивація працівника була високою, а робота продуктивною. Однак на сьогоднішній день не існує єдиного поняття, яке могло б вирішити всі проблеми, пов'язані з розвитком і підтримкою мотивації праці людини.

Всі розглянуті вище теорії дають уявлення про якийсь один аспект трудового життя, але не дозволяють робити більш глибокі узагальнення, тому майбутнє розвитку досліджень мотивації праці лежить в області поєднання різних підходів і тенденцій, від сильних сторін і перевірених методів.

Можна припустити, що одним з найбільш ефективних методів є створення комфортних умов праці, де співробітники відчувають себе шанованими і цінними членами колективу, працюючи безпечно. Цього можна досягти шляхом організації командних заходів, навчання новим навичкам і забезпечення правильної комунікації між колегами і керівництвом.

Оскільки розробка мотиваційних програм не стоїть на місці, останнім часом застосовуються нові підходи до мотивації на робочому місці. Основна ідея полягає в тому, що співробітники залучаються в процес прийняття рішень, беручи участь в цьому процесі і встановлення цілей. Гейміфікація, автономія на робочому місці і менторінг (наставництво) допомагають співробітникам відчувати себе більш залученими в робочий процес і дозволяють їм висловлювати свою думку.

Так що одним з підходів є мотивація за допомогою геймифікації, яка включає в себе елементи ігрової механіки на роботі. Наприклад, ви можете створити систему балів та нагород, які працівники можуть отримати за виконання завдань та досягти цілей. У комп'ютерних програмах виробництва ігрові елементи можуть бути представлені, наприклад, показники ефективності та прогрес працівника. Вона дозволяє співробітникам більш ефективно виконувати поставлені перед ними завдання і отримувати задоволення від процесу. Такий підхід до мотивації дозволяє значно підвищити продуктивність праці і поліпшити загальну атмосферу на робочому місці.

Наступний підхід полягає в обліку особистої працездатності співробітників. Йдеться про збільшення автономії на робочому місці, що надає пріоритет підвищенню рівня автономії на робочому місці.

Співробітники, яким довіряють, отримують більше свободи в прийнятті рішень, що дозволяє їм відчувати себе більш впевнено і мотивовано.

Одним з нових видів мотивації є розвиток лідерства за допомогою менторінг. Менторінг є одним із способів розвитку лідерства серед співробітників (не плутати з коучингом). При такому підході створюється наставник, який зможе допомогти співробітнику розвинути навички і знання, одночасно підвищуючи впевненість не тільки в своїх силах як керівника, але і в мотивації.

В цілому нові підходи до мотивації на виробництві ставлять на чільне місце людський фактор з урахуванням потреб і мотивів кожного працівника. Вони дозволяють співробітникам відчувати себе більш залученими в робочий процес, покращують якість роботи і сприяють поліпшенню загальної атмосфери на робочому місці.

Список використаних джерел:

1. *А. Маслоу, «Мотивація і особистість», 3-е видання, 2012.*
2. *С. Кові«7 навичок високоефективних людей», Алпіна Бізнес Букс, 2009*
3. *Д. Макклелланд «Мотивація людини», Санкт-Петербург Пітер, 2007*
4. *Кірхлер Е. Мотивація в організаціях. /Е. Кірхлер, К. Родлер/ «Психологія праці та організаціїз психології. Харків. Т.1.*

Бобылев А. В.

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

ОЦЕНКА ПЕРСОНАЛА ТОРГОВЫХ КОМПАНИЙ

Оценка персонала является важным процессом для любой компании, особенно для торговых, где качество обслуживания клиентов имеет важное значение для успеха бизнеса.

Целью данной научной статьи является изучение роли оценки персонала в повышении эффективности торговых компаний.

В статье рассматриваются преимущества оценки персонала в торговых компаниях, в том числе выявление пробелов в навыках, повышение мотивации и производительности труда сотрудников, снижение текучести кадров. В статье также исследуются проблемы внедрения оценки персонала в торговых компаниях и предлагаются стратегии преодоления этих проблем.

1. Введение

Успех торговой компании зависит от качества ее продуктов и услуг, а также от навыков и производительности ее сотрудников. Оценка персонала — это процесс, который включает в себя оценку навыков, знаний и производительности сотрудников для выявления сильных и слабых сторон, а также разработки стратегий для повышения их производительности. В данной статье исследуется роль оценки персонала в повышении эффективности торговых компаний.

2. Преимущества проведения оценки персонала в торговых компаниях

Выявление пробелов в навыках и знаниях: оценка персонала может помочь торговым компаниям выявить пробелы в навыках и знаниях среди сотрудников. Эта информация может быть использована для разработки программ обучения, для устранения этих пробелов и повышения качества обслуживания клиентов.

Повышение мотивации и производительности сотрудников. Оценка персонала также может повысить мотивацию и производительность сотрудников. Предоставляя отзывы о своей работе, сотрудники могут определить области для улучшения и работать над достижением конкретных целей. Это может повысить их удовлетворенность работой и мотивацию, что приведет к повышению производительности.

Сокращение текучести кадров. Оценка персонала может помочь торговым компаниям выявить причины текучести кадров и разработать стратегии по ее сокращению. Предоставляя отзывы о работе сотрудников, компании могут решать проблемы, связанные с неудовлетворенностью сотрудников, такие как некачественное обучение или плохое управление.

3. Проблемы внедрения оценки персонала в торговых компаниях

Сопротивление изменениям. Одной из самых больших проблем при проведении оценки персонала в торговых компаниях является сопротивление изменениям. Сотрудники могут сопротивляться идее оценки, особенно если они работают в компании в течение длительного времени.

Недостаток ресурсов. Еще одной проблемой является нехватка ресурсов для эффективного проведения оценки персонала. Сюда входят расходы на обучение оценщиков, разработку инструментов оценки и обеспечение обратной связи с сотрудниками.

Стратегии преодоления трудностей внедрения оценки персонала в торговых компаниях:

Коммуникация: Эффективная коммуникация необходима для преодоления сопротивления изменениям. Торговые компании должны сообщать своим сотрудникам о преимуществах оценки персонала и предоставлять им надлежащее обучение и поддержку для участия в этом процессе.

Распределение ресурсов: торговые компании должны выделять достаточные ресурсы для эффективной оценки персонала. Это включает в себя инвестиции в обучение оценщиков, разработку инструментов оценки и обеспечение обратной связи с сотрудниками.

Соблюдение законодательства: торговые компании должны обеспечить соблюдение соответствующих трудовых законов и правил при проведении оценки персонала. Это включает в себя обеспечение того, чтобы процесс оценки был справедливым, прозрачным и беспристрастным.

Оценка персонала является критически важным процессом для торговых компаний для повышения качества обслуживания клиентов и эффективности их операций. Несмотря на трудности, связанные с оценкой персонала, торговые компании могут решить эти проблемы, сообщая о преимуществах оценки персонала, выделяя достаточные ресурсы и соблюдая соответствующие законы и правила в области занятости. Инвестируя в оценку персонала, торговые компании могут повысить эффективность работы своих сотрудников, снизить текучесть кадров и повысить удовлетворенность клиентов.

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.*

Мазняк С. А.

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

КЛАССИФИКАЦИЯ И ВИДЫ ЗАТРАТ РАБОЧЕГО ВРЕМЕНИ ОРГАНИЗАЦИИ В СИСТЕМЕ ПЛАНИРОВАНИЯ

Рабочим временем считается тот период, в который происходит осуществление производственных функций. Таким периодом могут быть признаны: календарный год, месяц, неделя или одна рабочая смена.

Классификация затрат рабочего времени исполнителя помогает предприятию:

- изучить по назначению ли используется период труда работником или нет;
- установить предпосылки и основные причины временных затрат;
- определить, насколько необходимы существующие производственные процессы;
- понять оптимальность временных затрат; определить элементы классификации затрат рабочего времени.

Рабочее время сотрудника подразделяется на:

- период времени, в который осуществляется трудовая деятельность по производственному заданию (сюда же входят временные затраты на подготовку к выполнению задачи);
- период времени, в который происходит деятельность, непредусмотренная производственным заданием
- в этот отрезок времени сотрудник выполняет функции, которые обычно ему не свойственны и не входят в непосредственное выполнение задания (это может быть вызвано производственной необходимостью или конкретным распоряжением руководителя предприятия).

Классификация затрат рабочего времени производственных рабочих на выполнение задания имеет следующие элементы:

1. Подготовительно-заключительный период – временной промежуток, который тратится сотрудником на подготовительные мероприятия. Перед тем, как приступить к выполнению задачи, работнику необходимо подготовить себя, а также средства производства к непосредственному выполнению трудовых функций и задач производственного процесса. Сюда же входит окончание работ по конкретному заданию. В разрезе конкретных

действий этот элемент может включать получение задания, ознакомление с требованиями к результату, настройку оборудования, подготовку и сдачу отчетности по итогам выполненного задания.

2. Оперативный период – временной промежуток в классификации рабочего времени, когда работник выполняет повседневные повторяющиеся практические задания (виды работ).

Сюда же относятся вспомогательные действия работника, которые необходимо произвести для обеспечения необходимых изменений. К оперативному времени относят: основной период и вспомогательный.

Основной период – временной промежуток трудового процесса, в который происходит изменение свойств и характеристик предмета производства, требуемое по заданию предприятия. Вспомогательный период – временной промежуток, который тратится на действия, требуемые для обеспечения возможности выполнения производственного задания и основной работы.

3. Время на обслуживание рабочего места – период, который тратится на обеспечение порядка на рабочем месте, а также обеспечение чистоты и должного ухода за используемым оборудованием. В этот элемент входят: техническое обслуживание и организационное.

Период технического обслуживания – временной отрезок, которые тратится на обслуживание оргтехники, обновление данных в базе т.д. Период организационного обслуживания – временной промежуток, в который происходит поддержание порядка на рабочем месте. В этот элемент входят: обработка документации, передача документации, обеспечение чистоты рабочего места после трудового дня или выполнения задания. Существуют также временные промежутки, которые не соответствуют нормам классификации затрат рабочего времени. К ним относятся периоды, когда нарушается трудовая дисциплина и затраты, возникающие в результате технических сбоев, и прочих недостатков производственного процесса. Классификация затрат рабочего времени исполнителя включает также время, отведенное на перерывы. Классификация потерь рабочего времени содержит:

1. Перерывы, предусмотренные регламентом – временные промежутки, которые установлены правилами внутреннего трудового распорядка и иными локальными нормативными актами в зависимости от вида деятельности. Основные виды перерывов в работе установлены в нормах.

2. Перерывы, не предусмотренные регламентом и правилами – временные промежутки, которые могут быть вызваны неполадками производственного процесса, приводящими к остановке трудовой деятельности. Такие перерывы имеют следующие причины: нарушение

процесса производства и/или нарушения дисциплины труда. Временные отрезки нарушений процесса производства, как правило, вызваны различными поломками, отсутствием электроэнергии и иными причинами. К нарушениям дисциплины труда относят опоздания на рабочее место, разговоры на личные темы, «перекуры», отлучки с рабочего места без уважительной причины и т.д. На основании изученных классификации и видов затрат рабочего времени, следует рассмотреть основные элементы методологии планирования рабочего времени.

Список использованных источников:

1. *Балабанова, А. В. Макроэкономика: механизмы повышения качества роста: учебное пособие / А. В. Балабанова. М.: Высшая школа, 2011. 373с. 6.*

2. *Баскакова, О. В. Экономика предприятия (организации): Учебник / О. В. Баскакова, М.: Дашков и К, 2013. 372 с.*

3. *Большаков, А. С. Современный менеджмент: теория и практика / А. С. Большаков. – СПб.: Питер, 2012. – 416 с.*

4. *Боровская, М. Я. Экономика, организация и управление на предприятии / под ред. М. Я. Боровской. Спб: Феникс, 2010. 480 с.*

5. *Владимирова, Л. П. Экономика труда: учебное пособие / Л. П. Владимирова. М.: Дашков и Ко, 2012. – 300 с.*

6. *Волгина, Н. А. Экономика труда: социальнотрудовые отношения / Под ред. Н. А. Волгина, – М.: Экзамен, 2010. – 736.*

Новіков К. С.

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

УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ПЕРСОНАЛОМ ОРГАНІЗАЦІЙ УКРАЇНИ

Управління персоналом можна відзначити однією з найбільш важливих сфер діяльності організації, спроможною в значній мірі підвищити ефективність функціонування підприємства або довести його до збитковості. Бо саме персонал є джерелом розвитку компанії, її потенціалом, дієвим важелем, який впливає на прибутковість та інтелектуальний капітал. Тому система управління персоналом обов'язково повинна відповідати сучасним стандартам та вимогам, застосовувати інновації (такі як, наприклад, інноваційні методи мотивації співробітників), передбачати підвищення ефективності використання персоналу.

Кваліфіковані співробітники організації у достатній кількості для реалізації виробничого процесу виступають її головною рушійною силою, будучи при цьому проміжною об'єднуючою ланкою між економічними та технічними факторами виробництва. Виходячи з цього управління персоналом є сукупністю всіх управлінських рішень та видів діяльності на підприємстві, пов'язаних з плануванням та організацією впливу працівників, воно повинно мати досконалу систему з ефективними сучасними підсистемами. Тому система управління персоналом організації для забезпечення прибутковості безумовно повинна бути в стані постійного розвитку, особливо в частині безпосередньо персоналу та його людського капіталу як складової частиною інтелектуального капіталу через наступні ознаки якості: навички, знання, досвід, креативний спосіб мислення, творчі здібності, культура праці, моральні цінності та ін. Наразі існує багато наукових праць з висвітлення проблематики щодо ролі управління персоналом в частині забезпечення прибуткової діяльності підприємства, а також його економічної безпеки.

Незалежно від форми власності підприємства система управління персоналом є найбільш ефективним інструментом забезпечення конкурентоспроможності та розвитку. Саме тому виникає потреба в підвищенні ефективності системи управління людськими ресурсами з урахуванням вимог поточної ринкової економіки. Керівництво підприємства,

яке працює в ринкових умовах, може висувати високі вимоги до професіоналізму та компетенцій управлінського персоналу.

Служба з керування персоналом координує діяльність з управління трудовими ресурсами підприємства та реалізує кадрову політику; необхідне розширення функцій до створення нових систем стимулювання трудової діяльності, управління ринку трудових ресурсів, створення резервів кадрів для управлінського персоналу. Система управління персоналом надзвичайна складна, вона забезпечує безперервне вдосконалення методів роботи з кадрами й використанням успішного виробничого досвіду.

Ця система включає в себе підсистему лінійного управління, а також функціональних підсистем, які спеціалізуються на виконанні однорідних функцій. Кожна підсистема має власні конкретні функції, виконання яких має сприяти досягненню мети діяльності організації. Підсистема лінійного керівництва здійснює управління підприємством в цілому, управління окремими виробничими і функціональними підрозділами. Функції даної підсистеми виконують: керівник організації, його заступники, керівники виробничих і функціональних підрозділів, а також їх заступники, бригадири, майстри. Безперервно ведеться інтенсивний пошук шляхів формування найбільш оптимальної системи керування персоналом, котра б відповідала трьом основним вимогам: висока ефективність, гнучкість та регулярне оновлення.

Найчастіше при управлінні персоналом виникають такі проблеми, як: підбір, формування кадрів із сучасним економічним мисленням, забезпечення максимальної ефективності роботи працівників, оцінювання ефективності системи керування персоналом, збереження сприятливого клімату в колективі компанії, тощо.

Функціонування комплексної системи керування персоналом підприємства найбільш правильно розглядати як частину ефективності діяльності організації в цілому. Однак, наразі загальноприйнятий підхід до оцінки такої ефективності відсутній. Методологічний підхід представляється доцільною оцінкою ефективності на рівні системи управління, на рівні органу управління, на рівні окремих взятих працівників, при цьому звертаючи особливу увагу на співвідношення фактичної кількості персоналу до планової, відповідність професійного рівня, освіти, досвіду персоналу вимогам займаних робочих місць. Оцінка ефективності керування персоналом організації полягає саме у визначенні економічної ефективності за рахунок найбільш дієвого використання трудового потенціалу, соціальної ефективності шляхом задоволення потреб і інтересів працівників компанії, мотивації та організації праці,

організаційної ефективності через організаційну оформленість підприємства і та його цілісність.

Оцінка ефективності управління персоналом – це чітко формалізований систематичний процес, який спрямований на вимірювання вигод та витрат, пов'язаних із програмами діяльності керування персоналом, для співвіднесення їхніх результатів з підсумками роботи, з показниками конкурентів і поставленими цілями організації. В сучасних умовах оцінка ефективності функціонування системи управління персоналом вимагає систематичного досвіду, вимірювання витрат і вигод загальної програми управління персоналом і порівняння її ефективності з ефективністю роботи підприємства за аналогічний період.

В сучасних умовах є потреба в запровадженні статистичної економіко-математичної моделі показників економічного обґрунтування управлінських рішень для вирішення проблем оцінювання ефективності системи управління персоналом. Управлінські рішення, які приймаються керівництвом організації з метою вибору оптимальних варіантів, для їх впровадження в ту чи іншу систему операційної або іншої структури підприємства повинні мати достовірну статистичну інформацію управлінської діяльності компанії, використовуючи експертні оцінки компетентних менеджерів фахової кваліфікації. На базі сформованого масиву достовірної інформації має будуватися статистична оптимізаційна економіко-математична модель показників економічного обґрунтування управлінських рішень на підприємстві. Таких підхід може допомогти запобіганню небажаних втрат (в тому числі втрат цінних та кваліфікованих працівників), тому на підприємстві буде доцільно розробити та запровадити заходи для одержання інформації (такі як анкетування, індивідуальні співбесіди, тощо) щодо ступеня задоволеності кожного співробітника роботою, психологічного клімату в колективі, умовами праці та відпочинку, задоволеністю рівнем зарплати та системою мотивації.

Тож, кінцева мета роботи з керування персоналом в умовах ринкових відносин – це максимальне зближення очікувань підприємства та інтересів співробітника, відмова від політики мінімалізації вкладень в персонал підприємства і відведення вирішальної ролі системи управління персоналом у формуванні кадрової політики і механізму її реалізації. Також не менш важливим фактором щодо підвищення ефективності управління персоналом в компанії є наявність та зміст політики розвитку персоналу, яка має передбачати наявність ефективних адаптаційних програм, систем і програм навчання, підвищення кваліфікації та можливості саморозвитку особистості.

Список використаних джерел:

1. *Козак К. Б. Дослідження проблем управління персоналом на сучасних підприємствах / К. Б. Козак // Теоретичні та практичні аспекти менеджменту. – 2014.*

2. *Виноградський М. Д., Бєляєва С. В., Виноградська А. М., Шканова О. М. // Управління персоналом. Навч. пос. для ВНЗ. – 2006.*

Онишко В. О.

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

ЗМІНИ РОЛІ УПРАВЛІННЯ ПЕРСОНАЛОМ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ

Цифрові технології стали рушійною силою змін у всіх галузях. Темпи цифрової революції можна виміряти місяцями, тоді як організаціям та її співробітникам потрібні роки, щоб повністю усвідомити такі фундаментальні зміни у тому, як вони працюють. Управління змінами, безумовно, є найстійкішим вузьким місцем цифрової трансформації [3, 4].

Цифрові трансформації компанії реалізуються за допомогою HR за рахунок впровадження нових технологій.

HR – це люди, які працюють у компанії чи організації, та відповідають за роботу з персоналом. Управління людськими ресурсами (управління персоналом) - сучасний термін, який використовується для опису механізму управління персоналом організації. Також використовується як управління персоналом або талантами, тобто управління ресурсами включає моніторинг всіх компонентів, які пов'язані з управлінням людського потенціалу організації; характеризує процес найму та розвитку у співробітників здібностей підвищувати цінність для організації [5].

Можливості управління людськими ресурсами в організаціях, заснованих на технологіях, можуть значно підвищити ефективність організації. Поява концепції e-HRM [7] інтерпретується не лише у вузькому значенні як адміністративна підтримка функцій управління персоналом в організаціях, що ґрунтуються на інтернет-технологіях, що дозволяє підвищити ефективність діяльності з управління людськими ресурсами, а й як стратегічна детермінанта життєво важливих організаційних рішень.

Цифровізація зустрічається в організаціях у формі інтелектуальних операцій із використанням платформ, доступних для багатьох сторін [6]. Цифрові рішення дозволяють організаціям аналізувати великі обсяги даних, які всебічно необхідні бізнес-процесах, залежно від необхідного часу [7].

Цифрове управління персоналом - це планування та впровадження цифрових технологій для підтримки та мережевої взаємодії кадрової професії. Операційні функції HR, такі як обробка платіжних відомостей, і навіть управлінські функції, такі як компенсація, управління продуктивністю

чи розвиток, підтримуються «у цифровому вигляді» [1]. Позитивні операційні ефекти такого цифрового управління співробітниками, такі як менші витрати, більш висока швидкість та якість HR-процесів, зростання корпоративності та довіри між зацікавленими сторонами, більш стратегічна орієнтація тощо, очевидні. Деякі негативні проблеми, такі як неприйняття користувачами, загрози конфіденційності, втрата особистих контактів, скорочення кадрового відділу або обтяження фахівців з персоналу технічною реалізацією, адмініструванням та прикладними завданнями, не повинні залишатися поза увагою [4]. Завдання HR-професії — виявити, розвинути та використовувати позитивний потенціал цифровізації, уникаючи при цьому або принаймні скорочуючи супутні недоліки [1].

Взаємодія з цифровими технологіями сформувала нове покоління людей з різними поглядами, кваліфікацією, поведінкою та очікуваннями. Люди цього покоління - потенційно нові учасники в організаціях - більш багатозадачні, мають цифрові можливості / кваліфікацію, їм подобаються і шукають додаткову інформацію та мережі, які вони вивчають на практиці, і просять більшої та миттєвої винагороди [4]. Очевидно, що HRM слід змінити та узгодити свої стратегії та діяльність із цією новою когортою на ринку праці, такою як «цифрові співробітники». Стратегічна та оперативна адаптація HRM до мінливих кадрів є кроком, необхідним для подальшої підтримки організацій за допомогою нових, різних та автоматизованих методів найму, відбору та лідерства [2, 3]. Штучний інтелект (машини), наприклад, може заощадити час рекрутерів і дозволити їм більше зосередитися на людському аспекті чи наймі, а також покращити досвід кандидатів (тобто менший час відгуку, регулярне спілкування, планування співбесід) [1].

Цифровізація у сфері HR призводить до зміни балансу часу, що витрачається фахівцем з управління персоналом виконання операційних і стратегічних завдань. Якщо раніше 80% робочого часу йшло виконання операційних завдань і 20% на стратегічні, нині можна говорити про співвідношенні 40% до 60% [2, 3]. Тому в епоху цифрової трансформації фахівцю з управління персоналом необхідно сфокусуватися не лише на технологіях, а й на людях, допомагаючи корпоративним лідерам та працівникам перейти насамперед до нового способу мислення. Головна риса такого мислення – гнучкість та адаптивність, засновані на визнанні високої швидкості змін в епоху цифровізації [2]. У сучасних компаніях HR-фахівець є помічником, консультантом керівника, бізнес-партнером (HRBP), якого необхідно прислухатися при прийнятті кадрових рішень. Виходячи з цього, можна виділити наступний тренд - трансформація ролі та функцій HR [4].

Фахівці з управління персоналом у сучасних компаніях є провідниками культури, філософії та стратегії, яку задумали керівники компанії. Це потребує розвитку компетентності HR-фахівця у сфері кадрового консалтингу [3]. Наступний тренд, який можна виділити – це вміння чути та ефективно комунікувати зі співробітниками. Найважливішими напрямками роботи HR-фахівця в умовах цифрової трансформації та постковидної реальності є: розробка компенсаційних стратегій та кастомізація компенсаційних програм під конкретний сегмент людських ресурсів, розробка програм благополуччя персоналу, управління персоналом різних поколінь (X, Y, Z), управління мультикультурним колективом, проектування високопродуктивних крос-функціональних команд, синхронізація цілей та цінностей команд та компанії, «розпакування» потенціалу талантів, підвищення залучення віддалених співробітників, інтеграція штучного інтелекту в роботу з персоналом та ін [3].

Очевидно, що цифрові технології впливають на HR-діяльність та змінюють роль HR-менеджерів зі статичної на динамічну та стратегічну. Перед HR-менеджерами стоїть безліч завдань та можливостей підвищити продуктивність співробітників і, зрештою, прибутковість за рахунок ефективного підключення цифрових співробітників до автоматизованих робочих місць та нових цифрових форм та організаційної структури. Необхідні нові кадрові стратегії, щоб заповнити прогалину в цифрових навичках, підвищити лояльність і залученість, керувати різноманітністю, що дозволяє інтегрувати роботу та життя, та зберігати кадровий резерв цифрових співробітників [2]. Для успішного виконання своєї нової ролі менеджери з персоналу повинні діяти в першу чергу як стратегічні позиціонери (необхідно знати бізнес-контекст і зовнішні фактори), як агенти змін і як прихильники технологій (необхідно знати, як отримати доступ, проаналізувати, оцінити і ділитися інформацією) та як застосовувати нові інформаційні технології [3]. Самі менеджери з персоналу повинні набувати цифрових навичок і підвищувати свою цифрову спритність.

Список використаних джерел:

1. Александрова Н. А., Брюхова О. Ю., Васильцова Л. И., Внуковский Н. И., Волкова Т. П., Доценко А. М., Каштанова Е. В., Клепалова Ю. И. и др. / Управление персоналом в цифровой среде / – Екатеринбург: Изд- во УрГУПС, 2021.

2. Бердуэлл, Дж., Томпсон, А. /Управление человеческими ресурсами: современный подход/ - 2017.

3. Боксолл, П., Перселл, Дж. / Стратегическое управление человеческими ресурсами. Международный журнал управленческих обзоров/ – 2000. – № 2. – С. 183–203.

4. Bersin J., McDowell T., Rahnema A., Van Durme Y. / The Organization of The Future: Arriving Now, in Global Human Capital Trends/ - 2017 - pp. 19–28.

5. Dahlbom P., Siikanen N., Sajasalo P., Jarvenpää M. / Big Data and HR Analytics in The Digital Era, Baltic Journal of Management/ - № 15(1) - 2018 - pp. 120-138. DOI: 10.1108/BJM-11-2018-0393.

6. Khan M., Mushtaq U. /Evolution of Strategic Role of Organization's Human Resource Management: an Overview, Journal of Bussiness & Economics/ - № 7(1) - 2015 - pp. 236-257.

7. Voermans M., Van Veldhoven M /Attitude towards E-HRM: an Empirical sStudy at Philips, Personnel Review/ - № 36(6) - 2007 - pp. 887-902.

Ретізник А. В.

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

СУЧАСНІ МЕТОДИ УПРАВЛІННЯ ПЕРСОНАЛОМ

На даний момент, світ переходить у нову еру розвитку, яка називається четвертою промисловою революцією, або Industry 4.0. Ця революція ґрунтується на синергії кількох масштабних технологій, таких як біотехнології, нанотехнології, штучний інтелект, IT, цифрова трансформація, робототехніка, використання кібер-фізичних систем у виробництві та створення нових матеріалів і 3D-друку. Четверта технологічна революція, як і будь-яка інша, призводить до появи нових організаційних структур і технологій управління, а також радикально змінює характеристики бізнес-середовища.

Отже, можна стверджувати, що розвиток технологій четвертої промислової революції є головною причиною зміни практики управління персоналом. Цифрова трансформація та технологізація стають всеохоплюючою тенденцією, що охоплює не тільки інформаційно-комунікаційну галузь, але й усі сфери господарської діяльності [1]. Цифровізація полягає в проникненні інформаційних технологій в різні сфери виробничо-господарської діяльності. Розвиток цифрових технологій та використання кібер-фізичних систем призвели до появи нових форм зайнятості, таких як робота за запитом за допомогою додатків (work-on-demand via apps) та краудворк (crowdwork). У наш час найпопулярнішими інтернет-платформами для цих форм зайнятості є Uber, Airbnb, YouDo тощо.

Сучасні компанії все більше приділяють увагу впровадженню ERP-систем з метою оптимізації бізнес-процесів та підвищення ефективності управління в цілому. Вміння працювати з великими обсягами даних (Big Data) стає одним з ключових факторів, що допомагає HR-менеджерам ефективно виконувати свої обов'язки.

Феномен Big Data можна охарактеризувати за допомогою акроніма 5V: концепти volume – великий обсяг даних, який незручно обробляти на одній машині; velocity – швидкість надходження даних; variete – геторогенність даних; variability – мінливість; validity – валідність даних [2].

Концепція 5V описує умови, які потрібні для ефективного збору та обробки великих обсягів даних. Глибинний аналіз даних дозволяє здобути більш повну та достовірну інформацію для прийняття рішень управління.

У зв'язку з довготривалою інтеграцією штучного інтелекту та роботів в компаніях протягом багатьох років, змінюються знання, вміння та навички, необхідні для ефективного виконання роботи на будь-якій посаді(рис. 1).

Цифрова трансформація бізнес-процесів звільняє працівників від рутинних завдань та надає їм можливість зосередитися на більш складних та творчих завданнях. Одночасно це призводить до зростання вимог до кваліфікації працівників, але штучний інтелект та робототехніка забезпечують більш вагому роль «людських аспектів» роботи. Навички, такі як емпатія, особисте ставлення, переконання та прийняття стратегічних рішень, є більш цінними, ніж будь-коли раніше. У цільовій моделі компетенцій на перший план виходять когнітивні, цифрові та соціально-поведінкові навички.

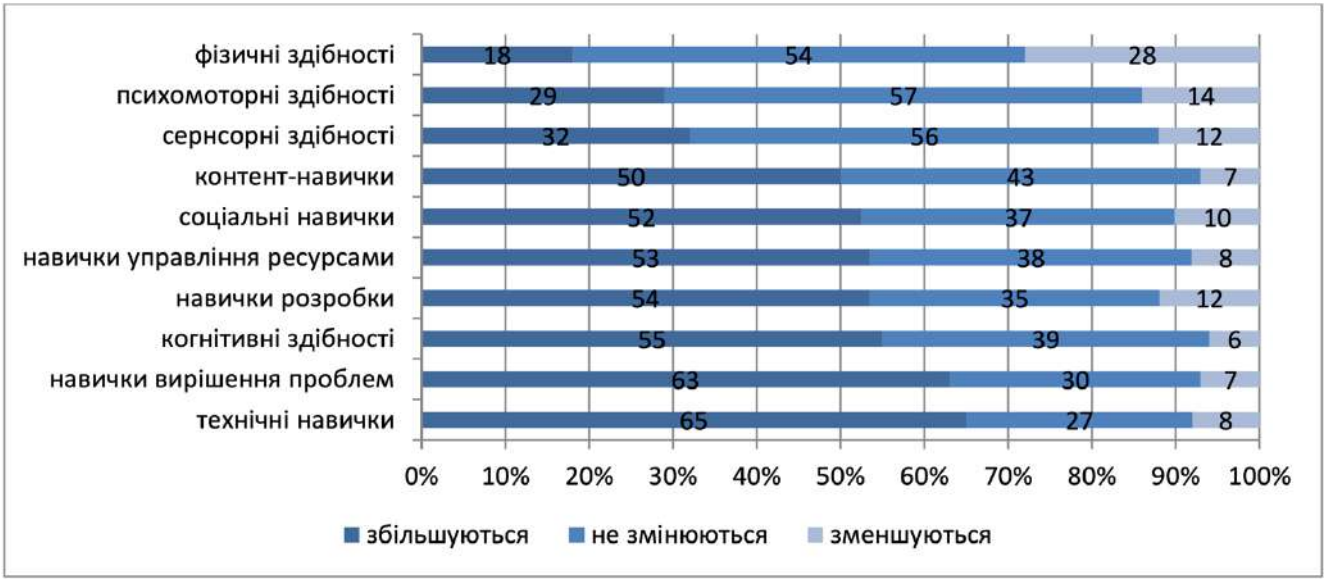


Рис. 1. Зміни в компетенціях співробітників під впливом роботизації [3]

Новою концепцією розвитку сучасного бізнесу є VUCA, що є акронімом від англійських слів: змінливість (volatility), невизначеність (uncertainty), складність (complexity) та неоднозначність (ambiguity). Ця концепція була запропонована Н. Беннетом та Дж. Дж. Лемуаном. Фактично, в світі спостерігається кілька помітних тенденцій: зростання швидкості змін, прискорення трансакцій та будь-якої діяльності, часті зміни стратегій соціальної взаємодії і політичних орієнтирів, постійні зміни у бізнес-оточенні та турбулентність процесів у всіх сферах діяльності [4].

В даний час відбувається подальша трансформація парадигми управління в усьому світі. Це не просто перехід від концепції управління персоналом до управління людськими ресурсами (HRM), але переходить до концепції управління людським капіталом (HCM) та управління людьми.

Останнє, з одного боку, спрямоване на активний пошук і розвиток талантів, а з іншого боку, покладає акцент на гуманізацію HR-практик та турботу про співробітника організації.

Для визначення ключових трендів, які набули поширення в управлінні персоналом на сьогоднішній день, було використано результати щорічного дослідження компанії Deloitte «Global Human Capital Trends». За результатами дослідження можна виділити наступні фундаментальні зміни в сфері управління персоналом.

1. Створення екосистеми персоналу: управління працівниками поза межами компанії. Останнім часом все більш популярними стають "альтернативні способи працевлаштування", такі як фріланс, проектна робота, неповний робочий день або гіг-робота. За даними експертів, до 2020 року більше 40% працівників у США були зайняті "альтернативними способами". Зараз традиційні відносини між роботодавцем і працівником замінюються на "екосистему робочих ресурсів", що включає різні пули співробітників, мережі талантів, гіг-працівників та постачальників послуг, що надає роботодавцям гнучкість, можливості та потенціал для вивчення різних економічних моделей пошуку талантів [3].

2. Увага до корпоративної соціальної відповідальності посилюється, і в країнах ЄС поширені критерії оцінки організацій за їхнім рівнем розвитку в цій сфері. Ці критерії включають такі аспекти, як відсутність дискримінації при наборі персоналу, рівень інтеграції працівників, інтеграція співробітників з обмеженими можливостями, наявність системи супроводу і перенавчання для співробітників на критичних посадах, якість діалогу з профспілками та дотримання коректних умов праці.

3. Активне впровадження нових методів роботи і нових місць для роботи. В останні роки стали популярні «гнучкі методи і методології» організації роботи. Одними з таких методів є Agile. Agile-методи базуються на двох принципах: спілкування між співробітниками особисто, та короткострокова орієнтація на постановку завдань, пошук рішень та оцінку результатів. Agile-підхід оцінює значення людського та професійного спілкування, забезпечує почуття впливу на відбуваючіся події, підвищує відчуття послідовності та визначеності та допомагає підтримувати баланс у взаємодії між людьми та організаціями [5].

4. Цифровізація технологій підбору персоналу. Ключовими тенденціями в цій сфері є автоматизація скринінгу і процесу найму співробітників.

5. Розвиток цілісних, гнучких та персоналізованих систем винагород. В порівнянні з іншими областями управління персоналом, зміни в системі

мотивації співробітників є еволюційними, а не революційними і сприяє підвищенню рівня ефективності працівника.

Всі ці методи надають більш ефективно і якісно використовувати людські ресурсі і суттєво полегшують управління персоналом навіть в умовах кризової ситуації, а також надають більше можливостей для планування і організації роботи компанії в цілому.

Список використаних джерел:

1. Підбір персоналуа в цифрову епоху. URL: https://www2.deloitte.com/ru/ru/pages/ humancapital/articles/2018/podbor-personala- v-cifrovuyu-ehpohu.html.

2. Петрова І. Л. Ідентифікація стратегії управління персоналом: родові ознаки та видові відмінності. Україна: аспекти праці. 2011. No5. С. 9-14.

3. Deloitte (2018). Global Human Capital Trends 2018. URL: https://hctrendsapp.deloitte.com/.

4. Kaufman B. E. Evolution of strategic HRM as seen through two founding books: A 30th anniversary perspective on development of the field. Human Resource Management. 2015. No54(3). PP. 389-407.

5. Петрова І. Л. Стратегічне управління розвитком персоналу. Науковий вісник PUET: Economic Sciences. 2014. №5 (50). С. 128-132.

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.*

Топчий А. Ю.

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

ОРГАНИЗАЦИЯ БИЗНЕСА И УПРАВЛЕНИЕ ПЕРСОНАЛОМ В УСЛОВИЯХ ВОЙНЫ

Вопрос как помочь своим сотрудникам, сейчас стоит перед многими компаниями. Что должен сделать руководитель для сохранения имиджа и работы своей организации.

Чтобы помочь команде выработать несколько стратегий для сохранения бизнеса, а в отдельных случаях и его развития нужно приложить немало усилий. Создать антикризисный комитет и организовывать регулярные встречи с персоналом.

Безопасность на первом месте. Работники должны знать, что компания ставит их безопасность превыше всего. Прежде всего вся руководящая ветка компании должна следить за ситуацией в регионах местонахождения своих сотрудников и стараться всегда иметь с ними связь. Напомнить персоналу, что их личная безопасность имеет первостепенное значение, и что работа стоит гораздо дальше по списку. Сейчас время быть более ориентированным на человека. Нужно регулярно проверять их статус и нужды.

Помощь в переезде. Руководитель должен узнать нужна ли потребность в переезде. Если переезд востребован и возможен, то помочь в его организации. Как пример компания Visa наняла маршрутные автобусы для вывоза рабочих из опасных зон.

Деньги не приоритет. Если руководство компании погонится за финансовым капиталом, а не человеческими ресурсами то можно потерять очень ценных сотрудников, опыт которых не заменить. Некоторые сотрудники могут обладать уникальными навыками и порой лучше если этот сотрудник несколько месяцев посидит без работы чем лишится его навсегда.

Отпуск по необходимости. Учитывая обстоятельства работникам следует давать столько времени, сколько необходимо для решения их ситуации. Убедится, что работа сейчас не является дополнительной причиной стресса. Безопасность, ментальное здоровье и доступ к потребностям сотрудника должны быть в приоритете. Для тех, кто возвращается к работе, важна гибкость. Это может включать перенос часов, перераспределение задач, изменение приоритетов, обязанностей или все

вышеперечисленное. Для руководителей же важно оставаться гибкими в том, как они заботятся об сотрудниках, и адаптироваться по мере развития ситуация и их потребностей.

Доступ к психологической помощи. Война может иметь травмирующие последствия для тех, кто с ней сталкивается. Предоставление доступа к консультированию является одним из способов помочь сотрудникам. Многие компании сотрудничают с терапевтами и дает доступ своим сотрудникам все возможное поддержание психологического здоровья. Поскольку даже чтение новостей и переживания за близких наносят серьезный ущерб психическому здоровью.

Любой кризис рано или поздно заканчивается, поэтому в такой ситуации важно найти и обосновать баланс между экономией и продолжением усилий, направленных на дальнейшее восстановление бизнеса до докризисного уровня и последующего развития. В рамках антикризисного управления руководитель проделывает огромную работу по «перепрофилированию» сотрудников, с целью максимального использования их потенциала и компетенций. Крайне важно сохранить ключевых людей в команде, предложив им на время войны ротацию в другие подразделения, что несомненно улучшит их ценность как специалистов и даст большее понимание того, как работает бизнес.

Таким образом, проанализировав все вышесказанное мы можем сделать вывод, что человеческий ресурс самое необходимое в прохождении сложного этапа в жизни компании. И если ценить свой персонал, то после окончания войны компания сможет увеличить рост, заручится имиджем и ценными топ менеджерами в своей команде.

Чорний С. С.

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

КАДРОВЕ ПЛАНУВАННЯ

Операційний менеджер - фахівець, який забезпечує підвищення ефективності роботи компанії. Ця професія пов'язана з аналізом, бюджетуванням, контролем та управлінням.

Операційний менеджер використовує методи та технології, які дозволяють збирати та аналізувати інформацію, а також формувати звіти. Останні використовуються для прийняття управлінських рішень за умов високої ринкової конкуренції.

Оскільки діяльність операційного менеджера відіграє першочергову роль у прибутковості та ефективності всіх бізнес-процесів підприємства, грамотно підібраний та навчений персонал є найважливішою складовою для старту успішних бізнес-процесів та, звичайно , створення сприятливого мікроклімату компанії для більш ефективної роботи та продуктивності, а також формування корпоративної культури організації.

Формування корпоративної культури є невід'ємною частиною даного процесу, оскільки корпоративна культура – це набір цінностей та принципів, які поділяються більшістю співробітників та визначають їхню поведінку стосовно самої організації, клієнтів і, звичайно ж, колег.

Таким чином, під корпоративною культурою розуміють домінуючі моральні норми та цінності, прийняті зразки поведінки та укорінені ритуали, традиції, які поділяються членами організації та здатні відтворюватися в цій організації через формальних чи неформальних лідерів.

Кожне підприємство має формувати свою систему корпоративної культури, щоб досягти наміченої бізнес-мети. Ця система має складатися з певних цінностей і бути сприйнята для розуміння з боку менеджерів підприємства. Саме тому корпоративна культура формується, стає своєрідною візитною карткою підприємства. Вона створює особливу внутрішню атмосферу, яка спонукає людей до виконання доручених їм завдань та місії: підвищуються якість та інтенсивність роботи кожного працівника, зводяться до мінімуму трудові конфлікти. А грамотно спланована кадрова політика суттєво полегшує цей процес і, як наслідок, підвищує ефективність та продуктивність.

Отже, у зв'язку з дефіцитом робочої сили кадрове планування стало у багатьох організаціях інтегруючою складовою підприємницького планування.

До 60-х років у питаннях управління персоналом орієнтувалися лише на поточні потреби організації. При такому підході роботодавець розраховував отримати у будь-який момент необхідну кількість працівників, для використання яких не потрібно тривалої спеціальної підготовки. Надлишковий ринок робочої сили давав роботодавцям таку можливість, а звільнення надлишкового персоналу практично нічого не коштувало. Зміни за умов діяльності організацій висунули як загальну всім вимогу орієнтуватися для формування ресурсів не тільки на поточні потреби, а й на тривалу перспективу. Ця вимога стосується всіх видів ресурсів, у тому числі людських.

У 70-80 рр. у практиці управління став застосовуватися систематичний аналіз перспективних потреб організацій та фірм в окремих категоріях персоналу. Сьогодні дедалі більше компаній виділяють як самостійний вид діяльності кадрових служб кадрове планування, чи планування людських ресурсів.

Ці зміни, що пов'язані з незворотністю економічних реформ і рухом до здорової конкуренції, змушують організації України приділяти значну увагу довгостроковим аспектам кадрової політики, що базується на науково обґрунтованому плануванні.

Планування персоналу (еквіваленти, що зустрічаються у літературі - кадрове планування, планування робочого складу підприємства) визначається як «процес забезпечення організації необхідною кількістю кваліфікованого персоналу, прийнятого на правильні посади у правильний час». За іншим визначенням, планування персоналу - це «система підбору кваліфікованих кадрів, при використанні двох видів джерел - внутрішніх (існуючі в організації службовці) та зовнішніх (знайдені або залучені із зовнішнього середовища), що має на меті забезпечити потреби організації у необхідній кількості фахівців у конкретні часові рамки».

По-суті, кожна організація використовує кадрове планування явно чи неявно. Деякі організації роблять у цьому плані серйозні дослідження, інші обмежуються поверхневою увагою щодо планування персоналу.

Несумлінно виконане, і тим більше - зовсім проігнороване кадрове планування здатне спровокувати серйозні проблеми вже в найкоротший час. А за допомогою ефективного кадрового планування можна «заповнити» вакантні позиції, а також зменшити текучість кадрів, оцінюючи можливості кар'єри фахівців у межах компанії.

Кадрове планування має дати відповіді такі питання:

- скільки працівників, рівень кваліфікації, коли та де будуть необхідні (планування потреби в персоналі);

- яким чином можна залучити необхідний та скоротити зайвий персонал, враховуючи соціальні аспекти (планування залучення чи скорочення штатів);

- яким чином можна використовувати працівників відповідно до їх здібностей (планування використання кадрів);

- яким чином можна цілеспрямовано сприяти підвищенню кваліфікації кадрів та пристосовувати їх знання до змінних вимог (планування кадрового розвитку);

- яких витрат вимагатимуть заплановані кадрові заходи (витрати на утримання персоналу);

Основними завданнями кадрового планування є:

- розробка процедури кадрового планування, узгодженої з іншими його видами;

- ув'язування кадрового планування з плануванням організації в цілому;

- організація ефективної взаємодії між плановою групою кадрової служби та плановим відділом організації;

- реалізація рішень, що сприяють успішному здійсненню стратегії організації;

- сприяння організації у виявленні основних кадрових проблем та потреб при стратегічному плануванні;

- покращення обміну інформацією з персоналу між усіма підрозділами організації.

Кадрове планування включає:

- прогнозування перспективних потреб організації у персоналі (за окремими його категоріями);

- вивчення ринку праці (ринку кваліфікованої робочої сили) та програми заходів щодо його «освоєння»;

- аналіз системи робочих місць організації;

- розробка програм та заходів щодо розвитку персоналу.

При здійсненні кадрового планування організація має такі цілі:

- отримати і утримати людей потрібної якості та в потрібній кількості;

- найкращим чином використати потенціал свого персоналу;

- бути здатною передбачати проблеми, що виникають через можливий надлишок або брак персоналу.

Виходячи з вищевикладеного можна зробити висновок, що процес грамотно спланованої кадрової політики та правильно підібраний персонал є

одним з найважливіших процесів на шляху досягнення бізнес-цілей компанії, організації сприятливих умов і взаємовідносин, формування корпоративної культури, що значно полегшує завдання будь-якому керівнику, в тому числі операційному менеджеру, оптимізувати і якісно виконувати свою роботу.

Список використаних джерел:

1. *Одегов Ю. Г., Журавлев П. В. Управление персоналом.- М., - 1997;*
2. *Основы управления персоналом. – (под ред. Генкина Б. М.), - М., 1996;*
3. *Алавердов А. Р. Управление человеческими ресурсами организации. - М.: Маркет ДС, 2013;*
4. *Балдин К. Корпоративная культура – М.: Экзамен, 2011;*
5. *Капитонов Э. А. Корпоративная культура: теория и практика – М.: Дело, 2010.*

Stanislav Fedorenko

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

ANALYSYS OF TEAM AND WORK GROUP CHARACTERISTICS IN SOFTWARE DEVELOPMENT TO BUILD EFECTIVE TEAM

Software development projects are becoming more and more complicated over the years [1]. They require collection, gathering, and processing of huge amount of information, coordination and cooperation of highly-skilled individuals that can accomplish their goal only combining their efforts [2]. Moreover, they operate in dynamically changing environment. Thus project team performance and efficiency predetermine company's success as a whole. Besides, the teamworking influences not only operational results but also creates positive worker attitudes. And the second outcome plays not less role in success of organization. [1]. The described approach represents a way of improvements areas identification to make software development team much productive and move from "working group" to "team" operation model.

As it was mentioned by Huczynski and Buchanan [3] creation of a team structure is one of the basic appearance of group formation. There is a common approach when customer decides how many people, with what qualification it is required to hire and when, depending on customer's plans, budget and its own corporate structure with which outsourcing team should align. Team structure in such case corresponds to traditional job roles (as described by Raymond [4], or Sheard [5]). From the other side, every software development methodology has its own view on job roles in the team, and determines a kind of process to follow [6]. *P*opular agile software development methodology - SCRUM. Agile [7] points much attention to people, their communications and interactions, and team working, altering the flow of information in a company, that leads to modification in roles previously defined in traditional software development and agreement with the customer. This realignment of roles could cause confusion of expectations from a team member both from the customer side as well as from an employee.

The traditional point of view on roles in software development is based on formal professions: architects, developers, analysts, testers, project managers etc. Hiring person to the team we always specify what profession and what level of qualification he or she should correspond [1]. It seems, that according to traditional roles individuals are supposed to work on their own piece of work not correlating

with others. For instance, Raymond [4] argued that roles in software development should be strictly defined making development similar to building a cathedral, where a small team of people working in an isolated environment. The drawback of such approach is that outcomes are only visible for a limited number of people [1]. When people join the team they are supposed to work on a common goal and frequently combining efforts with other teams. As emerging tasks are very complicated and diverse job roles cannot be strictly defined and here come SCRUM roles. Schwaber and Beedle [8] specified 14 SCRUM roles that should support process of development where everyone in the team works together to complete the set of tasks they have collectively committed to finish within a sprint (A sprint (or iteration) is the basic unit of development in scrum. The sprint is a timeboxed effort; that is, it is restricted to a specific duration). As a result each team member actually has two job roles i.e. formal position and SCRUM role. Finally, it should be mentioned that SCRUM roles are not completely different from traditional ones. As it was stated by Murat Yilmaz Rory V. O'Connor and Paul Clarke [9] some roles appeared in SCRUM with an other name but similar responsibilities, however, some roles really have been changed completely their responsibilities.

Summarizing the question of roles and their role in team development is could be said that SCRUM model itself tends to unite individuals into a team.

One of the famous theories used to analyse the processes of groups development is the one proposed in the works of Tuckman and Jensen [10]. They presented a model which featured and resuming the main characteristics inherent to groups. They created a five stage model and named the processes groups go through forming, storming, norming and performing with added by Jensen adjourning phase. Huczynski and Buchanan [3] noticed that team is a group that passed stages of forming, storming, norming of Tuckman and Jensen's model and reached stage of performing. Thus, it is assumed that team development is achieved through group development. Team in this context can be defined as a group of people sharing the common goal and possessing additional positive features. A lot of theoretical models have been emerged in order to explain how groups are developing. Moreover, due to a large number of these models other theories have developed to contrast and synthesize them creating typologies. The practical application of the topic of team formation through group development is defining the way how to improve the quality of the output produced by a team, how to manage conflicts and how to provide individual feeling of belonging to the team.

Starting analysis of the group dynamics in practice it is useful to analyze what is the current state of it. Tuckman and Jensen theory shows what are behavior

models for each phase but does not propose metrics according to which group starting point can be estimated. Analyzing a team in the context of characteristics proposed by Katzenbach and Santamaria [11] we can draw conclusions to what extend this organizational unit can be considered as a team. For example:

Characteristic	**Team description (lets call "DevTeam")**	**Team or work group**
Leadership	DevTeam as dual role structure (as it was described above). There is a formal leader (Team Lead) who is informal leader as well. From the other hand there is a rotating role of SCRUM master (facilitator). It is assumed that SCRUM team is a team of equal self-organizing professionals but in practice Team Lead would be responsible for team failures.	One assigned senior individual is a feature of work group
Goals	Goals in the DevTeam can be set by customer (deadlines for the project), by managers (designed model of work with the customer), by team leader (level of outcomes quality) or by the team itself (short- and mid-term goals within the project, goals for the sprint). it depends on situation and goal complexity.	In this extend DevTeam possess features of both team and group as goals can be defined by team discussion or set by formal leader
Work organization	One of the major idea of SCRUM is that work organization should be set and regularly adjusted by the team through retrospective meetings[1] and work coordination by SCRUM master. In DevTeam this process is implemented: team can decide how to work in order to create comfortable and effective work conditions	As work organization is decided by team members DevTeam can be considered as a team according to this characteristic
Outputs	DevTeam is responsible for developing complex projects in investment banking. Tasks are divided among team members and their accomplishment requires close collaboration. Often is practiced pair programming (technique in which two programmers work as a pair together on	This feature characterizes DevTeam as a team

Characteristic	Team description (lets call "DevTeam")	Team or work group
	one workstation in order to reach better designs, fewer bugs, and much better spread of knowledge across a development team, and therefore more functionality per unit time, measured over the long term..	
Performance	DevTeam works together half a year and their performance and stability of results raises	This feature characterizes DevTeam as a team as at the beginning team members learn how to work together
Accountability	DevTeam has clear accountability due to the SCRUM usage.	This feature characterizes DevTeam as a team as all team members hold each other accountable
Works well with	Right now DevTeam works better with time pressured tasks.	This feature characterizes DevTeam as a work group

Summarizing table above it could be observed that while according to some characteristics DevTeam could be considered as a team, other show it as a work group. This model is useful in terms of understanding what exactly characteristics should be developed to create real team and move from work group ways of working.

References:

1. Smoilovska, Y (2015) Teams formation in software development company. Bradford University School of Management MBA

2. Humphrey, W (2000). Introduction to the team software process. Addison-Wesley Professional.

3. Huczynski, A, Buchanan, D. (2013). Organizational behaviour. Edinburg Gate: Pearson Education Limited, p.357.

4. Raymond, E. (1999). The cathedral and the bazaar. Knowledge, Technology & Policy, 12, 23–49.

5. Sheard, S. (1996). Twelve systems engineering roles. In: Proceedings of INCOSE, Citeseer.

6. Zahran, S. (1998). Software Process Improvement: Practical Guidelines for Business Success. Addison Wesley.

7. Beck, Kent et al. (2001). Manifesto for Agile Software Development. Agile Alliance.

8. Schwaber, K., Beedle, M. (2002). Agile Software Development with SCRUM. Prentice Hall.

9. Yilmaz, M., O'Connor R., and Clarke, P. (2012). A Systematic Approach to the Comparison of Roles in the Software Development Processes. Conference paper. http://www.fh-kl.de/~amueller/vorlesungen/se/role%20comparison.pdf [Accessed 29/06/2015]

10. Tuckman, Bruce W. (1965). Developmental sequence in small groups. Psychological Bulletin, Vol 63(6), 384-399.

11. Katzenbach, J. R. and Santamaria, J. A. (1999) 'Firing up the front line', Harvard Business Review, 77(3), pp. 107-17. https://hbr.org/1999/05/firing-up-the-front-line

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

Mgr. Pavel Polián 5

THE EXEMPTION FROM CRIMINAL LIABILITY FOR CORRUPTION CRIMES 5

Копотун І. М. 10

НАДЗВИЧАЙНІ ПОДІЇ КРИМІНАЛЬНОГО ХАРАКТЕРУ У КРИМІНАЛЬНО-ВИКОНАВЧИХ УСТАНОВАХ 10

Рудик М. М. 15

ОСОБЛИВОСТІ ЗАПОБІГАННЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ У СФЕРІ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ ТА ЕКСПЛУАТАЦІЇ ТРАНСПОРТУ В УКРАЇНІ 15

Сибір І. В. 18

КРИМІНОЛОГІЧНІ РЕАЛІЇ ГУМАНІТАРНОЇ ДОПОМОГИ ТА БЛАГОДІЙНОСТІ В УКРАЇНІ 18

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

Лясота А. Є. 21

СТАГНАЦІЯ ПОЛІТИЧНОЇ СИСТЕМИ В УМОВАХ ДЕМОКРАТИЧНОГО ТРАНЗИТУ 21

Стеньгач Н. О. 26

ІДЕЯ ЗАХИСТУ ЗАГАЛЬНОСУСПІЛЬНОГО БЛАГА У ПОЛІТИКО-ПРАВОВІЙ КУЛЬТУРІ КОЗАЦЬКОЇ СТАРШИНИ ГЕТЬМАНЩИНИ (ДРУГА ПОЛОВИНА XVII – XVIII СТ.СТ.) 26

Коруняк А. В. **31**
ВЗАЄМОДІЯ СТАРОСТ ТЕРИТОРІАЛЬНИХ ГРОМАД ТА ОРГАНІВ САМООРГАНІЗАЦІЇ НАСЕЛЕННЯ **31**

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

Кушнєров Є. О. **34**
АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ РЕАЛІЗАЦІЇ ТА ЗАХИСТУ ПАТЕНТНИХ ПРАВ **34**

Васечко В. О. **38**
ПРАВОВІ ЗАСАДИ ОТРИМАННЯ ТИМЧАСОВОГО ЗАХИСТУ В ЧЕСЬКІЙ РЕСПУБЛІЦІ **38**

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

Власюк Р. А. **42**
ПІДВИЩЕННЯ ВИМОГ ДО ПРАЦІВНИКІВ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ В УМОВАХ ВІДДАЛЕНОЇ РОБОТИ **42**

Воробьев И. О. **46**
ОЦЕНКА СПОСОБНОСТИ ПЕРСОНАЛА ПРЕДПРИЯТИЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ К ПРОТИВОДЕЙСТВИЮ КИБЕРУГРОЗАМ **46**

Грішко Д. Ю. **50**
ЗВ'ЯЗОК ПРОБЛЕМ ЕТИКИ ТА КІБЕРБЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ **50**

Малюга Ю. І. **53**
КІБЕРВІЙНА ЯК СКЛАДОВА ГІБРИДНОЇ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ 2013-2022 РОКУ **53**

Мацько В. А. **58**
КІБЕРБЕЗПЕКА ТА КІБЕРРИЗИКИ В АВТОНОМНИХ ТА НАПІВАВТОНОМНИХ АВТОМОБІЛЯХ **58**

Медвідь І. А. **63**
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБ-ДОДАТКІВ **63**

Мирченко І. Є. **68**

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ 68

Науменко П. С. 71

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ 71

Радагуз М. В. 77

ГЕЙМІФІКАЦІЯ ПРОЦЕСУ ПЕРЕВІРКИ КІБЕРБЕЗПЕКИ ПРОДУКТУ 77

Срибный Р. О. 81

БЕЗОПАСНОСТЬ САЙТА: АНАЛИЗ 10 ОСНОВНЫХ УГРОЗ И КАК ОТ НИХ ОБЕЗОПАСИТСЯ 81

Ягнич І. М. 86

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЛЯ ВЕБ-САЙТІВ 86

Dmytro Barsukov 90

COMPREHENSIVE SECURITY-AS-A-SERVICE (CSAAS) AS AN EFFECTIVE SOLUTION TO ADDRESS CYBERSECURITY CHALLENGES FACED BY SMALL AND MEDIUM-SIZED BUSINESSES (SMBS) 90

Oleksandr Butyrin 94

REDUCTION OF Security RISKS WITH IT GOVERNANCE PROCEDURES 94

Kostiantyn Chapistrak 98

INTERNAL THREATS TO INFORMATION SECURITY IN SMALL BUSINESSES 98

Maksym Kozachenko 103

GLOBAL EFFORTS BY LEADING COUNTRIES IN CYBERSECURITY STRENGTHEN 103

Viktor Moskvych 106

FORMAL METHODS FOR SECURE CYBER SYSTEMS 106

Andrii Radahuz 110

CHAT-BASED ROLE-PLAYING GAMIFICATION OF CYBERSECURITY REVIEW 110

Ihor Roid 113

INFORMATION SECURITY CONCERNS IN ONLINE PAYMENT PROCESSING 113

Ievgenii Zhmur 117
INFORMATION SECURITY CONCERNS OF CIVILIAN INFORMATION SYSTEMS IN WARTIME CONDITIONS 117

ПСИХОЛОГІЯ; ПЕДАГОГІКА (в т. ч. ФІЛОЛОГІЯ)

Мороз Л. І. 121

Андрусик О. О. 121
ХАРАКТЕРИСТИКИ ЕМОЦІЙНОСТІ ВИКЛАДАЧА ЯК ЧИННИК ФОРМУВАННЯ ТВОРЧОЇ ОСОБИСТОСТІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ 121

Зубченко Л. В. 125
МОЖЛИВОСТІ ВИКОРИСТАННЯ ФІТБОЛ-АЕРОБІКИ НА ЗАНЯТТЯХ З ФІЗИЧНОГО ВИХОВАННЯ В ДОНЕЦЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ 125

ЕКОНОМІКА

Ромнов А. И. 129
ПРОБЛЕМЫ И ВОЗМОЖНОСТИ, СВЯЗАННЫЕ С ВНЕДРЕНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН В ЛОГИСТИКЕ И ТРАНСПОРТЕ 129

ФІЛОСОФІЯ

Герасимова Е. М. 133
ГЕНДЕРНА ПРОБЛЕМАТИКА ВІТЧИЗНЯНОГО ОСВІТНЬОГО ПРОСТОРУ: ДІЯЛЬНІСНИЙ ПІДХІД 133

Вихованець З. С. 138
КОНЦЕПТУАЛІЗАЦІЯ ЦІЛІСНОГО ЛЮДСЬКОГО БУТТЯ У ФІЛОСОФІЇ ТЕЇЗМУ 138

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ПРИКЛАДКА ІНФОРМАТИКА

Dmytro Levkin 142

Oksana Zhernovnykova 142
INFORMATION AND ANALYTICAL PROVISION OF MATERIAL PREPARATION FOR THE TECHNOLOGICAL PROCESS 142

Курочка С. В. **146**
БЕЗПЕЧНІСТЬ ТА ПРОБЛЕМИ ВИКОРИСТАННЯ ГОТОВИХ РІШЕНЬ ДЛЯ СИСТЕМ РОЗУМНОГО ДОМУ ТА ЇХНЄ ВИРІШЕННЯ **146**

Трофименко О. В. **149**
ОГЛЯД ПРОГРАМНИХ РІШЕНЬ ДЛЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ **149**

Mykhailo Bentsa **151**
GAP ANALYSIS: IDENTIFYING CURRENT SECURITY POSTURE AND AREAS FOR IMPROVEMENT **151**

Serhii Hrytsai **153**
MIGRATE TO THE CLOUD: WHY, WHEN, STAGES **153**

Volodymyr Kovbasiuk **157**
PRACTICAL ASPECTS OF PARALLEL DATA PROCESSING AT HIGH LOAD WITH APACHE KAFKA **157**

Maksym Proniaiev **162**
IMPACT OF TECHNOLOGIES ONTO THE FIELDS OF MANAGEMENT AND SALES. USES OF ARTIFICIAL INTELLIGENCE'S SUCH AS CHATGPT **162**

Artur Stepashkin **166**
VIRTUAL PRODUCTION IN FILMMAKING **166**

Roman Tsekov **169**
THE ADVANTAGES OF MIGRATING THE THE PUBLIC ORGANIZATION EUROPEAN INSTITUTE FOR POSTGRADUATE EDUCATION WEBSITE AWAY FROM THE UCOZ WEBSITE BUILDER AND REDEVELOPING IT WITHOUT RELIANCE ON THE WEBSITE BUILDER JUSTIFY THE RESOURCES AND TIME INVESTED **169**

Kyrylo Zinovyev **172**
ARTIFICIAL INTELEGENCE IN LEGAL SPACE **172**

МЕНЕДЖМЕНТ ТА МАРКЕТИНГ

Андрійчук Я. Р. **177**
ОРГАНІЗАЦІЯ ОПЕРАЦІЙНОЇ ДІЯЛЬНОСТІ БІЗНЕС-ОРГАНІЗАЦІЇ **177**

Басін А. О. **181**
СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ ПРОЕКТІВ ІТ-КОМПАНІЙ **181**
Белов М. С. **186**
ВОСПРИЯТИЕ УКРАИНСКИХ БРЕНДОВ ПОТРЕБИТЕЛЯМИ С МОМЕНТА НАЧАЛА ПОЛНОМАСШТАБНОЙ ВОЙНЫ В УКРАИНЕ **186**
Бурлака Ю. В. **190**
ВІЙНА ТА ІНШІ КАТАКЛІЗМИ ЯК КЛЮЧОВИЙ ФАКТОР МОТИВАЦІЇ ДЛЯ КОМАНДИ І РОЗВИТКУ ДЛЯ ПРОДУКТУ ТА БІЗНЕСУ **190**
Ващенко С. А. **194**
ВЛИЯНИЯ ТЕХНОЛОГИЙ НА СТРУКТУРУ И ОРГАНИЗАЦИЮ РАБОЧЕГО ПРОЦЕССА В ІТ-КОМПАНИЯХ **194**
Горенко С. Н. **198**
МЕНЕДЖМЕНТ МАРКЕТИНГОВОЙ СТРАТЕГИИ ОРГАНИЗАЦИИ: ОТ ТЕОРИИ К ПРАКТИКЕ **198**
Завгородный А. В. **202**
СРЕДСТВА ПРИВЛЕЧЕНИЯ И МОТИВАЦИИ СОТРУДНИКОВ В СОВРЕМЕННЫХ ІТ КОМПАНИЯХ **202**
Золотаренко А. О. **206**
НЕМАТЕРІАЛЬНА МОТИВАЦІЯ СПІВРОБІТНИКІВ ІТ КОМПАНІЇ **206**
Золотько Д. А. **212**
МАРКЕТИНГОВЫЕ ИССЛЕДОВАНИЯ **212**
Коваленко В. В. **215**
ПРИМЕНЕНИЕ МЕТОДОВ SWOT-АНАЛИЗА, PESTLE-АНАЛИЗА, АНАЛИЗА ПОРТФЕЛЯ ПРОДУКТОВ И АНАЛИЗА КОНКУРЕНТОВ ДЛЯ ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ ІТ-КОМПАНИЙ **215**
Липовяк Є. Ю. **221**
УПРАВЛІННЯ КОМАНДОЮ ТА ЛІДЕРСТВО **221**
Ложко И. В. **224**
ДЕМОТИВАЦИЯ И ЕЁ ВЛИЯНИЕ НА ОТДЕЛ ПРОДАЖ **224**

Лупаненко А. Ю. **226**
ОПЕРАЦИОННЫЙ МЕНЕДЖМЕНТ В СИСТЕМЕ УПРАВЛЕНИЯ ПРЕДПРИЯТИЯ **226**

Лучинський Д. В. **229**
ЕКОНОМІЧНА ТА МЕДИЧНА ЕФЕКТИВНІСТЬ ВПРОВАДЖЕННЯ НОВИХ ОРГАНІЗАЦІЙНИХ ПІДХОДІВ В РОБОТІ ПРИВАТНОЇ СТОМАТОЛОГІЧНОЇ ПРАКТИКИ В РЕАЛІЯХ ВІЙСЬКОВОГО СТАНУ **229**

Наконечний А. Ю. **233**
ЕФЕКТИВНІСТЬ СУЧАСНИХ ІНТЕРНЕТ-МАРКЕТИНГОВИХ ДОСЛІДЖЕНЬ ДЛЯ РОЗВИТКУ ПІДПРИЄМСТВА **233**

Нікітін Д. О. **237**
ЦИФРОВИЙ МАРКЕТИНГ: СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ **237**

Петросюк В. В. **242**
ФОРМУВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ МАРКЕТИНГ-МЕНЕДЖМЕНТ **242**

Рильцов Є. Р. **245**
АНАЛІЗ КОМПЕТЕНЦІЙ МЕНЕДЖЕРІВ ІЗ ПРОДАЖУ У СФЕРІ ПОСЛУГ НАДАННЯ ОНЛАЙН РЕКЛАМИ **245**

Рильцов Р. Є. **250**
МОДЕЛЬ ПРОФЕСІЙНОЇ УСПІШНОСТІ МЕНЕДЖЕРА З ПРОДАЖУ У СФЕРІ ПОСЛУГ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ **250**

Самойленко Н. В. **254**
КРОСС-КУЛЬТУРНАЯ КОМПЕТЕНТНОСТЬ МЕНЕДЖЕРОВ **254**

Сладецький Р. А. **258**
ОРГАНІЗАЦІЯ РОБОТИ КОМАНДИ ДЛЯ СТВОРЕННЯ НОВОГО ІТ ПРОДУКТУ **258**

Топчій О. Д. **262**
ЗАСТОСУВАННЯ СУЧАСНИХ ІНСТРУМЕНТІВ ІНТЕРНЕТ-МАРКЕТИНГУ ДЛЯ ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА НА РИНКУ НЕРУХОМОСТІ **262**

Чернявский В. И. **266**
КАК НАЧАТЬ РАБОТУ С EMAIL МАРКЕТИНГОМ **266**
Mykyta Bobniev **269**
DIGITALISATION OF BUSINESS PROCESSES **269**
Maksym Bondarchuk **272**
BRIEF OVERVIEW OF MANAGEMENT IN ANCIENT ROME LIFE **272**
Vitalii Ivanov **275**
MODERN ASPECTS OF REMOTE MANAGEMENT OF A SOFTWARE DEVELOPMENT TEAM **275**
Artem Kozlov **279**
PECULIARITIES OF TEAMWORK **279**
Artem Loktionov **282**
THE USE OF AI-POWERED TOOLS FOR ENHANCING DAY-TO-DAY BUSINESS OPERATIONS: BENEFITS AND RISKS **282**
Andrii Nikolin **286**
COMPARING PROJECT MANAGEMENT METHODOLOGIES IN SOFTWARE DEVELOPMENT **286**
Yevhenii Tyrsyna **289**
MODERN THEORETICAL ASPECTS AND THE MECHANISM OF FORMATION OF THE PERSONNEL MANAGEMENT SYSTEM OF A TRADING ENTERPRISE **289**
Anton Voronko **294**
COMBINED ITERATIVE APPROACHE FOR STRATEGIC INITIATIVES' IMPLEMENTATION **294**

УПРАВЛІННЯ ПЕРСОНАЛОМ

Білодід В. В. **297**
СУЧАСНІ МЕТОДИ МОТИВАЦІЇ ПЕРСОНАЛУ НА ПІДПРИЄМСТВАХ І ВИРОБНИЦТВІ **297**
Бобылев А. В. **301**
ОЦЕНКА ПЕРСОНАЛА ТОРГОВЫХ КОМПАНИЙ **301**
Мазняк С. А. **304**
КЛАССИФИКАЦИЯ И ВИДЫ ЗАТРАТ РАБОЧЕГО ВРЕМЕНИ ОРГАНИЗАЦИИ В СИСТЕМЕ ПЛАНИРОВАНИЯ **304**

Новіков К. С. 307
УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ПЕРСОНАЛОМ ОРГАНІЗАЦІЙ УКРАЇНИ 307
Онишко В. О. 311
ЗМІНИ РОЛІ УПРАВЛІННЯ ПЕРСОНАЛОМ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ 311
Ретізник А. В. 315
СУЧАСНІ МЕТОДИ УПРАВЛІННЯ ПЕРСОНАЛОМ 315
Салиенко А. А. 319
ЛОЯЛЬНОСТЬ ПЕРСОНАЛА IT КОМПАНИЙ 319
Топчий А. Ю. 322
ОРГАНИЗАЦИЯ БИЗНЕСА И УПРАВЛЕНИЕ ПЕРСОНАЛОМ В УСЛОВИЯХ ВОЙНЫ 322
Чорний С. С. 324
КАДРОВЕ ПЛАНУВАННЯ 324
Stanislav Fedorenko 328
ANALYSYS OF TEAM AND WORK GROUP CHARACTERISTICS IN SOFTWARE DEVELOPMENT TO BUILD EFECTIVE TEAM 328

Scientific publication

SCIENTIFIC ACHIEVEMENTS OF MODERN SOCIETY

COLLECTION OF ABSTRACTS
International scientific-practical conference
(Kunovice, Czech Republic, March 17-18, 2023)

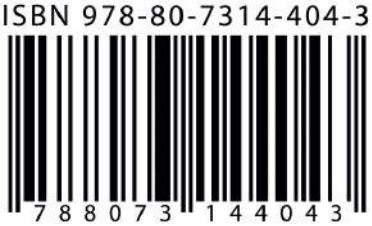
НАУКОВІ ДОСЯГНЕННЯ СУЧАСНОГО СУСПІЛЬСТВА

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ
Міжнародна науково-практична конференція
(Куновіце, Чеська Республіка, 17-18 березня 2023 року)

Under the editorship of I. Kopotun, S. Petkov, P. Polián

Signed for printing 03.04.2023
Press: Tiskárna Grafema, s.r.o., Hranice, Česká republika

Дизайн обкладинки: Кандиба Т. П.
Технічний керівник Кандиба Ю. А.

Підписано до друку 03.04.2023
Видавець і виготовлювач «ФОП Кандиба Т. П.»
Вул. Незалежності, 16, м. Бровари, 07400
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів идавничої продукції ДК № 5263 від 20.12.2016.
Тел.: 067 231-02-86

ISBN 978-80-7314-404-3