УДК 330.47:06.35

Т. В. Капелюшна,
к. е. н., доцент, доцент кафедри управління інформаційною та кібернетичною безпекою,
Державний університет телекомунікацій
ORCID ID: https://orcid.org/0000-0001-7490-6751

DOI: 10.32702/2306-6814.2023.8.125

ВРАХУВАННЯ ВПЛИВУ ЗАГРОЗ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ПРИ УПРАВЛІННІ БЕЗПЕКОЮ ПІДПРИЄМСТВА

T. Kapeliushna,
PhD in Economics, Associate Professor, Associate Professor of the Department
of Information and Cyber Security Management, State University of Telecommunications

CONSIDERING THE IMPACT OF SOCIAL ENGINEERING THREATS IN ENTERPRISE SECURITY MANAGEMENT

У статті розглянуто питання безпеки функціонування підприємства з урахуванням загроз, що спричиняються дією зловмисників на персонал та оточуюче середовище. Відзначено, що безпека підприємства досягається шляхом комплексного та системного вивчення її складових, тобто має забезпечуватися в цілому, за всіма можливими напрямками, якщо узагальнити: економічної безпеки, матеріальної (фізичної) безпеки, інформаційної безпеки. Закцентовано увагу на тому, що з діджиталізацією суспільства, яка пришвидшується з урахуванням умов невизначеності (в яких суспільство перебуває останні три роки) доцільно належну увагу приділяти інформаційній складовій безпеки підприємства.

Описано конкретні об'єкти, що підлягають захисту в підприємстві від можливих загроз, протиправних посягань. Наголошено на двонаправленість атак по відношенню до безпеки підприємства, а саме: техніко-технологічної та соціальної, під дією яких виникає досконала стійка загроза (Advanced Persistent Threat). Підкреслено важливість вивчення дії людського фактора та моніторингу й аналізу діяльності користувачів, оскільки маніпулювання вразливостями людини (слабкості, потреби, манії (пристрасті), захоплення) призводить до нової моделі її поведінки, створення сприятливих умов реалізації загроз безпеці інформації. Схематично представлено, яким чином досягається зловмисниками доступ до інформації за соціоінженерним підходом. Охарактеризовано підсистеми системи управління інформаційними ризиками підприємства з урахуванням можливих атак соціального інженера.

Відзначено, що врахування впливу інформаційних атак на персонал забезпечить посилення безпеки функціонування підприємства та усуне фінансові втрати від атак, які можуть порушити достовірність, цілісність інформації та фінансово-економічних даних.

The article considers the issue of security of enterprise functioning, taking into account the threats caused by the action of intruders on personnel and the environment. It is noted that the security of the enterprise is achieved through a comprehensive and systematic study of its components, that is, it should be ensured in general, in all possible directions, if we generalize: economic security, material (physical) security, information security. It is emphasized that with the digitalization of society, which is accelerating, taking into account the conditions of uncertainty (in which society has been in the last three years), it is advisable to pay due attention to the information component of enterprise security.

The specific objects to be protected in the enterprise from possible threats and illegal encroachments are described. The bidirectionality of attacks in relation to the security of the enterprise, namely: technical and technological and social, under the influence of which there is a perfect persistent threat (Advanced Persistent Threat), is emphasized. The importance of studying the human factor and monitoring and analyzing the activities of users is emphasized, since the manipulation of human vulnerabilities (weaknesses, needs, mania (passion), hobbies) leads to a new model of his behavior, creating favorable conditions for the implementation of threats to information security. It is schematically presented how attackers gain access to information using the socio-engineering approach. The subsystems of the enterprise information risk management system are characterized, taking into account possible social engineer attacks.

It is noted that the current conditions that have emerged (formerly pandemic, now - martial law, acting in the country) lead to an increase in the number of people who every day more and more uses information and telecommunications technology, software and in parallel there is a spread of social engineering incidents, implemented precisely through modern means of telecommunications. It was analyzed that according to the statistical data the human factor is the main reason of successful cyber attacks (91 % of the hackings are the result of phishing - mass mailing of e-mails to a big group of recipients, luring the trusty or careless staff out of the personal data of computer system). Based on the statistical data provided by ENISA, phishing accounts for the largest share of all categories in the overall structure of cybercrime incidents.

It is noted that taking into account the impact of information attacks on personnel will ensure the strengthening of the security of the enterprise and eliminate financial losses from attacks that can violate the reliability, integrity of information and financial and economic data.

Ключові слова: безпека підприємства, економічна безпека, досконала стійка загроза, соціальна інженерія, загрози інформаційній безпеці, управління інформаційними ризиками, інформаційні атаки на персонал, досконала стійка загроза.

Key words: enterprise security, economic security, advanced persistent threat, social engineering, information security threats, information risk management, information attacks on personnel, advanced persistent threat.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

В умовах невизначеності, що складаються останнім часом, підвищується інтерес до посилення безпеки функціонуючих підприємств. Зовнішні втручання, що порушували роботу серверів призвели до того, що більшість інформації зазнала впливу загроз цілісності, підлягала викривленню, що негативно вплинуло на роботу та результати діяльності підприємств. Безпека розглядається в глобальному вимірі, не заточується лише на одному із її елементів, нині передбачається дослідження всіх можливих складових безпеки та їх взаємовпливу.

У теперішніх умовах з кожним роком все більш нагальною стає проблема забезпечення безпечного функціонування підприємств. Нині господарюючі суб'єкти наражаються на небезпеку через загрози, що виникають під час кібератак і віртуального тероризму.

Безпечне функціонування підприємства формує його імідж, впливає на конкурентоспроможність, дозволяє отримувати заплановані результати діяльності, розвиватися та посилювати свої позиції на ринку.

Прослідковується, що безпека підприємства досягається шляхом комплексного та системного вивчення її складових, тобто має забезпечуватися в цілому, за всіма можливими напрямками, якщо узагальнити: економічної безпеки, матеріальної (фізичної) безпеки, інформаційної безпеки. З інформатизацією та цифровізацією суспільства, невизначеністю умов та масованих інформаційних атак, які відбуваються останнім часом, все більшу роль відіграє інформаційна складова.

Питанням безпеки підприємств, захисту інформації від навмисних дій зловмисників, що загрожують її цілісності, достовірності, конфіденційності з використанням для цього персоналу та оточуючого середовища присвятили увагу у своїх працях науковці: Васильєв А.В. [2], Євсеєв С.П. [1], Нам'ясенко В.М. [6], Яковенко В.С., Казеян Н.К. [8], Половенко Л.П., Мерінова С.В. [7], Яковів І.В. [9], Легомінова С. В., Мужанова Т. М., Якименко Ю. М [5]. Так, науковець Васильєв А.В. [2] більше десяти років тому у своїй праці закцентував увагу на важ-

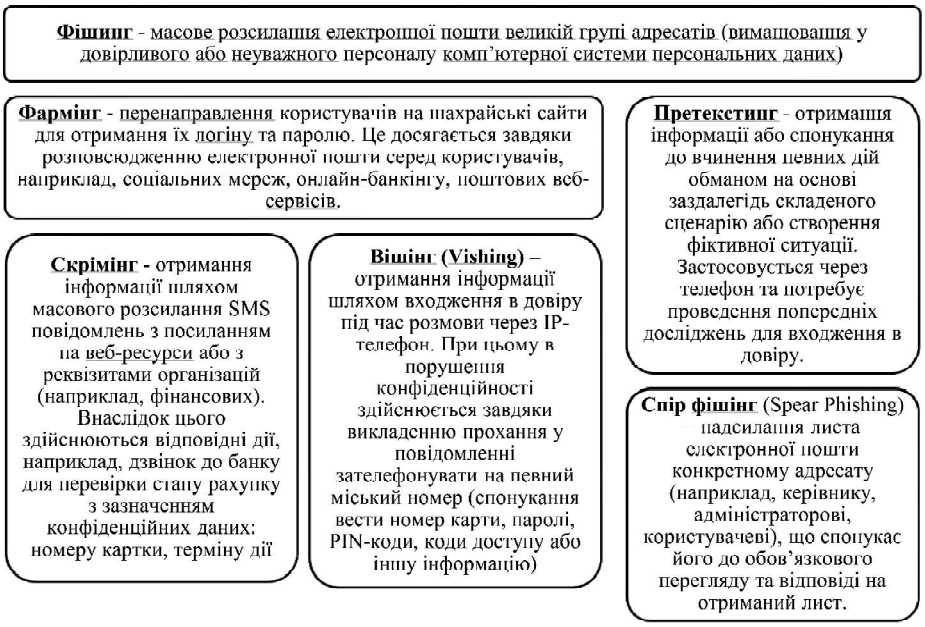

Рис. 1. Найбільш вживані інструменти в соціальній інженерії

Джерело: систематизовано та представлено за даними [1; 4].

ливості соціальної інженерії при створенні політики безпеки захисту інформаційних потоків від несанкціонованого доступу, при чому захист від соціальної інженерії, на думку науковця, можна було забезпечити без знань та розумінь працівниками дій з боку соціального інженера. Проте, важко погодитися із таким твердженням, оскільки соціальний інженер використовує психологічні прийоми для того, щоб об'єкт атаки став вразливим.

У своїй праці Євсеєв С.П. [1], розглядаючи питання забезпечення безпеки не тільки критичних транзакцій та банківських операцій, але і захисту всього комплексу банківської інформації згадує про соціальну інженерію, формуючи взаємозв'язок між бізнес-продуктами з типовими джерелами загроз, виокремлюючи людські джерела загроз (серед них у двох блоках згадується соціальна інженерія), але продовжує розгляд захисту суто з технічної сторони. Нам'ясенко В.М. [6] у роботі наводить основні принципи та ознаки, методи соціальної інженерії, а також пояснює відсутність ефективних бар'єрів захисту з подальшими пропозиціями інструментів захисту, знову ж таки вилучаючи людський аспект, подібними є результати досліджень Яковенко В.С., Казеян Н.К. [2], Половенко Л.П. та Мерінова С. В. [7] запропонували у своєму доробку дієві механізми, що дають змогу оперативно відслідковувати та виявляти ознаки соціальної інженерії на ранніх стадіях, попереджати кіберзагрози на підприємстві та протидіяти соціальному хакерству, наближаючи тим самим пропоновану у даній статті думку щодо важливості врахування людського фактору в забезпеченні безпеки функціонування підприємства.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Проаналізувати загрозу безпеці підприємства соціальної інженерії, обгрунтувати важливість її врахування в кризових станах, масованих інформаційних атаках задля безпечного функціонування підприємств.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

За нормативно-правовими документами, які визначають організацію діяльності, зокрема служби безпеки підприємств, виокремлюють конкретні об'єкти, що підлягають захисту від можливих загроз, протиправних посягань, а саме:

— персонал, який володіє інформацією, що є комерційною таємницею;

— активи, матеріальні цінності та фінансові кошти (будівлі, устаткування, споруди, обладнання, транспорт, валюта, фінансові документи, звіти);

— інформаційні ресурси з обмеженим доступом;

— засоби та системи комп'ютеризації діяльності підприємства;

— технічні засоби та системи охорони й захисту матеріальних та інформаційних ресурсів.

Стандарт ISO27000:2018 вказує: інформаційний ризик — це потенційна можливість того, що загроза буде використовувати уразливість активу або групи активів, завдаючи шкоди організації.

Ризик викликає інцидент інформаційної безпеки — одну або серію небажаних або несподіваних подій інформаційної безпеки, що мають значну ймовірність порушення бізнес-операцій або становлять загрозу для інформаційної безпеки [11].

На сьогодні соціальна інженерія реалізується, як правило, віддалено засобами сучасних телекомунікацій шляхом використання інтернету та телефону (найчастіше використовуються інструменти соціальної інженерії, представлені на рис. 1), рідше — особистий контакт, оскільки важче вводити людину в оману безпосередньо спілкуючись із нею.

Слід зазначити, що у переліку категорій кіберінцидентів (розроблений з використанням та відповідає рекомендації ENISA Reference Incident Classification Taxonomy (Європейської агенції з кібербезпеки)), документу Common Taxonomy for

Рис. 2. Доступ до інформації за соціоінженерним підходом

Джерело: систематизовано та представлено за даними [3; 4].

Law Enforcement and The National Network of CSIRTs та Європейського центру боротьби з кіберзлочинністю Європолу) знаходимо серед інцидентів "шахрайство" — фішинг, який відноситься до інструментів соціальної інженерії, що підтверджує частоту атак даного виду [10].

Нині ініціюються атаки в підприємствах у трьох напрямках через: мережеві пристрої, веб-ресурси та людей. Такі атаки є найбільш ефективними, оскільки охоплюють вразливості техніко-технологічні й соціальні, їх двонаправленість дозволяє досягти максимальний ефект від їх реалізації. До таких атак відноситься Advanced Persistent Threat (APT) — досконала стійка загроза, яка характеризується сукупністю дій зловмисника, за якими вибудувано ланцюг, що формує його стратегію та тактику, щоб досягти порушення цілісності, конфіденційності, захищеності інформації. Але таким атакам притаманний сценарій за якого, дії зловмисників є поступовими, розтягнутими у часі, що дозволяє їм бути непоміченими. Зазначається, що характерним для APT є складний набір взаємозв'язаних за часом і простором дій зловмисника, самі дії можуть не викликати підозр, оскільки підготовка до таргетованої атаки об'єкта-жертви може тривати від декількох місяців до більше року [9].

При чому засоби досягнення використовуються різні, а сама тактика (або їх набір) залишається незмінною. Тому захист має грунтуватися на виявленні атак, що спрямовуються на технології, а також персонал, який має чітко розумітися на питаннях соціальної інженерії та вміти вчасно розпізнавати соціального інженера, який використовує людські слабкості для швидкого отримання необхідної інформації. Лише за ініціації та постановки сценарію поведінки соціального інженера можна упередити персонал від цієї загрози та сформувати його стійкість до дій з боку зловмисника.

Існує думка, що зростаючий вплив людського чинника на стан захищеності інформаційних систем та ресурсів організації призводять до того, що підприємства мають активно запобігати та протидіяти загрозам інформаційній безпеці з вини персоналу. Використання традиційних засобів захисту таких, як антивіруси, міжмережеві екрани, системи запобігання вторгненням не забезпечують цілковитий захист від внутрішніх порушників, що обумовлює необхідність застосування комбінованих та системних інструментів контролю діяльності користувачів [3]. Слід підкреслити важливість вивчення дії людського фактора та моніторингу й аналізу діяльності користувачів, оскільки маніпулювання вразливостями людини (слабкості, потреби, манії (пристрасті), захоплення) призводить до нової моделі її поведінки, створення сприятливих умов реалізації загроз безпеці інформації і, як наслідок, зменшенню здатності систем захисту інформації протидіяти їх впливові. Саме тому, загроза використання соціальної інженерії є однією з найбільш небезпечних у кіберпросторі та у цілому для підприємств.

Загроза — соціальна інженерія полягає у маніпулятивному впливові на свідомість (підсвідомість) людини через властиві їй уразливості (довірливість, страх, жадібність, відкритість, зверхність, милосердя). Нині, у соціальних мережах легко отримати інформацію про вподобання, роботу, захоплення, цілі та прагнення людини, тому персонал стає вразливим до дій соціального інженера, який чинить атаку. Доступ до інформації за соціоінженерним підходом представлено на рис. 2.

Основою використання методів соціальної інженерії є:

— особливості, що керують людською свідомістю;

— аудиторія або поле діяльності;

— некомпетентність аудиторії у визначених термінах і предметних областях у сфері інформаційної безпеки;

— нестійкість психологічних властивостей особистості, що характеризуються поведінковими стереотипами. Їх можна використовувати для маніпулювання через основні потреби, слабкості, бажання, ідеали.

Підсистема захисту інформації (рис. 3) передбачає виявлення інформації, що підлягає захисту, визначення місць зосередження та носіїв інформації, яка підлягає захисту, визначення можливих способів несанкціо-

Рис. 3. Підсистеми системи управління інформаційними ризиками підприємства з урахуваннням атак соціального інженера

Джерело: систематизовано та представлено за даними [3; 4].

нованого доступу до такої інформації, розроблення й упровадження організаційних, правових, технічних, програмних, криптографічних та апаратних засобів захисту інформації.

Функціями цієї підсистеми є:

— формування комплексу організаційних, технічних, апаратних, криптографічних заходів і забезпечення гарантованого захисту від посягань на електронну інформацію підприємства;

— забезпечення контролю за носіями інформації, своєчасне реагування на всі порушення в захисті інформації, що зберігається та функціонує в інформаційних мережах підприємства;

— запровадження надійної системи документообігу в підприємстві;

— забезпечення надійної охорони підприємств, особливо з точки зору виключення можливості несанкціонованого доступу до них та викрадення документів чи електронних носіїв інформації.

Особливого поширення набула соціоінженерна атака за рахунок активного використання телекомунікацій, віддалена соціальна інженерія реалізується саме через сучасні засоби телекомунікацій. При цьому, за статистичними даними, основною причиною успішності кібератак є саме людський фактор, адже 91% зломів здійснюються в результаті вдалого фішингу [9] (масове розсилання електронної пошти великій групі адресатів, виманювання у довірливого або неуважного персоналу комп'ютерної системи персональних даних). Саме фішинг, як зазначалося вище, внесений до переліку категорій кіберінцидентів, який розроблений з використанням рекомендацій ENISA Reference Incident Classification Taxonomy (Європейської агенції з кібербезпеки) [10], що підтверджує його вагу у структурі інцидентів загроз безпеці даних та інформаційним ресурсам з використанням як техічних засобів, так і впливу на працівника, який має доступ до інформації.

Проведений аналіз останніх досліджень та подій, що нині відбуваються та чинять вплив на функціонування підприємств, а також моніторинг загроз соціальної інженерії щодо безпеки підприємств, надав підстав для обгрунтування важливості врахування, в сучасних умовах та кризових явищах, масованих інформаційних атаках, даних загроз як невід'ємної складової задля безпечного функціонування підприємств.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Загроза порушення цілісності інформації, втрата її конфіденційності для підприємств особливо зростає в часи криз: економічних, фінансових, або, як сьогодні, воєнного стану. Врахування цього потенційного втручання у роботу підприємства дозволяє упередити потенційні негативні явища, що можуть постати перед підприємством та порушувати його нормальне функціонування та призвести до: кризових явищ, втрат економічних вигід та проявів від загроз поширення інформації, що стосується виробництва, побудови збутової мережі, контрагентів, формування цін та перспективних напрямків розвитку підприємства, актуальних маркетингових досліджень щодо вподобань, розширення асортименту, стратегії розвитку. Саме людський фактор часто стає джерелом витоку інформації через необізнаність, неуважність, низьку інформованість щодо поводження з інформацією та шляхами її отримання зловмисником за допомогою технічних засобів та сконструйованої поведінки.

У результаті аналізу, підтверджується важливість дослідження поведінки персоналу та користувачів, що мають доступ до інформації для можливості їх захисту від зловмисників, які за використання знань про вподобання або слабкості людей, або під дією тиску на них, потрапляють у коло їх довіри, що дозволяє легко отримувати інформацію без застосування складних технічних комбінацій та прийомів, засобів.

Врахування впливу інформаційних атак на персонал забезпечить посилення безпеки функціонування підприємства та усуне фінансові втрати від кіберзагроз, які можуть виникнути у результаті реалізації дій зловмисника, за якими вибудувано ланцюг, що формує його стратегію та тактику, щоб досягти порушення цілісності, конфіденційності, захищеності інформації під час досконалих стійких загроз по відношенню до персоналу.

Література:

1. Yevseiev S. Methodology for information technologies security evaluation for automated banking systems of Ukraine. Ukrainian Scientific Journal of Information Security, 2016, vol. 22, Issue 3, p. 297—309.

2. Васильєв А.В. Загрози і захист від соціальної інженерії. Захист інформації. №2, 2009. С. 19—24.

3. Глушко А.Д. Інформаційна політика в системі забезпечення фінансової безпеки держави. Ефективна економіка, 2022. № 2. — URL: http://www.economy.nayka.com.ua/pdf/2_2022/97.pdf (дата звернення: 04.12.2022).

4. Капелюшна Т.В. Інформаційна складова в управлінні економічною безпекою діяльності підприємства. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 27 жовтня 2022 року). Навчально-науковий інститут захисту інформації, Державний університет телекомунікацій. Київ. С.171—172. — URL: https://dut.edu.ua/uploads/p_2121_20358827.pdf#page=171. (дата звернення: 29.11.2022).

5. Мужанова Т. М., Легомінова С. В., Якименко Ю. М., Мордас І. В. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. Кібербезпека: освіта, наука, техніка. № 1(13), 2021. С. 50—62.

6. Нам'ясенко В. М. Соціальна інженерія як одна із загроз економічній безпеці, що спричиняє негативний вплив на ефективність діяльності підприємства. Економіка та держава. 2016. № 3. С. 90—92.

7. Половенко Л.П, Мерінова С.В Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. Підприємництво та інновації, (10), 2020. С. 183—187.

8. Яковенко В.С., Казеян Н.К. Соціальна інженерія в Інтернет-просторі. Інформаційні технології та моделювання економічних процесів. 2016. Вип. III-IV(63-64). С. 119—126.

9. Яковів І. Кібернетична модель APT атаки. Technology and Security. 2018. №. 6, Вип. 1 (10). С. 46—58.

10. Офіційний сайт "The European Union Agency for Cybersecurity". Reference Incident Classification Taxonomy. — URL: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (дата звернення: 05.11.2022)

11. Офіційний сайт ISO. Стандарт ISO /IEC TR 15446:2017 "Information technology — Security techniques — Guidance for the production of protection profiles and security targets" — URL: https://www.iso.org/standard/68904.html (дата звернення: 27.10.2022)

References:

1. Yevseiev, S. (2016), "Methodology for information technologies security evaluation for automated banking systems of Ukraine", Ukrainian Scientific Journal of Information Security, vol. 22, Issue 3, pp. 297—309.

2. Vasyliev, A (2009), "Threats and protection against social engineering", Zakhyst informatsii, vol. 2, pp.19—24.

3. Hlushko, A. (2022), "Information policy in the system of ensuring financial security of the state", Efektyvna ekonomika, vol. 2, available at: http://www.economy.nayka.com.ua/pdf/2_2022/97.pdf (Accessed 4 Dec 2022).

4. Kapeliushna, T. (2022), "Information component in the management of economic security of the enterprise", Aktualni problemy kiberbezpeky: Materialy Vseukrainskoi naukovo-praktychnoi konferentsii [Actual problems of cyber security: Materials of the All-Ukrainian scientific and practical conference], Kyiv, Ukraine, pp. 171—172, available at: https://dut.edu.ua/uploads/p_2121_20358827.pdf#page=171 (Accessed 29 Nov 2022).

5. Muzhanova, T. And Lehominova, S and Yakymenko Yu. and Mordas I. (2021), "Technologies for monitoring and analysis of user activity in preventing internal threats to information security of the organization", Kiberbezpeka: osvita, nauka, tekhnika, vol. 1 (13), pp. 50—62.

6. Namyasenko, V. (2016), "Social engineering as one of the threats to economic security that causing a negative impact on the efficiency of the enterprise", Ekonomika ta derzhava, vol. 3, pp. 90—92.

7. Polovenko, L., Merinova S. (2019), "Identification of signs of social engineering and technology to counteract social hackers in the enterprise", Pidpryiemnytstvo ta innovatsii, vol. (10), pp. 183—187.

8. Iakovenko, V. and Kazeian, N. (2016), "Social engineering in the Internet space", Informatsiini tekhnolohii ta modeliuvannia ekonomichnykh protsesiv, vol. III-IV(63-64), pp. 119—126.

9. Yakoviv, I. (2018), "Cybernetic model of APT attack", Technology and Security, Vol. 6, Issue 1 (10), pp. 46—58.

10. The Official Website "The European Union Agency for Cybersecurity" (2018), "Reference Incident Classification Taxonomy", available at: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (Accessed 5 Nov 2022).

11. The Official Website ISO (2017), "Standard ISO / IEC TR 15446:2017 "Information technology — Security techniques — Guidance for the production of protection profiles and security targets", available at: https://www.iso.org/standard/68904.html (Accessed 27 Oct 2022).

Стаття надійшла до редакції 09.04.2023 р.