УДК 331.4

Т. В. Обелець,
к. е. н., старший викладач, Національний технічний університет України "Київський політехнічний інститут ім. І.Сікорського"
ORCID ID: https://orcid.org/0000-0002-1553-5150
В. В. Наверська,
студент бакалавр, Національний технічний університет України "Київський політехнічний інститут ім. І.Сікорського"
ORCID ID: https://orcid.org/0000-0001-7531-1119

DOI: 10.32702/2306-6814.2023.5.80

АНАЛІЗ ТРАНСФОРМАЦІЇ СИСТЕМИ УПРАВЛІННЯ ПЕРСОНАЛОМ ПІД ЧАС ВОЄННИХ ДІЙ

T. Obelets,
PhD in Economics, Senior Lecturer, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
V. Naverska,
Student bachelor, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

ANALYSIS OF THE TRANSFORMATION OF THE PERSONNEL MANAGEMENT SYSTEM DURING MILITARY ACTIONS

У статті досліджено сутність категорії "кібербезпека" та види загроз у кібер просторі, що несуть небезпеку для діяльності підприємств. Досліджено загрози DDoS-атак під час воєнних дій на території України, що несуть загрозу паралізації процесів управлінської чи виробничої діяльності підприємства, зашкоджують роботі додатків, шкодять репутації.

В даній статті розглянуто небезпеку фішинг атак та зміни в системі управління персоналом, що пов'язані з ними. Проаналізовано напрямки максимізації рентабельності інвестицій від навчання працівників кібербезпеки.

Водночас досліджено зміни в системах управління персоналом, що зумовлені діджиталізацією процесів на підприємствах. Зокрема розглянуто зміни під впливом впровадження хмарних систем зберігання та роботи з даними, а також реорганізацію підрозділів підприємств з метою підвищення ефективності їх діяльності.

The article examines the essence of the "cyber security" category and the types of threats in cyberspace that pose a danger to the activities of enterprises. The categories of DDoS attacks and targeted attacks were considered and the trend of their number on the territory of Ukraine was determined. The threat of DDoS attacks during military operations on the territory of Ukraine was investigated. It was found that such attacks threaten to paralyze the processes of management or production of enterprises, harm the normal operation of applications, and harm reputation. During the war, DDoS attacks on government, banking, and energy sites and applications played a significant role in disrupting threat response and spreading panic. The article provides an example of the largest DDoS attack in February 2022, which caused the paralysis of banking applications and state systems.

It has been established that the share of targeted attacks on the territory of Ukraine in 2021 reached 19% of global indicators. That makes it necessary to strengthen the cyber security of enterprises.

This article also discusses the dangers of phishing attacks and changes in the personnel management system associated with them. It has been established that phishing attacks are carried out for the purpose of fraud or disclosure of confidential information, which is later used against the enterprise. A separate type of phishing attack related to the targeted reconnaissance of corporate information from company managers was studied. It has been established that whaling phishing is most effective against a careless company manager.

The directions for maximizing the return on investment from the training of cyber security workers have been analyzed. The stages of training employees in cyber security measures have been established.

At the same time, the changes in personnel management systems caused by the digitization of processes at enterprises were investigated. In particular, the changes under the influence of the implementation of cloud storage systems and work with data, as well as the reorganization of enterprise divisions in order to improve the efficiency of their activities, were considered.

Ключові слова: кібербезпека, кібератака, фішинг, управління персоналом, рентабельність інвестицій.
Key words: cyber security, cyber attack, phishing, personnel management, return on investment.

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

Під впливом технологічного розвитку світ не стоїть на місці. Для підвищення ефективності власної діяльності все частіше застосовуються системи автоматизації робочих процесів, що призводить до вивільнення робочих місць на підприємствах і скорочення необхідного штату працівників. Розробка новітніх цифрових та технологічних систем призводить до трансформації на ринку праці, заміщаючи технічні спеціальності шляхом виявлення алгоритмів їх діяльності. Такі зрушення призводять до підвищення продуктивності діяльності підприємств з подальшим зменшенням витрат на оплату праці.

Проте з підвищенням рівня автоматизації процесів та розвитку цифровізації інформації підприємства стикаються не тільки зі сприятливими факторами, а і з загрозами. Логічно сконструйовані системи є вразливими перед більш гнучкими технологіями у кіберпросторі, проте з розвитком технологій існує все менше недоліків у системах захисту інформації.

Разом з цим тенденції на ринку праці вказують на підвищення уваги до розвитку персоналу, особливо спеціалістів, робота яких не має алгоритмів і стосується особистісних, лідерських та творчих здібностей. Витрати на оплату праці таких спеціалістів дедалі зростає. Це доводить, що персонал є найбільш цінним ресурсом підприємств, адже він стає рушійною силою розвитку та життєздатності підприємства, бо для досягнення мети організації працівникам необхідно мати можливість самостійно приймати рішення, винаходити, рішуче діяти, критично оцінювати ситуацію, мати суб'єктивні інтереси, вдосконалюватись та навіть діяти ірраціонально. Водночас персонал стає найбільш уразливою складовою у схемі кіберзлочинів.

Тому розвиток обізнаності персоналу у сфері кібербезпеки є безперечно важливим для підприємств та держави.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

В наукових працях В. С. Павленка [1], О. В. Дикого [2], С.В. Онищенко, А.Д. Глушко[3] висвітлено сутність кібербезпеки та досліджено тенденції кіберзлочинності в Україні.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Мета статті полягає в аналізі рентабельності навчання персоналу протидії загрозам кібератак на підприємствах фінансового сектору під час воєнних дій.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

На тлі повномасштабних воєнних дій на території України, що супроводжуються фізичним та економічним руйнуванням, відбувається економічний занепад та ліквідація багатьох підприємств країни, втрата контролю над підприємствами на окупованих територіях тощо. Така ситуація супроводжується масовою втратою робочих місць, внутрішньою та зовнішньою міграцією. Від початку повномасштабного вторгнення більш ніж 14,5 млн (35,21% від наявного населення) українців залишили країну, з яких 11,7 млн (11,41% від наявного населення) виїхали до Євросоюзу. Разом з цим зафіксовано 4,7 млн внутрішньо-переміщених осіб [4].

За таких тенденцій на ринку праці та в умовах економічної та політичної невизначеності та нестабільності, під час воєнних дій й швидких технологічних зрушень все більш відчутним є впив швидкості та якості обробки та передачі даних та її захищеності.

Рис. 1. Причини інцидентів з кібербезпеки, станом на 2019 рік

Джерело: систематизовано, узагальнено та згруповано за даними [1—3].

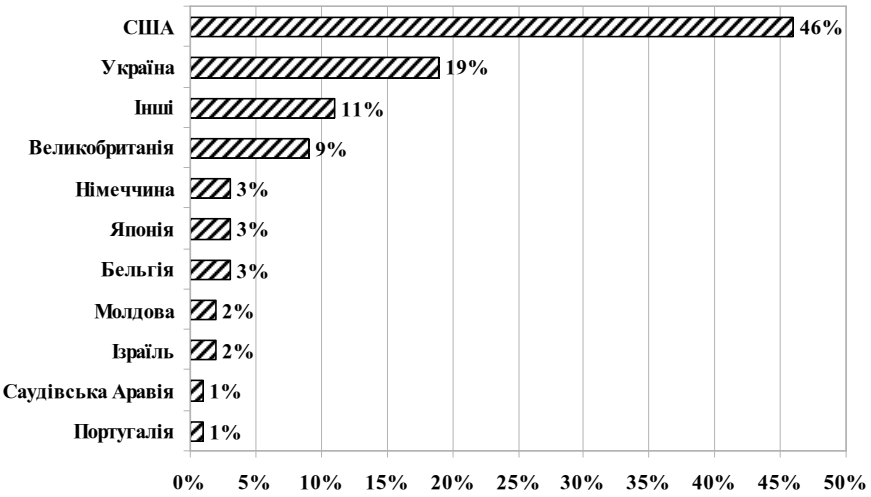

Рис. 2. Показники таргетованих кібератак на підприємства України за 2021 рік

Джерело: [6].

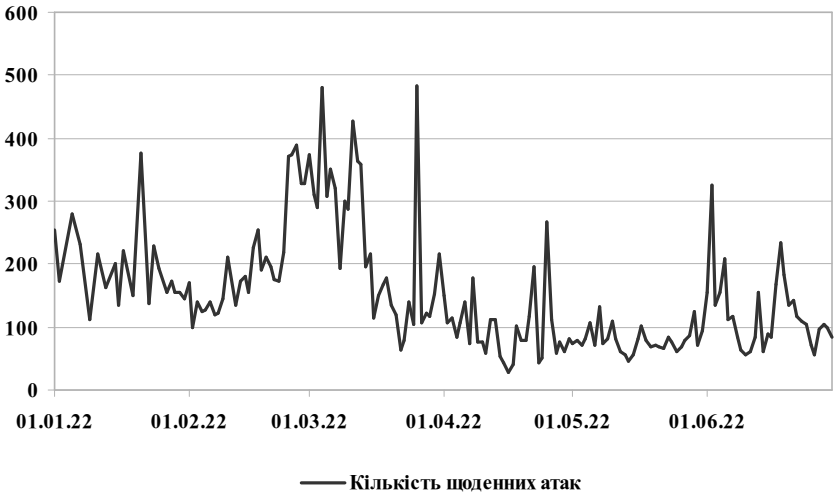

Рис. 3. Щоденні показники кібератак в Україні за 1 півріччя 2022 року

Джерело: [7].

Найбільш вразливими для кібератак є підприємства фінансового та державного секторів. Зі зростанням рівня розвитку диджиталізації та цифровізації процесів яких, все більш вагомою є безпека збереження інформації для таких підприємств.

З огляду на світові тенденції можна зазначити нагальність навчання співробітників навичкам протидії кіберзагрозам.

Категорія "кібербезпека" що є процесом протидії кіберзагрозам являє собою комплекс заходів забезпечення безпеки конфіденційної інформації, збереження її цілісності та доступності.

На даний час все більше набуває обертів кількість кібератак безпосередньо на компанію з метою дискредитації компанії, крадіжки конфіденційних даних, комерційного шпигунства та зараження всієї інфраструктури. При цьому однією з найслабкіших ланок входу, куди найчастіше спрямовані ресурси та намагання нападників — працівники.

На сьогоднішній час компрометація даних та кібератаки — це не питання "якщо", а "коли", що обумовлює необхідність навчання працівників кібербезпеки. Хоча навчання з кібербезпеки безпосередньо не приносить доходу, важливо розраховувати його як вимірюваний показник, і в кінцевому підсумку визначати рентабельність навчання співробітників з кібербезпеки.

З розвитком технологій змінюються засоби скоєння кібератак. Так світові тенденції вказують на зростання інцидентів DDoS-атак. У 2019 році Україна посіла перше місце за кількістю DDoS-атак у світі. Станом на 2021 рік частка кібератак проти підприємств та державних установ України досягла 19% світових показників [5].

З початком воєнних дій простежується тенденція до збільшення кількості кібератак на підприємства у першому кварталі 2022 року. Проте як наведено на рис. 3 у другому кварталі ситуація змінюється і переважають спадні тенденції кількості кібератак. Така ситуація свідчить про підвищення складності та цілеспрямованість атак на діяльність підприємств України.

DDoS-атака — це цілеспрямована атака на комп'ютерні системи підприємства, чи установи з метою повної чи часткової зупинки бізнес-процесів. В результаті такого нападу підприємство несе не тільки фінансові, а і репутаційні збитки; зазнає втрат цілісності та якості контролю над запитами, що призводить до появи критично уразливих місць у системі; піддається повторним атакам та втрачає комерційні таємниці чи дані. DDoS-атака створює величезну кількість зовнішніх запитів у системі взаємодії з користувачами чи споживачами (онлайн-ретейл та маркетплейси, фінансовий сектор, держпослуги, телекомунікація, онлайн-навчання, сервіси доставки, соціальні мережі, месенджери, відеоконференцзв'язок), а атакована система просто не в змозі їх обробити. Як наслідок — виникають збої [8]. DDoS-атаки не несуть прямої загрози, а стають слабкістю для проведення інших атак (цільових кібератак чи вкиду дезінформації). Дезінформаційний вкид несе в собі загрозу при прийнятті корпоративних рішень, створює комерційну плутанину та збої в управлінні, а також сіє сумніви серед співробітників та клієнтів.

Прикладом такої атаки може слугувати напад на державні та банкові додатки такі як "Дія", "Приват24", "Ощадбанк" 15 лютого 2022 року, що паралізувала роботу систем на декілька годин. Користувачі цих додатків виказали занепокоєння за збереження власних даних.

Не меншу загрозу несуть у собі фішинг атаки. Фішинг є методом шахрайства з метою отримання конфіденційних даних. Окрім загрози для пересічних громадян фішинг атаки є надзвичайно небезпечними та руйнівними для малого та середнього бізнесу. Цільовий фішинг на компанію чи працівника відбуваються шляхом підробки довірених контактів або збору особистої інформації про жертву. Існує окремий вид фішигу атак спрямований на вищі ланки керівництва підприємством — китобійний фішинг. За такої атаки злочинці імітують накази генерального директора підприємства, що є вкрай небезпечним для системи управління компанією.

На тлі цього вплив навчання працівників кібербезпеці на рентабельність підприємства стає все більш вагомим.

Для збільшення рентабельності інвестицій у навчання співробітників з кібербезпеки необхідно врахувати:

— Зацікавленість співробітників

Зробити тренування цікавим може не здатися конкретним способом максимізувати рентабельність навчання працівників, але це один з найважливіших факторів. Без зацікавленості співробітників ефективність тренінгів буде мінімальною, тому потрібно вводити певні заохочення за успішне проходження навчання та проводити щоквартальний зріз залишкових знань. Якщо не брати до уваги даний фактор, то прибуток після кібернавчання буде досить низьким, і організація не стане більш безпечною.

Натомість важливо обрати інтерактивну програму навчання, яка охоплює усі класи співробітників. Навчальна програма, яка включає в себе вебінари та віртуальне моделювання, може збільшити капітал. Важливо вкладати гроші в якісну підготовку персоналу і тільки в такому випадку ефективність діяльності підприємства підвищиться.

— Відстеження їхнього прогресу

Під час тренінгу потрібно приділяти потрібну увагу різниці обізнаності в той чи іншій сфері працівників. Відстежуючи прогрес співробітників і розуміючи, у чому полягають їх сильні та слабкі сторони, можна інвестувати більше часу та ресурсів у сфери, які потребують вдосконалення, замість того, що вже є стандартним.

— Здійснення рольового навчання

Незважаючи на те, що в кожному відділі підприємства (не лише IT) існує відповідальність за кіберзахист, не всі співробітники стикаються з однаковими проблемами, пов'язаними з кібербезпекою, тому потрібно враховувати різні підходи до навчання. Співробітники, керівництво, виконавці та технічні відділи відрізняються вимогами до навчання через різну природу їх ролей та чутливості даних, до яких вони мають доступ. Ефективність рольової програми навчання може допомогти вирішити вразливості на всіх фронтах, заощаджуючи час та гроші.

Наприклад, керівники рівня С часто націлюються на компроміси з електронною поштою або кібернапади. Освіта керівників повинна зосередитись на вирішенні проблем, пов'язаних із запобіганням атак, пов'язаних з рівнем їхньої діяльності.

Важливою частиною тренінгів з кібербезпеки є вмінння протидії соціальній інженерії.

Згідно з дослідженнями станом на 2018 рік, майже половина усіх кіберінцидентів великих компаній приходиться на вразливості внутрішньої інфраструктури, тобто виникає саме з вини самих працівників. Оскільки корпоративний кіберзахист, як правило, є більш досконалим, ніж захист приватного користувача, методи нападу часто вимагають активного залучення когось із середини, щоб досягти повного захоплення системи. Однак це не означає, що співробітник свідомо бере участь у нападі. Зазвичай це стосується того, що зловмисник розгортає цілий ряд методів соціальної інженерії, таких як фішинг.

Для того, щоб спочатку оцінити рентабельність навчання співробітників з кібербезпеки, доведеться зважити вартість навчання з вартістю того, щоб взагалі не проводити жодної підготовки. Вартість кіберзлочинності може варіюватися між галузями та розмірами бізнесу, але в цілому середня вартість останнім часом зросла до 13 мільйонів доларів.

Після підрахунку ризику в грошових одиницях повинна враховуватись вартість навчання, а також будь-які додаткові переваги для бізнесу, такі як: збільшення довіри та визнання у галузі діяльності завдяки кіберзахисту.

Нижче наведений приклад являється спрощеним рівнянням рентабельності інвестицій з точки зору навчання працівників кібербезпеки [9]:

$$(SRR-CC)\backslash CC=ROI \quad (1),$$

де: кошти, витрачені на навчання з кібербезпеки — CC (cost of training);

зниження ризику — SRR (saved reducing risk);

рентабельність інвестицій — ROI.

$$SRR=AR*EML*RP \quad (2),$$

де: річна частота, з якою відбувається загроза — AR;

очікувані грошові втрати за одну подію — EML;

зменшення ймовірності виникнення ризику при здійсненні контролю — RP.

Насправді рівняння може бути набагато складнішим, якщо врахувати низку факторів та перерахувати ці показники у грошову одиницю. Слід зазначити, що не всі тренінги є однаковими і якість кожного з них може призвести до значної суми втрачених у майбутньому та теперішньому коштів. Важливо оцінювати навчальні програми, виходячи з унікальних потреб організації і організовувати адаптивну програму виходячи з рівня обізнаності та природою ролей співробітників.

Для прикладу буде наведено розрахунок рентабельності навчання, якщо компанія має вразливість до фішинг атак.

Скажімо, організація розраховує на кількість атак (фішинг) 5 разів на рік, за приблизною вартістю 35000 доларів за успішну атаку. Очікується, що вартість навчання працівників для виявлення та уникнення фішинг-електронних листів становить 25 000 доларів. Ось як виглядатиме рентабельність інвестицій у безпеку:

AR=5

EML=35000$

RP=-85%

CC=25000$

Зниження ризику становить (saved reducing risk):

SRR=5*35000*0.85=148750$

Рентабельність інвестицій становить:

ROI=(148750-25000)\25000$=4.95

Збережені кошти на рік складають:

ROI*CC=4.95*25000$=123750$

У цьому прикладі є сенс вкласти 25000 доларів у навчання, щоб зменшити ризик успішної фішинг-атаки. Потрібно врахувати той факт, що кожна організація різна, і визначення цих змінних буде грунтуватися на обставинах та толерантності до ризику організації. Як і у будь-якому застосуванні засобів контролю країн СНД, вартість впровадження залежатиме від оцінки зменшення ризику та інших місцевих факторів.

Від початку 2022 року, окрім підвищення обізнаності працівників у сфері кібербезпеки, зміни у системах управління торкнулися розвитку рівня діджиталізації систем управління персоналом.

Все більше підприємств України, для покращення систем управління даними та адміністрування, а також для усунення розривів між даними в основній системі управління персоналом компанії та функцією управління документами співробітників, вдаються до впровадження хмарної системи зберігання та передачі даних. Дана зміна не тільки може слугувати засобом протидії кібератакам і захистити корпоративні дані, а і допомагає оптимізувати роботу відділу кадрів й автоматизувати деякі HR-процеси.

Хмарні рішення мають перевагу у роботі відділу бухгалтерії, відділу кадрів, відділу маркетингу і продажів. Під час воєнних дій дане рішення дозводяє працювати представникам наведених відділів більш гнучко та ефективно. При використанні хмарного простору працівник має змогу працювати з даними та документами дистанційно. Водночас автоматизація процесів та централізованість даних дозволяє знизити втрати робочого часу майже на 80%. Перевага впровадження хмарного сховища в умовах нестабільної ситуації під час воєнних дій полягає у можливості відновленням операційних систем й опрацьованих даних навіть у важких випадках та при відключеннях енергії.

Водночас деякі підприємства України, зокрема "ПриватБанк", реорганізували організаційні структури своїх підрозділів. "ПриватБанк" провів реорганізацію своїх IT-департаментів, усуваючи дублювання їх функцій й водночас збільшуючи рівень їх взаємодії. Тобто було ліквідовано ізольовані IT-підрозділи, а штат було перенаправлено до нового департаменту. Така зміна дозволила банку зменшити неефективні витрати робочої сили та спростити управління, водночас збільшивши контроль над діяльністю працівників.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Зміни в системі управління персоналом у 2022 році зумовлені кіберзагрозами з боку злочинців й хакерів рф, нестабільністю ситуації під час воєнних зіткнень на території України та технологічним прогресом.

За результатами аналізу виявлено найбільш небезпечні види кіберзагроз для діяльності підприємств. Досліджено, що тенденція DDoS-атак на веб-ресурси України вказує на вагомий вплив даних кібератак, не тільки у ході воєнних дій, при підготовці нападів на територію України військами рф, а і при навмисному запобіганні нормальної роботи фінансового, державного та енергетичного секторів України. DDoS-атаки створюють уразливі точки для подальших нападів на підприємство, таргетованих атак, фішингових атак тощо.

Задля захисту корпоративних таємниць та конфіденційних даних підприємства України долучилися до підвищення рівня кібербезпеки власних підприємств.

Визначено, що для порівняння результатів річних рішень з кібербезпеки, з однаковим ступенем ризику, підприємствам необхідно прорахувати кожне з них за ROI для зменшення ризику та визначити, що найбільш необхідне задля зменшення рівня ризику конкретного підприємства. Даний показник можна використати для визначення ризиків, які є найвигіднішими для подолання, та які допоможуть визначити пріоритетну оборонну стратегію підприємства. Звичайно, будь-яка стратегія також повинна бути відкалібрована відповідно до операційних та організаційних цілей бізнесу з урахуванням ризику найбільшого значення або контролю, який вважається найважливішим для кібербезпеки. Тим не менш, даний показник виявиться корисним для того, щоб допомогти організації переглянути вартість рішень за технічний контроль.

Неминуче на підприємстві, навіть після навчань, можуть з'явитися прогалини — не лише у процесах безпеки та реалізації, а й у вимірюванні ефективності контролю. Ці прогалини мають бути ідентифіковані та керовані як елементи дій для поліпшення загальної позиції безпеки організації. Визначальним фактором для багатьох організацій є нейтралізація зусиль, пов'язаних з кібербезпекою, що потребує подальших досліджень.

Виявлено зміни у роботі підприємств, в особливості структурі роботи відділів кадрів, адміністрації та бухгалтерії, що стосується впровадження хмарних рішень для зберігання та роботи з даними.

Виявлено зміни в організаційних структурах підприємств. Зокрема скорочення департаментів шляхом усунення дублювання їх функціоналу.

Дані зміни свідчать про розвиток управлінських систем у напрямку диджиталізації процесів пов'язаних з управлінням персоналом та підприємством в цілому.

Література:

1. Павленко В. С. Сутність кібербезпеки у теорії інформаційного права. Право та державне управління. 2021. № 2. С. 28—33. URL: http://pdu-journal.kpu.zp.ua/archive/2_2021/6.pdf

2. Дикий О. В. Кіберзлочинність та кібервійна: сучасні виклики. "Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття" (до 25-річчя Національного університету "Одеська юридична академія" та 175-річчя Одеської школи права). 2022. Т. 2. С. 493—495. URL: https://hdl.handle.net/11300/19926.

3. Онищенко С. В. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Економіка і регіон. 2022. № 1 (84). С. 13—20. URL: https://doi.org/10.26906/EiR.2022.1(84).2540.

4. Біженці з України — від початку війни виїхало понад 14,5 мільйона громадян. Слово і Діло. URL: https://www.slovoidilo.ua/amp/2022/12/01/novyna/polityka/ombudsmen-rozpoviv-skilky-ukrayinczivvyyixalo-kordon-24-lyutoho.

5. Кібербезпека бізнесу в умовах нестабільності. PwC Україна. 2022. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html.

6. Microsoft Digital Defense Report OCTOBER 2021. Microsoft Digital Defense Report. 2021. С. 53. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

7. Europe, Middle East, and Africa. Netscout. 2022. URL: https://www.netscout.com/threatreport/emea/.

8. Що таке DDoS-атака?. Державна служба звязку та захисту інформації України. URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka.

9. Робледа П. Як розрахувати рентабельність інвестиційної ініціативи BPM? Medium. 2017. URL: https://medium.com/@pedrorobledobpm/how-to-calculate-the-roi-of-a-bpm-initiative-43cf25f35287

References:

1. Pavlenko, V. S. (2021), "The essence of cyber security in the theory of information law", Pravo ta derzhavne upravlinnia, vol. 2, pp. 28—33, available at: http://pdu-journal.kpu.zp.ua/archive/2_2021/6.pdf (Accessed 5 Feb 2023).

2. Dykiy, O. V. (2022), "Cybercrime and cyber warfare: modern challenges", "Yevropejs'kyj vybir Ukrainy, rozvytok nauky ta natsional'na bezpeka v realiiakh masshtabnoi vijs'kovoi ahresii ta hlobal'nykh vyklykiv XXI stolittia" (do 25-richchia Natsional'noho universytetu "Odes'ka iurydychna akademiia" ta 175-richchia Odes'koi shkoly prava) ["The European choice of Ukraine, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century" (to the 25th anniversary of the National University "Odesa Law Academy" and the 175th anniversary of the Odessa School of Law], vol. 2, pp. 493—495, available at: https://hdl.handle.net/11300/19926 (Accessed 5 Feb 2023).

3. Onyshchenko, S.V. (2022), "Analytical measurement of cyber security of Ukraine in the conditions of growing challenges and threats", Ekonomika i rehion, vol. 1 (84), pp. 13—20.

4. Slovo i Dilo (2022), "Refugees from Ukraine — more than 14.5 million citizens have left since the beginning of the war", [Online], available at: https://www.slovoidilo.ua/amp/2022/12/01/novyna/polityka/ombudsmen-rozpoviv-skilky-ukrayinczivvyyixalo-kordon-24-lyutoho (Accessed 5 Feb 2023).

5. PwC Ukraine (2022), "Cyber security of business in conditions of instability", [Online], available at: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html (Accessed 7 Feb 2023).

6. Microsoft (2021), "Microsoft Digital Defense Report OCTOBER 2021", [Online], available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi (Accessed 7 Feb 2023).

7. Netscout (2022), "Europe, Middle East, and Africa", [Online], available at: https://www.netscout.com/threatreport/emea/ (Accessed 7 Feb 2023).

8. State Service of Special Communications and Information Protection of Ukraine (2022), "What is a DDoS attack?", [Online], available at: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka (Accessed 7 Feb 2023).

8. Robledo, P. (2017), "How to calculate the return on investment of a BPM initiative?", Medium, [Online], available at: https://medium.com/@pedrorobledobpm/how-to-calculate-the-roi-of-a-bpm-initiative-43cf25f35287 (Accessed 8 Feb 2023).

Стаття надійшла до редакції 13.02.2023 р.