КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

УДК 004.7.056.5:616-036.21
JEL Classification: M20, M21, M59, C80 DOI: https://doi.org/10.31617/tr.knute.2021(37)03

Юлія БІЛЯВСЬКА к. е. н., доцент, доцент кафедри менеджменту Київського національного торговельно-економічного університету вул. Кіото, 19, м. Київ, 02156, Україна
E-mail: y.biliavska@knute.edu.ua
ORCID: 0000-0002-8183-4036

Неля МИКИТЕНКО к. е. н., доцент, доцент кафедри менеджменту Київського національного торговельно-економічного університету вул. Кіото, 19, м. Київ, 02156, Україна
E-mail: n.mykytenko@knute.edu.ua
ORCID: 0000-0002-5694-0531

Ярослав ШЕСТАК директор Інформаційно-обчислювального центру Головного центру інформаційних технологій, ст. викладач кафедри програмної інженерії та кібербезпеки Київського національного торговельно-економічного університету вул. Кіото, 19, м. Київ, 02156, Україна
E-mail: shestack@knute.edu.ua
ORCID: 0000-0002-5102-9642

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ ПІД ЧАС ПАНДЕМІЇ *COVID-19*

Зроблено огляд світових тенденцій кіберзлочинності, а також її географії та світових брендів, що зазнали найбільших збитків від неї. Досліджено структуру злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку. Сформовано "портрет" сучасного кіберзлочинця. Узагальнено категорії жертв та типи кібератак в Україні, що спричинені пандемією COVID-19. Проведено й опрацьовано результати онлайн-опитування щодо впливу COVID-19 на кібербезпеку підприємства. Сформовано модель й обґрунтовано рекомендації з дотримання кібербезпеки підприємства в умовах COVID-реальності.

Ключові слова: кібербезпека, кібератака, кіберризик, кіберзлочинець, пандемія *COVID-19*, *COVID*-реальність, токен, фішинг.

Постановка проблеми. Диджиталізація, роботизація, інтелектуальна економіка спонукають світ переходити на новий рівень життєдіяльності, коли керівними чинниками виробництва стають інновації та творчі досягнення людей. Суспільство увійшло в еру інновацій, де промислові роботи, 3*D*-друк, хмарні джерела інформації, 4*G*- та 5*G*-зв'язок, геноміка, *VR*-технології, розумні міста стають звичайною річчю. Проте, не зважаючи на умови масштабної глобалізації та стрімкого розвитку індустрії 4.0, пандемія *COVID-19* змінює буденне життя: населення відчуває стурбованість і занепокоєння, що актуалізує необ-

хідність отримання допомоги та підтримки, відчуття безпеки та прагнення до визначеності. Водночас організовані злочинні групи спекулюють на невпевненості, страхах і сумнівах, пов'язаних з *COVID-19*, роблячи деяких людей та підприємства вразливими до їхнього втручання.

Внаслідок пандемії коронавірусу значна частина персоналу підприємств переведена на режим дистанційної роботи, тому має бути обізнаною щодо ризиків, пов'язаних з нею, а саме з незахищеним віддаленим підключенням до установи; поширенням використання офісної техніки в особистих цілях; атаками на акаунти в соціальних мережах; спробами фішингових атак, які експлуатують тематику *COVID-19*; шахрайством та незахищеністю інформаційних даних різного генезису.

Аналіз останніх досліджень і публікацій. Питанням кібербезпеки нашої країни та формуванню механізму міжнародної приділяли увагу численні науковці. Так, Д. С. Безуглий обґрунтував необхідність інформаційної безпеки як складової частини національної безпеки країни. Крім того, проблеми інформаційної безпеки у той чи інший спосіб досліджувались у наукових працях А. І. Марущака [2], М. В. Гуцалюка [3]. Питанню формування ефективного механізму правового регулювання протидії загрозам у кібернетичній сфері присвячено праці Д. В. Дубова [9], В. В. Куцаєва, А. В. Печенюка [10]. Проте зазначені дослідження здебільшого зосереджені на теоретичних аспектах інформаційної безпеки. Втім занепокоєння масштабами та впливом пандемії *COVID-19* змушує підприємства аналізувати свої реакції та розробляти заходи, яких потрібно вжити для захисту інформації.

Метою дослідження є визначення тенденцій поширення кіберзлочинів під час пандемії *COVID-19* та обґрунтування рекомендацій з дотримання кібербезпеки підприємства в умовах *COVID*-реальності.

Матеріали та методи. У процесі дослідження використано комплекс загальнонаукових і спеціальних методів: аналітичних, історичних та логічних узагальнень – для уточнення понятійного апарату і визначення ключових ознак окремих дефініцій, аналізу підходів до визначення сутності й особливостей управління кібербезпекою; економіко-статистичних методів (вибіркового спостереження, порівняльного та техніко-економічного аналізу, групування на основі використання програмних продуктів *MS Excel*) з метою візуального представлення результатів досліджень; маркетингових і соціологічних досліджень (опитування), а також експертних оцінок – для оцінювання ефективності результатів кібербезпеки.

Результати дослідження. З кожним роком підприємства все більше долучаються до сучасного інформаційного простору, імплементуючи диджитал-інструменти, як-от: *CRM*-системи, *ERP*-системи, *CAD*-системи та системи з *WEB*-доступом. Інноваційні технології допомагають підприємствам бути на зв'язку зі своїми клієнтами в режимі 24/7, оптимізувати свої бізнес-процеси, вивільнити час від оперативних завдань на користь стратегічних та більш креативних. Водночас цифрова ера готує й низку випробувань для систем захисту інформації та кібербезпеки сучасних підприємств.

За українським законодавством, *кібербезпека* являє собою захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [1]. Під час пандемії *COVID-19* майже в усьому світі кібербезпека опинилася під загрозою: підприємства відчувають постійне посилення цільових атак, які стають більш витонченими та прихованими, часто з елементами фінансової мотивації.

Серйозне занепокоєння викликає використання та розповсюдження програм-вірусів, фішингових програм, спаму, поширення фактів несанкціонованого доступу до державних інформаційних ресурсів, викрадення інформації з баз даних, знищення та модифікація даних в інформаційних системах, перехоплення інформації [2].

Практично всі фахівці визнають, що ситуація з кіберзлочинністю у світі має тенденцію до погіршення, зокрема, зазначається посилення організованості злочинної діяльності. Серед причин посилення організованості кіберзлочинності, наприклад, у мережі Інтернет, можна вважати те, що така діяльність стає більш вигідною, ніж інші способи незаконного збагачення [3, с. 199].

Щодня групи досвідчених кіберзлочинців захоплюють контроль над чужим хмарним середовищем, серверами, комп'ютерами та мобільними гаджетами, запускаючи серію руйнівних програм проти певних сайтів. Шляхом враження серверів та клієнтських комп'ютерів організовуються потужні атаки, в результаті яких за лічені секунди припиняють функціонування банкомати, телефонні лінії, цілі компанії та навіть президентські сайти світових держав. У різних країнах дедалі більше уваги приділяється кібербезпеці й керуванню інформаційними ресурсами. На *рис. 1* представлено світову тенденцію кіберзлочинів упродовж останніх 5 років.

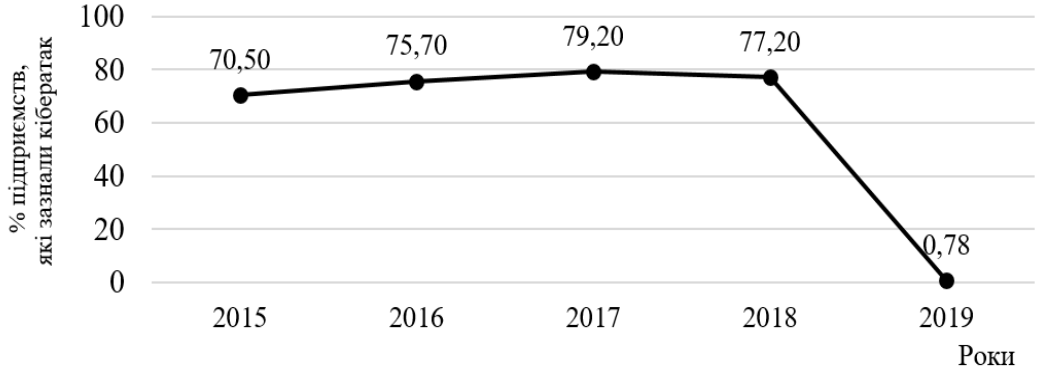

Рис. 1. Світова динаміка кіберзлочинів за 2015–2019 рр.

Джерело: узагальнено на основі звітів з інформаційної безпеки Мережевої академії *Cisco* [4].

У 2020 р. на тлі пандемії коронавірусу поліцейська служба ЄС зафіксувала активізацію кібернападів, шахрайств, крадіжок та підроблення товарів. З погляду географії кібератак їх лідером є США, друге місце посідають Нідерланди, третє – Німеччина *(рис. 2)*.

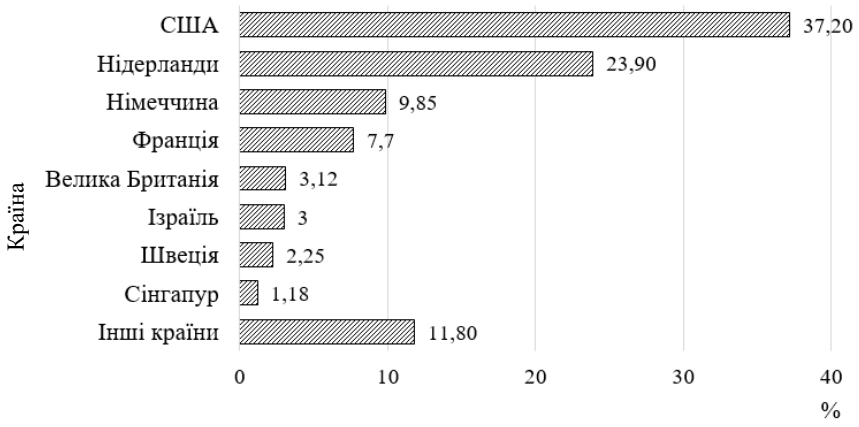

Рис. 2. Географія кібератак у світі у 2020 р.

Джерело: узагальнено на основі звітів з інформаційної безпеки Мережевої академії *Cisco* [4].

Якщо розглядати світові бренди, які зазнали найбільших збитків від кібератак, то особливо слід виділити *Microsoft* і *Amazon (рис. 3).*

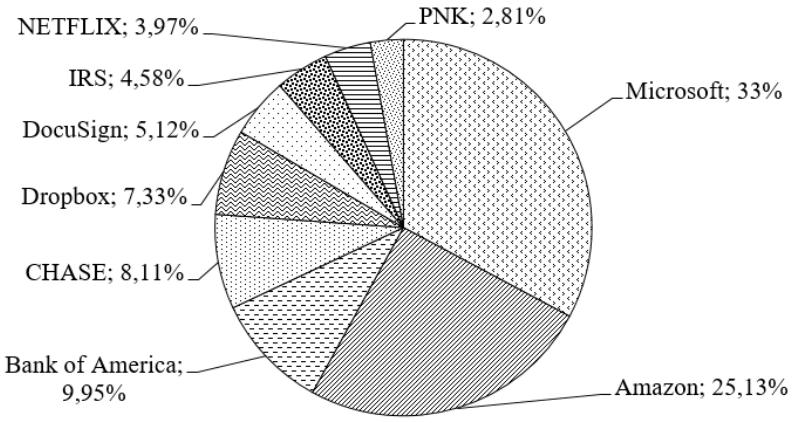

Рис. 3. Світові бренди, що зазнали найбільших кібератак у 2020 р.

Джерело: узагальнено на основі звітів з інформаційної безпеки Мережевої академії *Cisco* [4].

Сьогодні впровадження режимів віддаленої роботи, дистанційного навчання, практик міжособистісного спілкування і відеоконференцій докорінно змінює світовий кіберпростір. В Україні політика щодо кібербезпеки покладається на низку державних органів: Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України, Генеральний штаб Збройних сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи.

За інформацією Департаменту кіберполіції, щороку кількість кіберзлочинів в Україні збільшується в середньому на 2.5 тисячі. Згідно зі звітом, який міститься на вебсайті цього правоохоронного органу, працівники Департаменту кіберполіції були залучені до розслідування понад 11 тисяч виявлених кримінальних злочинів, вчинених у сфері високих інформаційних технологій [5].

Однак, незважаючи на велику кількість кримінальних проваджень, Департамент кіберполіції не озвучує реальних результатів таких розслідувань. Вказуючи у звіті на число виявлених правопорушників у кількості 800 осіб, він не надає будь-якої інформації про кількість реальних вироків щодо вказаних осіб та притягнення їх до відповідальності. Зі звіту не зрозуміло, чи оголошено цим особам підозру, чи висунуто обвинувачення та в якому статусі вони перебувають.

Аналіз даних статистичної звітності за 2019 р. показав, що переважну більшість у структурі досліджуваних кіберзлочинів становлять ті, відповідальність за які передбачено ст. 362 Кримінального кодексу України "Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї" [6], (*рис. 4)*.

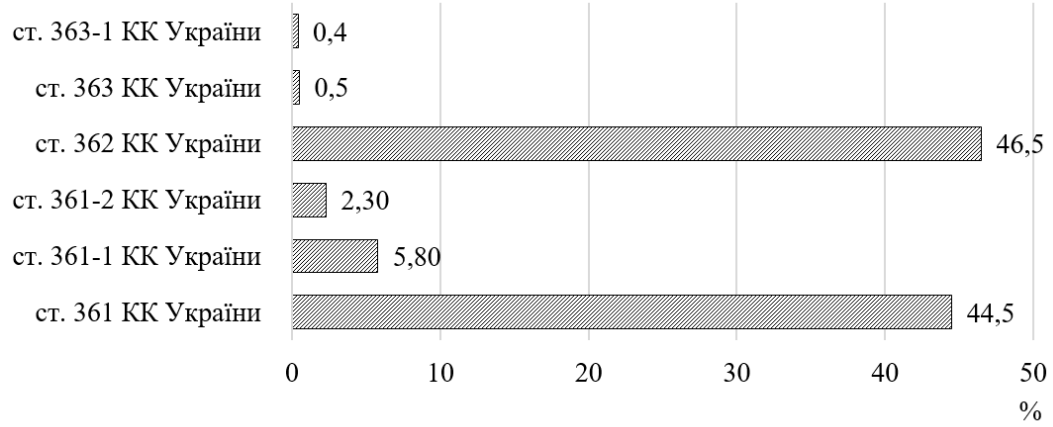

Рис. 4. Структура злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в Україні у 2019 р.

Джерело: побудовано на основі даних Департаменту кіберполіції України [5].

На другому місці – злочини, передбачені ст. 361 Кримінального кодексу України (44.5 %), тобто несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Решта злочинів становить незначну частку. Отже, можна констатувати, що персональні й облікові дані найчастіше цікавлять зловмисників, коли вони атакують юридичних осіб: у компаніях можуть зберігатися великі за обсягом бази як персональних, так і облікових даних клієнтів. Крім того, зловмисники можуть бути зацікавлені в облікових даних співробітників обраної компанії-жертви.

"Під прицілом" опиняються й облікові записи в соціальних мережах, особливо якщо акаунт добре "розкручений" та має велику кількість передплатників. Користувачі, своєю чергою, не завжди дбають про безпеку акаунтів: використовують нестійкі й однакові паролі, вводять облікові дані, не переконавшися в надійності ресурсу, видають інформацію про себе, яка може допомогти підібрати пароль. Це пояснює високу частку вкрадених облікових даних (44 % в атаках на фізичних осіб) *(рис. 5)*. Так, до категорії людей, що входять до зони підвищеного ризику атак з боку хакерів, належать любителі комп'ютерних ігор, адміністратори баз даних підприємств.

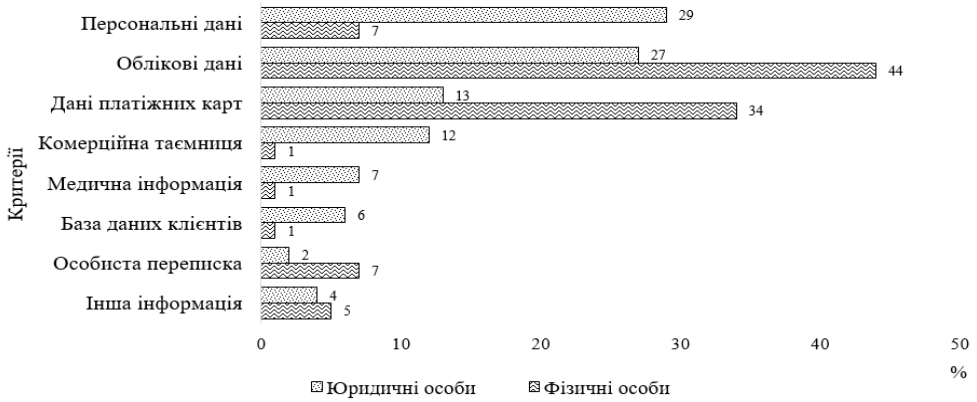

Рис. 5. Категорії даних, які зазнають кібератак в Україні

Джерело: побудовано на основі даних Департаменту кіберполіції України [5].

Зазвичай дані банківських карт клієнтів захищені криптографічними методами, тому зловмисникам простіше дізнатися їх у клієнта за допомогою методів соціальної інженерії. Як наслідок, 34 % вкраденого в результаті кібератак – це дані банківських карт.

Цікаво дослідити, які сфери діяльності більшою мірою атакують хакери *(рис. 6)*.

У 2020 р. частка цілеспрямованих кібернападів істотно зросла – до 59 %. Частка кіберінцидентів, внаслідок яких постраждали приватні особи, склала 24 %. Серед юридичних осіб зловмисники частіше атакували державні організації, промислові підприємства, медичні заклади, банки й організації фінансової сфери.

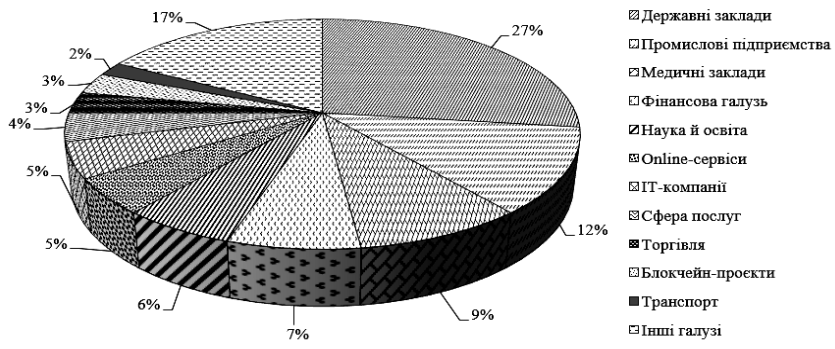

Рис. 6. Структура жертв кібернападів серед юридичних осіб у 2020 р. за категоріями

Джерело: побудовано на основі даних Департаменту кіберполіції України [6].

В умовах пандемії інтерес хакерів до кіберпростору підприємств посилюється. Дослідження "портрета" комп'ютерного злочинця показує, що в електронну злочинність втягнуто широке коло осіб – від висококваліфікованих фахівців до дилетантів. Правопорушники мають різний соціальний статус, а також рівень освіти та виховання *(рис. 7)*.

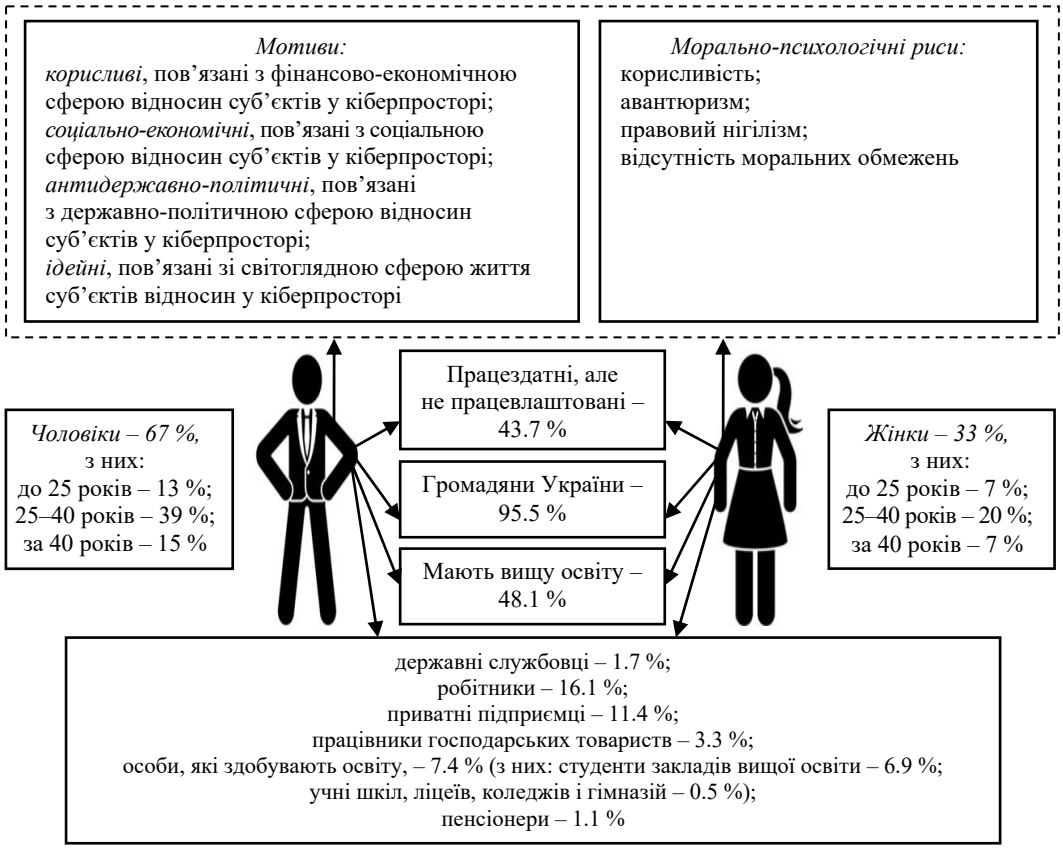

Рис. 7. "Портрет" сучасного кіберзлочинця в Україні

Джерело: побудовано на основі даних Департаменту кіберполіції України [6].

З метою розгляду технологій на ринку кібербезпеки й захисту інформації під час пандемії *COVID-19* проведено онлайн-опитування 147 респондентів з 50 підприємств України різної форми власності та сфери діяльності. Кожен з них оцінював, як вплинула ситуація з *COVID-19* на кібербезпеку їхнього підприємства. Результати опрацювання отриманої з опитування інформації уможливили дати відповідь на низку запитань, що мали за мету з'ясувати, наскільки готовим виявилося підприємство до шокових змін внаслідок пандемії та спричинених нею обмежень, зокрема й у цифровому просторі. Детальніше підсумки анкетування представлено у *табл. 1*. Аналіз результатів опитування свідчить, що близько половини респондентів переконані, що їхні підприємства або не мають плану дій у разі надзвичайних ситуацій, або не знають про наявність у них плану дій на випадок пандемії або іншої надзвичайної ситуації. Переважна більшість респондентів (78.92 %) зазначає, що пандемія *COVID-19* у довгостроковій перспективі змінить методи роботи підприємства з пріоритетом на стратегічні зміни за непередбачуваних подій.

Таблиця 1

Аналіз результатів анкетування
"Вплив пандемії *COVID-19* на кібербезпеку підприємства"

Запитання	Відповіді	Кількість опитаних респондентів	% відповідей
Чи мало Ваше підприємство план дій у разі надзвичайних ситуацій, на випадок розвитку світової пандемії?	Так	77	52.4
	Ні	61	41.5
	Невідомо	6	4.1
	Сформували оперативно	3	2.0
Чи змінить пандемія *COVID-19* методи роботи підприємства у довгостроковій перспективі?	Так	50	34.01
	Ні	19	12.92
	Невідомо	12	8.16
	Певною мірою	66	44.91
Які саме кібератаки посилилися на підприємстві під час пандемії *COVID-19*?	*DDoS attack*	18	12.24
	Trojans	26	17.69
	Advanced Persistent Threat	8	5.44
	Відсутність можливості оновити ПК	37	25.17
	Фішингові атаки	26	17.69
	Атаки на соціальні мережі/чат-боти	17	11.56
	Атаки на замовників та систему постачання товарів і послуг	10	6.81
	Відсутні кібератаки	5	3.40
Які ризики безпеки турбують керівників підприємств найбільше, коли персонал працює віддалено?	Працівники почуваються вільно щодо інформаційної безпеки завдяки роботі в домашніх умовах	41	27.89
	Працівники не дотримуються протоколу, особливо за можливості втручання підозрілих контактів	34	23.13
	Працівники стають жертвами фішингових атак	32	21.77
	Витік інформації від співробітників у зовнішнє середовище	25	17.01
	Хакерство	15	10.20
За якими напрямами можна зробити висновки в політиці кібербезпеки у довгостроковій перспективі (після завершення пандемії *COVID-19*)?	24/7 IT-підтримка	37	25.17
	Проведення тренінгів щодо IT-безпеки	35	23.81
	Впровадження інструментів визначення й оцінювання ризиків	19	12.92
	Розширення досвіду аутсорсингу IT-безпеки	18	12.24
	Інвентаризація доступу до інфраструктури підприємства	16	10.88
	Впровадження на 100 % електронного документообігу та токенів	22	14.98

Джерело: розраховано за даними анкетного опитування 147 респондентів 50 підприємств України в листопаді 2020 р.

Швидкі зміни в бізнесі часто надають зловмисникам можливості для отримання доступу до корпоративної інформації. Опитані зазначають, що під час пандемії почастішали випадки фішингових атак, здирництва, загроз у соціальних мережах або чат-ботах, "троянів" й атак на ланцюжках постачання – і це лише деякі з методів нападів. Оскільки під час пандемії *COVID-19* велика кількість співробітників працює вдома, респонденти помітно стурбовані наслідками для кібербезпеки. Більш ніж

кожний третій вважає, що співробітники спокійніше ставляться до питань кібербезпеки, оскільки працюють в домашньому середовищі. Понад 23 % працівників не дотримуються прото-колів безпеки й не турбуються про виявлення підозрілих зазіхань у кіберпросторі.

Пандемія надала важливого поштовху навчитися розв'язувати проблеми, пов'язані зі змінами в кадровій моделі, й планувати альтернативні сценарії поведінки за непередбачуваних подій. Кожний третій фахівець має намір отримувати цілодобову IT-підтримку та збільшити кількість навчань з питань IT-безпеки для співробітників. Майже 15 % IT-фахівців планують впровадження електронного документообігу та токенів (носіїв захищеного ключа), що дасть змогу якісно та безпечно працювати з інформацією.

Нинішня ситуація потребує абсолютно нових підходів до управління підприємством та його ресурсами. Успіх цих змін, а відтак, і виживання підприємства за сучасних умов значною мірою залежать від того, наскільки гнучко організовуються бізнес-процеси та як швидко відбувається перехід до нових методів роботи. Через постійні зміни та неможливість точно спланувати цей процес підприємства відчули наслідки кіберризиків більшою мірою, ніж це відбувалося раніше. Такі аргументи обумовлюють необхідність дотримання нової моделі кібербезпеки підприємства в умовах *COVID*-реальності *(табл. 2)*.

Таблиця 2

Кібербезпека за умов *COVID*-реальності

Проблема	Характеристика	Рекомендації щодо розв'язання	Платформи для роботи
Незахищене віддалене підключення до підприємства (офісу)	Не всі підприємства технічно готові до впровадження масової віддаленої роботи. IT-персонал під тиском часу може придбати та запропонувати не найбільш безпечні рішення	Доречно впровадити багатофакторну автентифікацію для доступу до даних підприємства та використовувати безпечні й надійні хмарні рішення для співпраці щодо бізнес-процесів	*Microsoft Teams, Google Hangouts Meet, LogMeIn Emergency Remote Work Kit, Cisco Webex*
Розширене використання офісної техніки в особистих цілях	Підвищення ризику зараження робочої техніки вірусами або зловмисним програмним забезпеченням під час відвідування менш захищених вебсайтів (пов'язаних з особистими інтересами)	Доречно оновлювати офісне обладнання автоматично, дотримуючись порад постачальника програмного забезпечення	Особливо важливо оновлювати вебпереглядачі та відповідне програмне забезпечення сторонніх виробників (наприклад програми для перегляду *PDF*-файлів, *Flash*-програвачі та *Java*)
Спроби фішингових атак, які експлуатують тематику *COVID-19*	Багато злочинних кіберугруповань змінили свою тактику на використання матеріалів *COVID-19* як приманки. Створено велику кількість підроблених вебсайтів, пов'язаних із *COVID-19*	Консультування співробітників щодо моніторингу новин про *COVID-19* в Україні та світі з використанням суто офіційних джерел інформації	Вебсайт Міністерства охорони здоров'я України, Центру громадського здоров'я або внутрішні корпоративні ресурси підприємства

Джерело: узагальнено на основі даних ТОВ "КПМГ-Україна" [7].

Отже, сучасні підприємства мають бути обізнані з підвищеними кіберризиками під час застосування віддаленої праці в умовах пандемії *COVID-19*, про які варто замислитися керівникам підприємств. Пандемія змусила переглянути інфраструктуру підприємств і переорієнтуватися на актуальні інформаційні потреби користувачів та співробітників. Проведене дослідження показало, що сучасні зміни обумовлюють необхідність переосмислення стратегії й інвестування значних коштів у забезпечення надійного захисту корпоративної інформації та даних працівників підприємств.

Гіганти світової IT-індустрії *(Google*, *Microsoft*, *Amazon*, *Intel*, *Intella*, *IBM*, *Infineon*, *NXP*, *Lenovo*, *RSA)*, відомі фінансові компанії *(PayPal*, *MasterCard*, *VISA*, *Goldman Sachs*, *ING)* і безліч компаній меншого масштабу пропонують безпечний спосіб реєстрації в хмарі та забезпечують захист транзакцій за допомогою перевірки відбитків пальців. У цьому разі паролі більше не спрямовуються на сервери баз даних. Шифрування виконується за допомогою відкритих ключів, водночас ключі залишаються на пристроях. Така схема захисту, що називається *FIDO*, унеможливлює відстежити взаємозв'язок між сервісами [8].

До переваг багатофакторної ідентифікації належить її здатність захистити інформацію як від внутрішніх загроз, так і від зовнішніх вторгнень. Вона створена на основі спільного використання низки факторів автентифікації, що значно підвищує інформаційну безпеку.

Усім відомий приклад – автентифікація за допомогою *SMS*, заснована на використанні одноразового пароля. Перевага такого підходу проти постійного пароля полягає в тому, що цей пароль не можна використовувати повторно. Приклад застосування біометричних пристроїв і методів автентифікації – використання сканера відбитка пальця з підтвердженням повноважень паролем. Аналогічно можуть бути використані й інші біометричні автентифікатори: обриси та розміри особи; характеристики голосу; візерунок райдужної оболонки й сітківки очей.

Існують також програмно-апаратні рішення, як-от: автономні ключі для генерації одноразових паролів, зчитувачі *RFID*-міток, програмні й апаратні токени, *Mobile ID*, електронні ключі різних типів.

Як інший фактор автентифікації може використовуватися і біометрія. Наприклад, *Match-on-Card*, *Match-on-Chip* і подібні технології уможливлять замінити введення *PIN*-коду аналізом відбитка пальця, що додає зручності використання, оскільки не потрібно запам'ятовувати й вводити *PIN*-код [8].

Також набувають популярності "платформи безпеки", або *ThinkShield*, які розроблені для захисту пристроїв, особистих або конфіденційних даних від крадіжки в Інтернеті. Набору інструментів безпеки *ThinkShield* для комп'ютерів *ThinkPad* відводиться ключова роль, адже він містить у собі цілий комплекс захисних засобів, починаючи з найпростіших і закінчуючи досить просунутими *(табл. 3)*.

Таблиця 3

Засоби захисту від кіберзлочинів в умовах *COVID*-реальності

Технологія безпеки	Переваги під час пандемії *COVID-19*
ThinkShutter	Механічна шторка на камері захищає приватне життя від сторонніх очей
Сертифікація *FIDO*	Забезпечує спрощену та надійно захищену автентифікацію для входу в систему і безпечних платежів
Багатофакторна автентифікація *Intel*	*PIN*-коди, біометричні дані, ключі та токени безпеки, а також пов'язані сертифікати зашифровані та зберігаються в місці, надійно захищеному від стандартних методів злому
Технологія *Smart USB Protection*	Блокує передачу даних через *USB*-порти
Безпечна док-станція	Фізичне блокування ноутбука, встановленого на док-станцію, дає змогу запобігти крадіжці
Сканер відбитків пальців *Match-on-Chip*	Збереження сканів відбитків пальців у безпечному сховищі на чипі забезпечує додатковий захист біометричних даних від зловмисників
Absolute	Надає IT-адміністраторам інструменти двостороннього зв'язку з пристроями, що уможливлюють дистанційно оцінювати ризики, запобігати інцидентам небезпеки та реагувати на них
Буферна зона	Використання технологій віртуалізації для ізоляції кібератак на кінцевій точці або в мережі
Послуга "Залиште жорсткий диск у себе"	Дає змогу клієнтам зберегти свій жорсткий диск/файли після заміни за гарантією
Winmagic	Захист даних, забезпечення відповідності нормативно-правовим вимогам, оптимізація роботи, підтримка уніфікованого шифрування в масштабах усього підприємства
Резервне копіювання онлайн *(OLDB)*	Дає змогу підприємствам швидко і безпечно автоматично зберігати конфіденційну інформацію в хмарі
Захищений жорсткий диск *USB*	Повністю зашифрований зовнішній пристрій для зберігання даних, для доступу до якого потрібний цифровий пароль
Lenovo WiFi Security	Блокування показу даних користувача в ненадійних мережах
ThinkPad PrivacyGuard	Активізація захисту екрану натисканням кнопки, повідомлення у разі появи кіберзлочинця, який намагається отримати доступ до інформації на екрані

Джерело: узагальнено на основі [8].

Упродовж наступних десятиріч на всі держави світу чекають специфічні випробовування, викликані стрімким розвитком інформаційно-комунікаційних технологій [9, с. 11]. Тому головною темою обговорення у світі має стати зміцнення кібербезпеки в умовах пандемії *COVID-19* та скорочення кількості кібернападів у кіберпросторі. Ця проблема потребує якнайшвидшого розв'язання, оскільки винайдені нині зразки кіберзброї вирізняються глобальною досяжністю та практично миттєвим впливом без будь-якого способу отримання попередження про її застосування.

Висновки. Визначено основні напрями захисту підприємств від кіберзагроз, збереження суверенітету кіберпростору та національної безпеки країн світу. Так, автоматизовані системи управління уможливлять використання технічних пристроїв замість робочої сили за небезпечних для життя людей обставин.

Важливо змінити стереотип у суспільстві, що людина та її особисті дані нікому не цікаві, доцільно навчати фахівців користуватися захищеними протоколами передавання інформації, використовувати захищені інформаційні системи для роботи, а працівникам IT-сфери – обґрунтовувати необхідність застосування нових безпечних принципів роботи клієнтів в інформаційних системах підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII (В редакції Закону України від 24.10.2020 р. № 2163-VIII). URL: https://zakon.rada.gov.ua.
2. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право*, 2018. № 1 (24). С. 127-132.
3. Гуцалюк М. В. Окремі аспекти боротьби з організованою кіберзлочинністю. *Актуальні проблеми управління інформаційною безпекою держави:* зб. тез наук.-практ. конф. (м. Київ, 4 квітня 2019 р.). Київ: Нац. акад. СБУ, 2019. С. 199-201.
4. Офіційний сайт Мережевої академії *Cisco*. URL: https://www.netacad.com/ru/about-networking-academy.
5. Офіційний сайт Кіберполіції України. URL: https://cyberpolice.gov.ua.
6. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-XIV. Верховна Рада України. URL: http://zakon.rada.gov.ua.
7. Офіційний сайт ТОВ "КПМГ-Україна". URL: https://home.kpmg/ua/uk/home/about/overview.html.
8. Новые угрозы кибербезопасности: все намного масштабнее, чем вы думали. URL: https://habr.com/ru/company/lenovo/blog/445184.
9. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.
10. Печенюк А. В. Інформаційна безпека України як складова національної безпеки. URL: https://www.ndifp.com/1561.

Стаття надійшла до редакції 05.01.2021.

Biliavska Yu., Mykytenko N., Shestak Ya. Cybersecurity and the information protection during the COVID-19 pandemic.

Background. The society has entered the era of innovation, where industrial robots, 3D-printing, cloud sources of information, unmanned vehicles in mass production, 4G and 5G communications, genomics, VR-technologies, smart cities are becoming the usual practice and form the new face of management. However, the COVID-19 pandemic is changing our everyday life: the population is experiencing concern and worry, making actual the need for help and support, a sense of safety and a desire for certainty.

The aim is to identify trends in the spread of cybercrime in the information security market during the COVID-19 pandemic and to substantiate the recommendations for cybersecurity by enterprises in the conditions of COVID-reality.

Materials and methods. In the research process we used a set of general scientific and special methods: analytical, historical, and logical generalizations; economic and statistical methods (selective observation, comparative and technical and economic analysis, grouping based on the usage of MS Excel software products); marketing and sociological researches (surveys) as well as the expert assessments.

Results. Every day groups of experienced cybercriminals seize the control of someone else's cloud environment, servers, computers and mobile gadgets by launching the series of destructive programs against particular web-sites. Powerful attacks are organized by affecting the servers and clients' computers, which in a matter of seconds shut down ATMs, the telephone lines, the whole companies, and even the Presidential websites around the world. In different countries, more and more attention is paid to the cybersecurity and the information resources management.

Conclusion. Automated control systems will make possible the use of technical devices instead of workforce in the life-threatening circumstances. In addition, it is very important to change the stereotype in society that a person and his personal data are not interesting to anyone, it is advisable to train professionals to use secure information transfer protocols, use secure information systems to work, and IT workers – to justify the need to apply new secure customer principles in information systems of enterprises.

Keywords: cybersecurity, cyberattack, cyber risk, cybercrime, COVID-19 pandemic, COVID-reality, token, fishing.

REFERENCES

1. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrai'ny: Zakon Ukrai'ny vid 5 zhovtnja 2017 roku № 2163-VIII (V redakcii' Zakonu Ukrai'ny vid 24.10.2020 r. № 2163-VIII) [On the Basic Principles of Cyber Security of Ukraine: Law of Ukraine of October 5, 2017 № 2163-VIII (As amended by the Law of Ukraine of October 24, 2020 № 2163-VIII)]. (2020). Retrieved from https://zakon.rada.gov.ua.
2. Marushhak, A. I. (2018). Informacijno-pravovi aspekty protydii' kiberzlochynnosti [Information and legal aspects of combating cybercrime]. *Informacija i pravo – Information and law, 1 (24),* 127-132.
3. Gucaljuk, M. V. (2019). Okremi aspekty borot'by z organizovanoju kiberzlochynnistju [Some aspects of the fight against organized cybercrime]. *Aktual'ni problemy upravlinnja informacijnoju bezpekoju derzhavy – Actual problems of information security management of the state:* Proceedings of the International Scientific and Practical Conference. (pp. 199-201). Kyi'v: Nacional'na akademija SBU.
4. *Oficijnyj sajt Merezhevoi' akademii' Cisco [Official site of the Cisco Networking Academy].* Retrieved from https://www.netacad.com/ru/about-networking-academy.
5. *Oficijnyj sajt Kiberpolicii' Ukrai'ny [Official site of the Cyber police of Ukraine].* Retrieved from https://cyberpolice.gov.ua.
6. Kryminal'nyj kodeks Ukrai'ny vid 5 kvitnja 2001 r. № 2341-XIV [Criminal Code of Ukraine of April 5, 2001 № 2341-XIV]. *Verhovna Rada Ukrai'ny – Verkhovna Rada of Ukraine.* Retrieved from http://zakon.rada.gov.ua.
7. *Oficijnyj sajt TOV "KPMG-Ukrai'na" [Official site of "KPMG-Ukraine" Ltd.].* Retrieved from https://home.kpmg/ua/uk/home/about/overview.html.
8. *Novye ugrozy kiberbezopasnosti: vse namnogo masshtabnee, chem vy dumali [New cybersecurity threats: everything is much larger than you thought].* Retrieved from https://habr.com/ru/company/lenovo/blog/445184.
9. Dubov, D. V. (2014). *Kiberprostir jak novyj vymir geopolitychnogo supernyctva [Cyberspace as a new dimension of geopolitical rivalry].* Kyi'v: NISD.
10. Pechenjuk, A. V. *Informacijna bezpeka Ukrai'ny jak skladova nacional'noi' bezpeky [Information security of Ukraine as a component of national security].* Retrieved from https://www.ndifp.com/1561.