УДК (330.34+004.77):(334.71+327.88)

КРАУС Катерина Миколаївна
кандидат економічних наук, доцент, доцент кафедри управління
Київський університет імені Бориса Грінченка, Україна
ORCID ID: 0000-0003-4910-8330
e-mail: k23k@ukr.net

КРАУС Наталія Миколаївна
доктор економічних наук, професор, професор кафедри фінансів та економіки
Київський університет імені Бориса Грінченка, Україна
ORCID ID: 0000-0001-8610-3980
e-mail: k2205n@ukr.net

ШТЕПА Олена Валентинівна
кандидат економічних наук, доцент, доцент кафедри управління
Київський університет імені Бориса Грінченка, Україна
ORCID ID: 0000-0003-2220-2052
e-mail:o.shtepa@kubg.edu.ua

ЦИФРОВА ТРАНСФОРМАЦІЯ КІБЕРБЕЗПЕКИ НА МІКРОРІВНІ В УМОВАХ ВОЄННОГО СТАНУ

У статті описуються можливі трансформаційні процеси кібербезпеки суб'єктів господарювання в умовах воєнного стану. Автори стверджують, щодо критеріїв безпеки сучасного цифрового підприємництва варто відносити наступні обов'язково наявні факти: дані завжди мають бути зашифровані при зберіганні та передачі; шифрування має відбуватися на клієнтському рівні; лише клієнт має мати доступ до ключів шифрування; фактичні дані не мають передаватися по відкритим каналам пошти; компанія повинна контролювати сховище зашифрованої інформації і ключі доступу до неї.

Вказано низку сучасних зовнішніх та внутрішніх загроз для ведення бізнесу, серед чого зокрема названо проникнення в мережу, втрата пристроїв зі збереженими паролями, віруси-шифрувальники. Визначено основні задачі підприємств в частині забезпечення кібербезпеки, а саме: виявлення потенційних загроз кібербезпеки підприємств і вражливостей; попередження кіберінцидентів; нейтралізація або мінімізація загроз інформаційної безпеки підприємства.

Автори розглядають вплив системи управління інформаційною безпекою ISO/IEC 27001:2013 на роботу організацій. З'ясовано, що дана система дає можливість впровадити найкращу практику для удосконалення захисту даних та усунення загрози порушення безпеки інформаційних систем.

У статті зосереджено увагу на тому факті, що в рамках забезпечення кібербезпеки в умовах воєнного стану та в ході подальшого відцифрування діяльності на мікрорівні, до базових та першочергових задач повинні відноситися, в основному, нова якість виробничих процесів технологічних лабораторій: планування робіт у відповідності з вимогами галузевих стандартів, інструкцій і передових практик; відбір проб в систему шляхом присвоєння їй визначеного ідентифікатора; розрахунок результатів та їх оформлення.

Практикою підприємницької діяльності засвідчено, що до прикладу, Ramsomware являється найбільш розповсюдженою загрозою в ході реалізації бізнес-процесів. Ramsomware ділять на два основних типи – шифрувальники (криптори – "cryptoransomware") і блокувальники (блокери – "blockers"). Шифрувальники, потрапляючи до головного комп'ютера підприємства, кодують цінні файли такі як документи, фотографії, бази даних. Загрози Ramsomware через вплив на бізнес полягають до прикладу в часових втратах даних, що може повністю порушити надзвичайно важливі для бізнесу процеси; постійних втратах даних, що ведуть до падіння конкурентоспроможності компанії, скорочення доходів від продажу у довгостроковій перспективі, порушені неперервного доступу до даних.

Автори статті дійшли висновку, що в світлі таких злочинних кібератак звісно логічним є напрацювання різного роду видів захисту з метою убезпечення даних від їх перехоплення. Цей захист має бути: невидимим для сторонніх очей; мати канал безпечної пошти; e-mail сертифікат; e-mail сейф; e-mail шредер; центр кібербезпеки; шифрування листів і вкладень; захищений перегляд.

***Ключові слова**: цифрова трансформація, кібербезпека, мікрорівень, кібератаки, кіберзагрози, кібергігієна*

JEL classification: H56; L86; N40; O11; O12; O14; O40
DOI: https://doi.org/10.31649/ins.2022.3.26.37

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

Цифрова економіка являє собою деяку господарську діяльність, в якій ключовими факторами виробництва є дані в цифровому вигляді або діяльність по створенню, розповсюдженню і використанню цифрових технологій і пов'язаних з ними продуктів та послуг. Переслідуючи мету ефективного функціонування в сьогоднішніх умовах, бізнес змушений швидко давати відсіч кібератакам та низці існуючих кіберзагроз. Так, за 2017 рік в США відбулося 130 витоків інформації. 31 % організацій зіштовхнулись з атаками на інфраструктуру експлуатаційних і операційних технологій. Витрати на безпеку у 2017 році у порівнянні з 2016 виросли на 23 % і становлять $ 11,7 млн.. До прикладу, масштабний витік даних 147,9 млн. американців стався через "взлом" бюро кредитних історій Equifax. Зловмисники використали вразливість у системі безпеки додатків на веб-сайті компанії і отримали доступ до номерів соціального страхування, дат народження та адрес.

Тож сучасні технологічні тенденції, такі як електронна комерція, блокчейн, Інтернет речей, комп'ютерний інжиніринг, сучасні технології бездротового зв'язку, поширення нових бізнес-моделей в умовах використання передових цифрових технологій, хмарні обчислення, аналіз великих даних створюють всі можливості для нової якості ведення бізнесу. В той же час, поряд з інноваційністю, з'являється деяке ускладнення і прискорення в умовах цифрового середовища, що викликає проблему становлення цифрової безпеки в умовах воєнного стану в Україні.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Цінними, в науковому сенсі, дослідженнями проблематики кіберзагроз, кібератак, кібербезпеки в умовах цифровізації та військового стану є наукові праці та практичні дослідження і розробки таких українських вчених-економістів як:С. Вітер [1], А. Десятко [2], І. Дрозд [3], Ю. Когут [4], Н. Краус [7], К. Краус [6, 8], О. Маковець [3], О. Манжура [5, 16], О Марченко, В. Осецький [15], А. Раєцький [11], О. Сунічук [9], І. Світлишин [1], О. Штепа [14], Д. Швець [9] та інші.

Українські науковці І. Дрозд та О. Маковець в своїх дослідженнях розглядається необхідність забезпечення належного рівня фінансової безпеки підприємства крізь призму існування такого виду втручання у діяльність суб'єктів господарювання як кіберзагрози [3]. Для всебічного та об'єктивного висвітлення науковці провели огляд таких теоретичних понять як фінансова безпека підприємства, кіберзагроза, кібербезпека, кіберзахист у їх взаємозв'язку. Основну увагу зосередили на висвітленні збитків та втрат для бізнесу, які за собою тягнуть кібератаки. Дослідники запропоновано враховувати категорії кіберзагроза та кібербезпека у дослідженні питання інвестиційної привабливості підприємства, що на наше переконання є досить цінним науковим здобутком.

Не менш цінною в науковому та практичному сенсі є праця українських дослідників С. Вітера та І. Світлишина під назвою "Захист облікової інформації та кібербезпека підприємства" [1]. Так науковці вказали відмінність між інформаційною безпекою та кібербезпекою, запропонували авторське бачення "кібербезпеки облікової

інформації", обґрунтовано актуалізували питання організації на підприємствах системи кібербезпеки облікової інформації. Дослідникам вдалось визначити принципи і заходи захисту облікової інформації в контексті кібербезпеки.

Проблемам кібергігієни, кібербезпеки і безпеки держави присвячені матеріали наукового семінару, організованого колективом вітчизняних науковців під керівництвом О. Криворучко, А. Десятка й В. Звєревим [2]. Матеріали круглого столу присвячені питанням у сфері економічного, соціального, нормативно-правового, адміністративного безпечного функціонування кіберпростору, технічного забезпечення кібербезпеки, боротьби з кіберзлочинністю, захисту інформації в комп'ютерних системах і мережах.

3. ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ ОЗНАЧЕНА СТАТТЯ

Разом з тим, значна кількість проблем щодо бачення концепції цифрового розвитку в частині кібербезпеки суб'єктів господарювання та їх інклюзивного доступу в умовах цифрової трансформації економіки, залишаються недостатньо розкритими.

4. ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження перспективних можливостей для безпечного функціонування суб'єктів господарювання, цифрової трансформації кібербезпеки в умовах воєнного стану. Аналіз досвіду минулих кібератак та визначення критеріїв безпеки сучасного цифрового підприємництва. Визначення задач підприємств в частині забезпечення кібербезпеки. Обґрунтування змістових можливостей роботи лабораторних інформаційних менеджмент систем (LIMS) для посилення кібербезпеки українських суб'єктів господарювання. Напрацювання низки шляхів, інструментів посилення кібербезпеки на мікрорівні та рекомендаційних вказівок в частині процедурного управління кіберінцидентами.

5. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБҐРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

Протягом двох останніх десятиліть стрімко розвивалися цифрові технології. Це викликало великий ажіотаж з приводу можливостей, які відкриває нова епоха цифрових гаджетів. Перехід від аналогових технологій до цифрових, тобто ера цифрової революції, передумовами якої є широке розповсюдженням інформаційно-комунікаційних технологій, вже настала і дуже активно прогресує. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом найбільш вразливим до кіберзагроз.

Нині у сучасному інформаційному суспільстві комп'ютерні злочини стали характерною ознакою сьогодення. Розрізняють різні категорії комп'ютерних злочинців: "хакери", "кракери", "пірати", "шкідники". Злочини, що утворюються злочинними угрупуваннями з використанням інформаційних технологій (ІТ): кібертероризм, загроза фізичної розправи, дитяча порнографія, "відмивання" грошей, крадіжка грошей з банківських рахунків, шахрайські операції з пластиковими платіжними картками, розповсюдження інформації про наркотики через Інтернет. З розвитком ІТ з'являються нові системи управління корпоративним підприємством, контролем над операціями в підприємстві, передачі інформації та її захист [2, с. 12].

Кібербезпека являє собою складний процес, але вона є обов'язковою складовою успішного бізнесу. Час, в який ми живемо можна ознаменувати епохою Інтернету. До того ж кожна організація відцифровує свою діяльність, і так чи інакше використовує в своїй роботі новітні технології і процеси, застосовують нові принципи організації праці. Кожна складова бізнес-процесів, представляє лише окрему ланку в нескінченному ланцюзі взаємопов'язаних елементів. Сьогодні підприємствам складніше ніж коли-небудь чітко визначити критичні точки у власній багатогранній інфраструктурі через яку вони взаємодіють з оточуючим світом. Такі умови створюють підґрунтя для хакерських атак [11].

Статистикою підтверджено, що 96 % кібератак і витоку даних розпочинається з e-mail. E-mail захищений так само, як поштова листівка, адже електронні листи "проходять" через вразливі та потенційно небезпечні поштові сервери. При цьому, SSL/TSL не гарантує безпеки. Сьогодні перехоплення даних та "взлом" можливі всього за $ 200, а

мережеві імпланти для перехоплення трафіку коштують всього від $ 60. Не дивно, що браузери назвичайно вразливі до "взломів". E-mail інфраструктура не верифікує відправника. Засоби захисту периметру компанії не захищають e-mailпісля відправки листів.

Так, станом на 01.01.2019 рік, 46 % всіх зкомпроментованих систем не мали шкідливого ПЗ; 63 % зкомпроментованих облікових даних користувачів використовувалися для проникнення; 86 % комп'ютерів в ботнетах мають встановлений антивірус; $ 6 млрд. втратили жертви шахрайства з електронної пошти з 2013 року по 2018 рік; $ 100 тис. становить середній збиток від атаки на електронну пошту. З цих фактів стає очевидним, що недооцінка кібербезпеки підприємством призводить до великих збитків і втратам, до порушення конфіденційності і відтоку даних, розголошенню комерційної таємниці, можливості промислового шпіонажу, непередбачуваних проблем бізнес-процесів, інтелектуального піратства, зниження якості продукції і послуг.

Цифрова економіка є по суті, інноваційною надбудовою реальної економіки, котра, в той же час, не може існувати відсторонено від матеріального виробництва. Потенційні переваги даних цифрових технологій, безумовно, величезні, але їх впровадження створюють загрози безпеки особистої інформації членів суспільства, а найменший відтік даних підриває віру до інновацій та економіки загалом. До того ж, стрімкий ріст кількості порушень кібербезпеки в умовах цифровізації економіки, який простежується сьогодні, є тісно пов'язаний з постійним ускладненням та ростом масштабів застосування цифрових технологій, які до того ж, постійно вдосконалюються [5, с. 212]. З цих причин, для підтримки конкурентоспроможності на ринку важливо використовувати всі доступні можливості, що надаються сучасними засобами забезпечення кібербезпеки.

До критеріїв безпеки сучасного цифрового підприємництва варто відносити наступні обов'язково наявні факти:

- дані завжди мають бути зашифровані при зберіганні та передачі;
- шифрування має відбуватися на клієнтському рівні;
- лише клієнт має мати доступ до ключів шифрування;
- фактичні дані не мають передаватися по відкритим каналам пошти;
- компанія повинна контролювати сховище зашифрованої інформації і ключі доступу до неї;
- рішення має відповідати законодавству (наприклад GDPR).

Більше того, зовнішніми загрозами для бізнесу є: шкідливе ПО; DDoS-атаки; фішингові атаки; проникнення у мережу; втрата пристроїв зі збереженими паролями. Внутрішніми найпопулярнішими загрозами називають вразливе програмне забезпечення та витоки через співробітників або їх з вини.

Головними загрозами кібербезпеки цифрової економіки на мікрорівні на сьогодні є віруси-шифрувальщики, наприклад, cryptoiocker, який проникає не лише до персональних комп'ютерів, але і до мереж стратегічних об'єктів, АЕС, аеропортів, оборонних підприємств, великих заводів, - віруси, здатні викликати техногенні катастрофи. Втрати і збитки від таких проникнень обчислюються сотнями мільйонів доларів. До найбільш актуальних для підприємств кіберзагроз відносять фішинг (22 %), кібератаки (з метою дезорганізації діяльності) (13 %), кібератаки (з метою розкрадання грошових коштів) (12 %), шахрайство (10 %), кібератаки (з метою розкрадання об'єктів інтелектуальної власності) (8 %), спам (6 %), атаки з середини підприємства (5 %), стихійні лиха (2 %), шпигунство (2 %) [4, с. 36].

Основними задачами підприємств в частині забезпечення кібербезпеки повинні стати:

- виявлення потенційних загроз кібербезпеки підприємств і вразливостей;
- попередження кіберінцидентів;
- нейтралізація або мінімізація загроз інформаційної безпеки підприємства.

Переслідуючи мету кібербезпеки суб'єкта господарювання в умовах цифровізації економіки та воєнного стану, на нашу думку, для відцифруванння процесів управління якістю потрібна повна автоматизація виробничих і бізнес-процесів технологічних лабораторій. Не всі суб'єкти господарювання належним чином оцінюють важливість та потрібність залучення інвестицій до впровадження лабораторних інформаційних менеджмент систем (LIMS),

хоч вони вирішують низку важливих для підприємства проблем, серед чого:вихід на світові ринки, що висуває вимоги до організації системи управління якістю за міжнародними нормами, тобто з обов'язковим використанням LIMS;дані про якість не враховуються в процесі оперативного прийняття рішень зі сторони виробничих служб, що неминуче призводить до втрат і зниження ефективності;без LIMS немає можливості зберігання даних з якості, забезпечення інформаційного шлейфу і прозорості процесу виробництва, збору даних з генеалогії продукції для наступного аналізу;невиправдано високі витрати часу персоналу на ввід даних і формування вихідної документації, замість того, щоб займатись аналізом для підвищення ефективності виробництва;недостатня достовірність даних з якості через людський фактор при передачі даних і розрахунках;невпорядкована методична база технологічних лабораторій.

Та ми переконані, що найбільш важливою причиною для впровадження такого інструменту як LIMS, є зважене рішення з переходу до політики постійного покращення процесів управління якістю продукції на протягом всього його життєвого циклу. Саме про це йдеться у міжнародних стандартах в сфері якості ISO 14001 (Система екологічного менеджменту), ISO 9001 (Система менеджменту якості) і ISO/IEC 17025 (Загальні вимоги до компетентності пробних та калібрувальних лабораторій).

Міжнародні стандарти по якості не встановлюють напряму стандарти якості окремих товарів або послуг, але визначають ефективність організації виробництва і управління, від яких власне і залежить якість продукції, тобто передбачають використання LIMS.

Так, до прикладу компанія Індасофт-Україна має великий досвід впровадження різного роду цифрових інструментів, які дозволяють убезпечити їх діяльність на нафтогазових, хімічних, металургійних виробництвах і цей досвід однозначно свідчить про найбільш ефективний шлях впровадження і LIMS як частини єдиної інформаційної управляючої системи підприємства. Такого роду єдина цифрова система управління має за ціль підвищення ефективності виробництва і зниження втрат за рахунок покращення прозорості ведення процесів. В основі завжди лежить єдиний ресурс всієї важливої виробничої інформації, а саме сервер даних реального часу. В рамках комплексної системи управління виробництвом LIMS є джерелом даних про якісні та кількісні результати випробувань і характеристик об'єктів контролю, надає можливості в режимі реального часу інтегрувати дані в диспетчерські системи і системи планування ресурсів підприємства (ERP).

Розширення і наступні задачі впровадження LIMS повинні охоплювати автоматизацію бізнес-процесів, саме центрів відцифрування, з метою посилення кібербезпеки суб'єкта господарювання в умовах воєнного стану (рис. 1).

Система управління інформаційною безпекою ISO/IEC 27001:2013 дає можливість впровадити найкращу практику для удосконалення захисту даних та усунення загрози порушення безпеки інформаційних систем. А ефективне управління безпекою інформаційних систем підтримується при регулярному моніторингу або аудиті системи [10]. Вплив ISO/IEC 27001:2013 на роботу компанії/організації можна спостерігати в різних сферах прояву бізнесу:

- репутація – встановлення процедури швидкого виявлення порушень інформаційної безпеки;
- зацікавлені сторони – визначення всіх внутрішніх та зовнішніх зацікавлених сторін, яких стосуються система управління інформаційною безпекою;
- відповідності – надає основу, яка допомагає керувати своїми юридичними та нормативними вимогами, змушує переглядати та повідомляти свої регулярні вимоги іншим зацікавленим сторонам;
- ризик управління – оцінювання ризики інформаційної безпеки, щоб була можливість виявити потенційні недоліки та реагувати [17].

Шляхи відцифрування:

- нову якість управління персоналом (тобто від слідкування всіх даних про персонал (освіта, атестація, підвищення кваліфікації), формування всієї звітності про персонал);
- управління обладнанням (ідентифікація лабораторного обладнання, контроль стану парку з обладнанням, процесів метрологічної повірки);
- управління реактивами, матеріалами і стандартними зразками (в тому числі, облік матеріалів, контроль їх надходження, зберігання і планування закупок);
- облік нормативної документації (в тому числі ведення реєстрів нормативних документів, від слідкування історії зміни документів, їх версії, контроль за терміном їх дії);
- внутрішньо лабораторний контроль (реалізує основні види внутрішньо лабораторного контролю якості шляхом оперативного контролю, контролю стабільності з використанням контрольних карт на основі контрольних зразків і контрольних процедур, між лабораторних порівняльних випробувань);
- розвиток функціональності у відповідності з вимогами замовника.

Рис. 1. Шляхи посилення кібербезпеки суб'єкта господарювання в умовах воєнного стану ***(розробка авторів)***

Розуміння сфери застосування стандарту ISO/IEC 27001 впливає на процес управління підприємством та даними про клієнтів. Також важливим питанням сьогодення є створення культури поінформованості про безпеку на підприємстві, яка є відповідною ISO/IEC 27001, зміцнюючи довіру клієнтів до здатності захищати їхні дані [2, с. 23].

В рамках забезпечення кібербезпеки в умовах воєнного стану та в ході подальшого відцифрування діяльності на мікрорівні, до базових та першочергових задач повинні відноситися, в основному, нова якість виробничих процесів технологічних лабораторій в частині:

- планування робіт (планування відбору проб при реалізації графіка аналітичного контролю (ГАК) у відповідності з вимогами галузевих стандартів, інструкцій і передових практик. Здійснення реєстрації надійшовши до лабораторії позапланових зразків через присвоєння їм унікальних ідентифікаційних номерів. Здійснення реєстрації заявок на проведення випробувань з метою від слідкування порядку проведення додаткових досліджень і взаємодії зацікавлених осіб);

- підготовка до вимірювання (розрахунок градуйованих характеристик з побудовою калібрувальних графіків. Побудова і затвердження градуйованої характеристики (ГХ). Автоматичний контроль за терміном дії ГХ. Проведення розрахункових значень визначного компонента за значенням аналітичного сигналу. Здійснення перевірки стабільності ГХ);

- відбір проб (реалізація процесу внесення інформації про проби (зразки) в систему шляхом присвоєння їй визначеного ідентифікатора. При здійсненні реєстрації зберігаються наступні параметри проби:

- *ідентифікаційні* (посилання на об'єкт аналізу, точка технологічної лінії, місце відбору, дослідні показники);

- *індивідуальні дані про відбір* (дата, час, метод відбору, використовуване обладнання);

- *параметри реєстрації* (час вводу, виконавець, унікальний ідентифікатор);

- *за необхідності внесення інших реєстраційних атрибутів зразків* (етикетування і штрих кодування зразків: розробка форми етикетки, печатка етикетки, ідентифікація проб етикеткою, пошук зразків по штрих-коду);

- проведення вимірювань (здійснення управління зразками: введення первинних вимірів; математична обробка даних, обрахунок результатів через алгоритм обробки результатів вимірів у відповідності з методикою випробувань);

- розрахунок результатів (оцінка наступності результатів вимірювань, визначення середнього значення і меридіани, дотримання алгоритму проведення досліджень, автоматизована оцінка результатів досліджень і метрологічних характеристик. Розподіл повноважень в частині прийняття рішення по затвердженню, корегуванню або відхиленню результатів. Затвердження результатів вимірювань: випуск зразків; авторизація результатів, після проведення авторизації фактичних результатів приймають участь у формуванні супровідних і звітних документів);

- оформлення результатів (формування протоколів випробувань: налаштування

бланків, формування перегляд і затвердження протоколу випробувань; експорт переліку протоколів. Формування звітності про результати: створення різних вихідних документів по встановленій формі регламентуючих органів; формування пакету документів, відповідно до датків паспорту якості; генерація різних звітів, збереження звітів різних форматів. Представлення даних про результати у вигляді таблиць і графіків для оцінки ефективності бізнес-процесів лабораторій).

Практикою підприємницької діяльності засвідчено, що до прикладу, Ramsomware являється найбільш розповсюдженою загрозою в ході реалізації бізнес-процесів. Ramsomware можна розділити на два основних типи – шифрувальники (криптори – "cryptoransomware") і блокувальники (блокери – "blockers"). Шифрувальники, потрапляючи до головного комп'ютера підприємства, кодують цінні файли: документи, фотографії, бази даних тощо. За розшифровку творці шифрів вимагають викуп – в середньому близько $ 300.

Види Ramsomware існують наступні:

1. Блокування екрану (показує загрозливе вікно й вказує, що комп'ютер користувача заблокований; зазвичай можна вирішити проблему без негативних наслідків).

2. Файлове шифрування (шифрує файли користувача, відображаючи вікно із загрозливим надписом; зазвичай не розшифровується, оскільки лише у кіберзлочинців є ключ дешифрування).

3. BootRamsomware (переписує MBR (головний завантажувальний запис), шифрує жорсткий диск, показує повідомлення про загрозу при завантажені системи; зазвичай не розшифровується, оскільки лише у кіберзлочинців є ключ дешифрування).

Загрози Ramsomware через вплив на бізнес полягають в наступному, а саме:

- часова втрата даних може повністю порушити надзвичайно важливі для бізнесу процеси (втрачені продажі, зниження продуктивності, значні витрати на відновлення системи, втрата репутації);

- постійні втрати даних ведуть до падіння конкурентоспроможності компанії, скорочення доходів від продажу у довгостроковій перспективі, порушення неперервного доступу до даних.

До головних проблем з якими зіштовхуються шифрувальники варто віднести:

- виплата викупу (це дорого, то ж заохочує злочинців створювати нових шифрувальників);

- відповідно до статистики 20 % тих, хто все ж заплатив злочинцям викуп, так і не отримав назад свої файли.

З вище вказаного, стає зрозумілим, що в рамках даної публікації є доречним з'ясування причин росту кількості злочинів. Так велика кількість різноманітних гаджетів призвела до того, що користувачами стають абсолютно непідготовлені люди. Не рідкість, коли в Інтернет виходять 3-4 річні діти. Основна проблема сьогодні – вкрай низька комп'ютерна грамотність населення. Розробники програмного забезпечення занепокоєні швидким виходом продукту на ринок. Проблема безпеки користувача, що купив продукт, їм нецікава. Кіберзагрози ближчі і реальніші, чим можна про них думати. Навіть акції протесту вже переходять у кіберпростір. Кібератаку можна здійснити на будь-який ресурс або цифровий сервіс, доступний 24 години на добу 365 днів у році, так же вільно, а головне – анонімно можна придбати кіберзброю або замовити атаку "під ключ". Цей факт безумовно сприяє розвитку тіньового, нелегального і злочинного ринку в кіберпросторі, адже в ньому вже є значні технічні можливості для "ідеального" злочину.

Чим викликане таке стрімке зниження комп'ютерної грамотності? Статистика засвідчує, що число персональних цифрових засобів у сім'ях незмінно росте. Рівень знань про кіберзагрози і способи захисту від них серед одних Інтернет-користувачів відсутній як такий, а у інших – помітно знижується. Як показують дослідження, користувачі віддають все більше перевагу мобільним засобам: 59 % респондентів сьогодні виходять в Інтернет переважно зі смартфона, а у 2012 році цей показник складав лише 36 %. Однак, саме в цьому сегменті нехтування захистом найбільш помітне.

Загрози при використанні смартфонів наступні: перехоплення і прослуховування розмов абонентів; фальсифікація розмов

абонентів з метою компроментації; дистанційне включення мікрофона і камери телефону й подальше несанкціоноване прослуховування розмов, фото- і відеозйомка; відправка повідомлень SMS і MMS, які містять віруси й "крадуть" інформацію; неавтоматизований доступ до мобільного телефону; шкідливе програмне забезпечення, здатне виконувати несанкціоновані абонентами віддалені команди; помилкові аутентифікації і авторизація призводять до несанкціонованого доступу до інформації, в т.ч. шляхом підробки унікального ідентифікатора абонента; помилкова базова станція, т.з. пастка IMSI, яка понижує стандартний рівень шифрування і полегшує перехоплення та прослуховування даних мобільних телефонів; втрата даних із втрачених та украдених мобільних телефонів; злам захисту модулів безпровідного високочастотного зв'язку малого радіусу дії Near Field Communication (NFC), вбудованих в мобільні телефони. Серед відомих атак на конфіденційну інформацію та персональні дані можна пригадати також: переписку Dentons, що була опублікована в Інтернеті; продаж особистої кореспонденції державних діячів в Україні.

Що стосується викрадення акаунтів співробітників компаній, то вони відбувається регулярно. Так, до прикладу, VAL.UA: 2 533 загальна кількість підданих атаці записів компанії; OSCHDBANK.UA: 33 загальна кількість підданих атаці записів компанії; PRIVATBANK.UA: 24 338 загальна кількість підданих атаці записів компанії; NAFTOGAZ.COM: 114 загальна кількість підданих атаці записів компанії; ZAPORIZHSTAL.COM: 293 загальна кількість підданих атаці записів компанії; UZ.GOV.UA: 1 381 загальна кількість підданих атаці записів компанії.

Заслуговує на увагу і світовий досвід кібератак. Так, зламаний поштовий сервер MOSSACKFONSECA, призвів в результаті до того, що стали доступними особисті дані акціонерів і директорів 214 000+ компаній в 200 країнах світу в 21 офшорній зоні; стала відомою власність 140 політиків та держслужбовців; "витік" документів за угодами на $ 2 трлн.Досвід зламаного поштового серверу DELOITTE зробив доступною конфіденційну інформацію Держдепартамента США, американських міністрів енергетики, внутрішньої безпеки та оборони; стали відомими дані 350 клієнтів, включно з 30 провідними компаніями, 4 міжнародними банками і 3 авіакомпаніями; відсутня двофакторна аутентифікаця.

В світлі таких злочинних кібератак звісно логічним є напрацювання різного роду видів захисту з метою убезпечення даних від їх перехоплення. Цей захист має бути:

- невидимим для сторонніх очей;
- мати канал безпечної пошти;
- e-mail сертифікат;
- e-mail сейф;
- e-mail шредер;
- центр кібербезпеки;
- шифрування листів і вкладень;
- захищений перегляд.

Досягатися кібербезпека на мікрорівні повинна шляхом:

- організації збору інформації про внутрішнє і зовнішнє середовище підприємства;
- проведення інформаційно-аналітичного дослідження клієнтів, бізнес-партнерів і конкурентів, інформаційного аудиту та інформаційного моніторингу на підприємстві, аналітичної обробки інформації;
- організацією системи інформаційного забезпечення рішень керівництва і власників підприємства;
- визначенням категорій інформації, що обробляється підприємством і відпрацюванням відповідних заходів по її захисту;
- дотримання відповідних режимів діяльності компанії;
- дотримання всіма співробітниками підприємства норм і правил роботи з інформацією з обмеженим доступом; своєчасне виявлення можливих каналів відтоку інформації з обмеженим доступом [4, с. 70].

Підсумовуючи вище сказане варто зазначити, що всім без виключення суб'єктам господарювання, особливо в умовах воєнного стану в Україні, варто дотримуватися принципів забезпечення кібербезпеки відповідно до статті 7 Закону України "Про основні засади забезпечення кібербезпеки України" [8], серед чого:

- відкритості, доступності, стабільності та захищеності кіберпростору, розвитку

мережі Інтернет та відповідальних дій у кіберпросторі;

- державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових і дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

- пропорційності та адекватності заходів кіберзахисту реальним і потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

- пріоритетності запобіжних заходів;

- міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях.

Державні інститути повинні здійснити розробку загальних принципів політики в сфері цифрової економіки, які торкаються всіх секторів економіки і спрямованих на досягнення стійкого економічного росту, а також аналізувати проблеми, що виникають в результаті цифрової трансформації, ризиків і ефектів цифровізації економіки, в тому числі, тих що пов'язані з забезпеченням громадян навиками та знаннями, які потрібні в умовах цифрової економіки [12].

На підприємствах повинні бути реалізовані наступні перераховані нижче вказівки в частині процедурного управління кіберінцидентами. А саме:

1. Розробити процедури обробки різних видів кіберінцидентів, включаючи: відмова інформаційної системи; зловмисний код; помилка в результаті неповних або неточних бізнес-даних; порушення конфіденційності та цілісності; зловживання інформаційними системами.

2. Додатково, до звичайних планів дій в аварійних обставинах, включити наступні процедури: аналіз та ідентифікація причин кіберінцидентів; локалізація; планування та впровадження корегуючи дій для попередження рецидивів (за потреби); зв'язок з тими, хто постраждав від інциденту або залучений до відновлення; звітність про дії тому, хто має відповідні повноваження.

3. Журнали аудиту та аналогічні докази повинні збиратися і за необхідності, захищатися з метою внутрішнього аналізу проблеми, представлення в якості судового доказу відносно потенційного порушення контрактних чи нормативних вимог, або у випадку громадянського, або кримінального позову; ведення переговорів про компенсацію від постачальників програмного забезпечення і послуг.

4. Діяльність з відновлення після порушення безпеки і відмов в коректній роботи системи повинна детально контролюватися з офіційним оформленням. Процедури повинні забезпечувати, щоб лише чітко ідентифікованому і автоматизованому персоналу дозволяється доступ до діючих систем й оперативних даних; всі прийняті аварійні дії були чітко задокументовані; про аварійні дії звітували керівництву і системно переглядалися; цілісність бізнес-систем та заходів безпеки підтверджувались з мінімальною затримкою [4, с. 74–75].

Окрім того, уряду України для переведення економіки на рейки кіберпростору в умовах воєнного стану потрібен новий рівень знань населення та соціальні мережі, які позбавлені ознак розваги. Соціальні мережі повинні розглядатися як робочий інструмент навчання суспільства потрібним навичкам та вмінням, можливим "містком спілкування" з державними структурами. Варто також зазначити, що загальносвітовий тренд розвитку теорії та практики кібербезпеки полягає в тому, що сформовані в різних країнах підрозділи кібербезпеки не повинні стати надбудовою над державним управлінням чи пак над бізнес-процесами на підприємствах. Підрозділи кібербезпеки повинні бути органічною частиною єдиного механізму, так би мовити "вписатись" в загальну стратегію розвитку держави як на макро-, так і на мезо- та мікрорівнях.

6. ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМКУ

В умовах воєнного стану та прискореного розвитку цифрових технологій, що націлені на

подолання кіберзагрози, що чиняться на всі сектори національної економіки, слід розглядати комплексно. Адже втрата коштів і витік інформації є лише одним сценарієм реалізації кібератаки. Під загрозою знаходяться об'єкти критичної інфраструктури країни, а саме: енергетичний сектор, транспортна система. З цих причин попередження та усунення загроз для цифрової трансформації кіберзахисту є основою конкурентоспроможності як підприємницької діяльності, так і держави загалом.

Сьогодні вже ні в кого не виникає сумнівів, що цифрова трансформація промисловості та врахування кібербезпеки в ході даної зміни є найбільш передовим шляхом до росту виробництва, покращення якості й зниження собівартості продукції безпечним шляхом, а також до підвищення ефективності використання інвестицій і покращення рейтингів конкурентоспроможності на ринку.

Перехід на принципи Четвертої промислової революції на засадах кібербезпеки означає перехід на цифровий формат всіх важливих виробничих і бізнес-процесів суб'єкта господарювання, формування єдиного інформаційного простору з вільним обміном даних між рівнями управління в реальному часі. Система управління якість на засадах кібербезпеки є однією з основних складових будь якого сучасного виробництва, особливо в сферах, де основні параметри сировини, напівфабрикатів і кінцевої продукції неможливо автоматично виміряти, а управління процесами ведеться за лабораторним аналізом.

Література

1. Вітер С., Світлишин І. Захист облікової інформації та кібербезпека підприємства. *Економіка і суспільство*. 2017. Вип. 11, С. 497–502.

2. Десятко А.М. *Кібергігієна. Кібербезпека. Безпека держави:* матеріали наукових семінарів. Київ: КНТЕУ. 2020. 101 с.

3. Дрозд І., Маковець О. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право*. 2020. № 5/3, С. 31–35.

4. Когут Ю.И. *Кибербезопасность цифровой экономики для собственников бизнеса.* Киев: ООО "Консалтингова компания "СИДКОН". 2019. 88 с.

5. Краус К.М., Краус К.М., Манжура О.В. *Електронна комерція та Інтернет-торгівля: навчально-методичний посібник*. К.: Аграр Медіа Груп. 2021. 454 с.

6. Краус К.М., Краус Н.М. (2019) *Ретроспектива і сучасність оподаткування в Україні та за кордоном:* монографія. К.: Аграр Медіа Груп.

7. Краус Н., Краус К. (2018) Цифровізація в умовах інституційної трансформації економіки: базові складові та інструменти цифрових технологій. *Інтелект XXI століття,* 1, С. 211–214.

8. Краус Н.М. (2019) *Інноваційна економіка в глобалізованому світі: інституціональний базис формування та траєкторія розвитку:* монографія. К.: Аграр Медіа Груп. 2019. 420 с.

9. Криворучко О.В., Сунічук О.М., Швець Д.В. (2020) Аналіз стану захищеності інформаційно-телекомунікаційних систем. *Управління розвитком складних систем,* 42, С. 56–62.

10. Про основні засади забезпечення кібербезпеки України: Закон України від 24.10.2020, підстава – 912-IX, Документ 2163-VIII.URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

11. Раєцький А. (2022) Кібербезпека бізнесу це не лише технічні заходи. *LegalIT group.*URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/.

12. Стратегії майбутнього Нова ера цифрової трансформації Центральна та Східна Європа. *DELOITTE.* URL: https://www2.deloitte.com/content/dam/Deloitte/ua/Documents/research/c500/CETop500_2016_ua.pdf.

13. ISO/IEC 27032:2012. Informationtechnology. Securitytechniques. Guidelinesforcybersecurity. *ISO.* URL: https://www.iso.org/standard/44375.html.

14. Kraus K., Kraus N., ShtepaO. *Teaching Guidelines for Digital Entrepreneurship.* Cracow University of Economics, Kiev-Cracow. 2021. URL: https://ted.uek.krakow.pl/output-1-teaching-guidelines/ (assessed 8 January 2022).

15. Kraus N., Kraus K., Osetskyi V. New quality of financial institutions and business management. *Baltic Journal of Economic Studies*. 2020. vol. 6, no. 1, pp. 59–66.

16. Manzhura O., Kraus K., Kraus N. Digitalization of Business Processes of Enterprises of the Ecosystem of Industry 4.0: Virtual-Real Aspect of Economic Growth Reserves. *WSEAS Transactions on Business and Economics,* 2021. vol. 18, P. 569-580. DOI: 10.37394/23207.2021.18.57.

References

1. Viter, S. and Svitlyshyn, I. (2017) Zakhyst oblikovoi informatsii ta kiberbezpeka pidpryiemstva [Protection of accounting information and cybersecurity of the enterprise], *Ekonomika i suspilstvo,* vol. 11, pp. 497–502.

2. Desiatko, A.M. (2020), *Kibergigiena. Kiberbezpeka. Bezpekaderzavy* [Cyberhygiene. Cybersecurity. State security], KNTEU, Kyiv, Ukraine.

3. Drozd, I. and Makovets, O. (2020) Kiberbezpeka yak faktor finansovoi bezpeky pidpryiemstva [Cybersecurity as a factor of financial security of the enterprise], *Ekonomika. Finansy. Pravo,* no. 5/3, pp. 31–35.

4. Kohut,Yu.I. (2019) *Kiberbezopasnost tsyfrovoi ekonomiki dlia sobstvennikov biznesa* [Cybersecurity of digital economy for business owners].LLC "Consulting company "SIDCON", Kyiv, Ukraine.

5. Kraus, K. M., Kraus, N. M. andManzhura, O.V. (2021), *Elektronna komertsiya ta Internet-torhivlya* [E-commerce and Internet commerce]**,** Agrar Media Hryp, Kyiv, Ukraine.

6. Kraus, K. M. and Kraus, N. M. (2019) *Retrospektyva I suchasnist opodatkuvannia Ukrainy ta za kordonom* [Retrospective and modern taxation in Ukraine and abroad], Agrar Media Hryp, Kyiv, Ukraine.

7. Kraus, N. M. and Kraus, K. M. (2018) Tsyfrovizatsiia v umovakh instytutsiinoi transformatsii ekonomiky: bazovi skladovi ta instrumenty tsyfrovykh tekhnolohii [Digitalization in the conditions of institutional transformation of economy: basic components and tools of digital technologies], *Intelekt XXI stolittia,* vol. 1, pp. 211–214.

8. Kraus, N. M. (2019), *Innovatsijna ekonomika v hlobalizovanomu sviti: instytutsional'nyj bazys formuvannia ta traiektoriia rozvytku* [Innovative economy in a globalized world: institutional basis of formation and development trajectory], Agrar Media Group, Kyiv, Ukraine.

9. 9. Kryvoruchko, O.V., Sunichuk, O.M. and Shvts, D.V. (2020), "Analysis of the state of security of information and telecommunication systems", *Uprzvlinniarozvytkomskladnykh system,* no. 42, pp. 56–62.

10.On the basic principles of cybersecurity in Ukraine: Law of Ukraine from 24 October 2020, basis on 912-IX, Document 2163-VIII,available at:https://zakon.rada.gov.ua/laws/show/2163-19#Text

11. Raietskyi, A. (2022), Kiberbezpeka biznesu tse ne lyshe tekhnichni zakhody [Business cybersecurity is not just about technical measures], *Legal IT group,*available at:https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi.

12. Strategies for the future. A new era of digital transformation Central and Eastern Europe, *DELOITTE,*available at:https://www2.deloitte.com/content/dam/Deloitte/ua/Documents/research/c500/CETop500_2016_ua.pdf.

13. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity", *ISO,*available at:https://www.iso.org/standard/44375.html.

14. Kraus, K., Kraus, N. and Shtepa, O. (2021) Teaching Guidelines for Digital Entrepreneurship, Cracow University of Economics, available at: https://ted.uek.krakow.pl/output-1-teaching-guidelines.

15. Kraus, N., Kraus, K. and Osetskyi, V. (2020) New quality of financial institutions and business management, *Baltic Journal of Economic Studies,* vol. 6, vol. 1, pp. 59–66.

16. Kraus, K. and Kraus N. (2021) Digitalization of Business Processes of Enterprises of the Ecosystem of Industry 4.0: Virtual-Real Aspect of Economic Growth Reserves, *WSEAS Transactions on Business and Economics*, vol. 18, pp. 569-580. DOI: 10.37394/23207.2021.18.57.

Abstract

KRAUS Kateryna, KRAUS Nataliia, SHTEPA Olena. Digital transformation of cyber security at the micro-level under martial status

The article describes the possible transformational processes of cybersecurity of business entities in martial law. Authors argue that the security criteria of modern digital entrepreneurship include the following mandatory facts: data must always be encrypted during storage and transmission; encryption must take place at the client level; only the client should have access to the encryption keys; actual data should not be transmitted through open mail channels; the company must control the storage of encrypted information and access keys to it.

A number of current external and internal threats to doing business are listed, including network intrusion, loss of devices with saved passwords, and encryption viruses. Main tasks of enterprises in terms of cybersecurity, namely: identification of potential threats to cybersecurity of enterprises and vulnerabilities; cyber incident prevention; neutralization or minimization of threats to information security of the enterprise.

Authors consider the impact of the information security management system ISO / IEC 27001: 2013 on the work of organizations. It has been found that this system provides an opportunity to implement best practices to improve data protection and eliminate the threat of security breaches of information systems.

The article focuses on the fact that in the framework of cybersecurity in martial law and in the further digitization of activities at the micro level, the basic and priority tasks should be mainly new quality of production processes of technological laboratories: planning work in accordance with requirements industry standards, guidelines and best practices; sampling into the system by assigning it a specific identifier; calculation of results and their design.

Entrepreneurial practice shows that, for example, Ramsomware is the most common threat in the implementation of business processes. Ramsomware is divided into two main types – cryptographers ("cryptoransomware") and blockers (blockers –"blockers"). Encryptors, when they get to the main computer of the enterprise, encrypt valuable files such as documents, photos, databases. Ramsomware's business threats include, for example, temporary data loss, which can completely disrupt critical business processes; constant data losses, leading to a decline in the company's competitiveness, reduced sales revenue in the long run, disrupted continuous access to data.

Authors of the article came to the conclusion that in the light of such criminal cyberattacks, of course, it is logical to develop various types of protection in order to protect data from their interception. This protection must be: invisible to the naked eye; have a secure mail channel; e-mail certificate; e-mail safe; e-mail shredder; cybersecurity center; encryption of letters and attachments; protected view.

Key words: *digital transformation, cybersecurity, micro level, cyber-attacks, cyber threats, cyber hygiene*

Стаття надійшла до редакції 30.06.2022 р.

Бібліографічний опис статті:

Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability.* 2022. № 3. С. 26-37.

Kraus K., Kraus N., Shtepa O. (2022) Digital transformation of cyber security at the micro-level under martial status. *Innovation and Sustainability*, no. 3, pp. 26-37.