DOI: 10.26565/2310-9513-2024-19-02
УДК 65.012.8(613)

ТЕНДЕНЦІЇ, ВИКЛИКИ ТА РІШЕННЯ ЦИФРОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЦЕНТРАЛЬНІЙ ТА СХІДНІЙ ЄВРОПІ

Лубенець Сергій Васильович
кандидат технічних наук, доцент
доцент кафедри міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, м. Харків, 61022
e-mail: s.lubenec@karazin.ua
Контактний тел.: 097-361-55-09
ORCID: https://orcid.org/0000-0003-1061-8763

Харченко Ігор Михайлович
кандидат технічних наук, доцент
доцент кафедри міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, м. Харків, 61022
e-mail: kharchenko@karazin.ua
Контактний тел.: 067-576-63-21
ORCID: https://orcid.org/0000-0002-1372-0408

Шедякова Тетяна Євгенівна
доцент кафедри міжнародного бізнесу та економічної теорії
Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, м. Харків, 61022
e-mail: shedyakova@karazin.ua
Контактний тел.: 050-500-09-23
ORCID: https://orcid.org/0000-0001-6492-4542

Розглянуто проблеми та напрями забезпечення ефективної міжнародної цифрової інформаційної безпеки в Центральній та Східній Європі (ЦСЄ), які ґрунтується на аналізі поточного стану, ключових тенденцій та викликів інформаційної безпеки даного регіону, з використанням актуальних звітних матеріалів міжнародних компаній, що спеціалізуються на проблематиці інформаційної безпеки та розробці відповідних комплексних інструментів для її забезпечення. Предметом дослідження в статті є питання забезпечення міжнародної цифрової інформаційної безпеки в ЦСЄ. Мета – полягає в дослідженні поточного стану, актуальних проблем та тенденцій міжнародної цифрової інформаційної безпеки на прикладі регіону Центральної та Східної Європи для пошуку напрямів підвищення її ефективності. Завдання: обробити та проаналізувати актуальну звітність, що стосується сучасного стану міжнародної цифрової інформаційної безпеки в регіоні ЦСЄ; дослідити ключові тенденції, виклики, проблеми та галузеві особливості цифрової інформаційної безпеки в ЦСЄ; проаналізувати підходи до оцінки поточного стану інформаційної безпеки міжнародних організацій регіону ЦСЄ та напрями її покращення. Використовується загальнонауковий метод системного аналізу – для визначення поточного стану, ключових тенденцій та викликів цифрової інформаційної безпеки, а також для дослідження перспективних напрямів підвищення її ефективності. Отримано такі результати: на основі обробки звітності, що стосуються сучасного стану міжнародної цифрової інформаційної безпеки в Центральній та Східній Європі, досліджено ключові тенденції, виклики та проблеми цифрової інформаційної безпеки регіону ЦСЄ. Визначено галузеві особливості цифрової інформаційної безпеки у сферах фінансових послуг, виробництва та роздрібної торгівлі даного регіону. Проаналізовано ефективні підходи до оцінки поточного стану інформаційної безпеки міжнародних організацій в ЦСЄ. Визначено можливі напрями її покращення та перспективи подальших наукових досліджень щодо даної тематики. Висновки: отримані результати дали можливість в цілому осмислити поточний ландшафт кібербезпеки в Центральній та Східній Європі. Виявлено позитивні імпульси у зосередженні компаній регіону на зміцненні кібербезпеки, що вимагає від них чіткої орієнтації в системі управління інформаційними ризиками. Виділено найбільш актуальні проблеми кібербезпеки ЦСЄ. Встановлено, що існуюче занепокоєння та реальна поведінка щодо інформаційної безпеки в ЦСЄ суперечать одне одному: більшість міжнародних компаній мають суттєвий дисонанс між побоюваннями інформаційних загроз та діями свого керівництва. Визначено, що одними з найбільших проблем організацій ЦСЄ щодо забезпечення інформаційної безпеки є низький рівень залучення до цього процесу їх керівників, а також нехтування обізнаністю працівників організацій про безпеку та кіберзахист. Встановлено, що організація віддаленої роботи зі створенням безпечного віддаленого робочого середовища залишається головним пріоритетом разом із постійною боротьбою зі шкідливими атаками зловмисного програмного забезпечення. Визначено, що використання хмарних технологій залишається особливо актуальним для міжнарод-

них компаній та установ ЦСЄ. Виявлено потребу у співпраці організацій з зовнішніми постачальниками відповідних рішень при забезпеченні інформаційної безпеки регіону. Встановлено, що у галузевому порівнянні існують деякі унікальні моменти щодо проблем інформаційної безпеки; серед таких особливих галузей ЦСЄ виділяються сфера фінансових послуг, виробництво та роздрібна торгівля. Запропоновано дієвий список контрольних питань щодо адекватної оцінка поточного стану інформаційної безпеки організації для визначення потенційних напрямів її покращення. Окреслено плани підвищення ефективності цифрової інформаційної безпеки організацій в регіоні ЦСЄ.

Ключові слова: *цифрова інформаційна безпека, кіберзахист, кібербезпека, кіберзагрози, Центральна та Східна Європа.*

Як цитувати: Лубенець С.В., Харченко І.М., Шедякова Т.Є. Тенденції, виклики та рішення цифрової інформаційної безпеки в Центральній та Східній Європі. *Вісник ХНУ імені В. Н. Каразіна. Серія«Міжнародні відносин. Економіка. Країнознавство. Туризм»*. 2024. № 19. С. 16–24. DOI: https://doi.org/10.26565/2310-9513-2024-19-02
In cites: Lubenets S., Harchenko I., & Shediakova T. (2024). Trends, challenges and solutions of digital information security in Central and Eastern Europe. *The Journal of V. N. Karazin Kharkiv National University. Series International Relations. Economics. Country Studies. Tourism*, (19), 16–24. https://doi.org/10.26565/2310-9513-2024-19-02 (in Ukrainian)

Постановка проблеми. В останні час продовжують виявлятися численні проблеми цифрової інформаційної безпеки в усьому світі. Минулі роки принесли безпрецедентні зміни в міжнародну бізнес-спільноту, підштовхнувши багато організацій до прискорення цифрової трансформації. Розширення можливостей співробітників працювати з дому та заміна звичайних операцій онлайн-альтернативами рекордно швидко розширили цифрову власність більшості компаній. Міжнародні компанії та установи намагаються адаптуватися до нових норм віддаленої та гібридної роботи, переосмислюючи свої бізнес-моделі та управлінські операції.

У цій ситуації актуальним є розгляд останніх тенденцій, існуючих викликів і проблем щодо нових інформаційних ризиків, підвищеної цифрової вразливості, інформаційної безпеки та кіберзагроз, з аналізом ефективних стратегій цифрової безпеки для їх наслідування компаніями та установами як в окремих регіонах, так і по всьому світу.

Аналіз останніх досліджень і публікацій. Проблеми та напрями забезпечення ефективної міжнародної інформаційної безпеки та кіберзахисту досліджувалися рядом науковців, аналітиків та профільних фахівців.

Зокрема, в статті [5] аналізуються питання поточного ландшафту та основні актуальні виклики кібербезпеки безпосередньо в регіоні Центральної та Східної Європи. Зроблено висновки, що країнам ЦСЄ в найближчий час може знадобитися посилити або оновити свої національні стратегії кібербезпеки, щоб адекватно реагувати на нові загрози, що розвиваються.

У роботі [1] розглянуто питання підвищення ефективності корпоративної інформаційної безпеки компаній та установ шляхом розробки універсальної консолідованої стратегії взаємодії служб інформаційної безпеки та IT на основі аналізу статистичних даних щодо регіону EMEA. В науковій статті [2] досліджуються проблеми та напрями забезпечення ефективної міжнародної інформаційної безпеки, які ґрунтується на аналізі поточного стану світової кіберзлочинності, існуючих основних напрямків глобальних кібератак і вироблення можливих методів та засобів протидії їм.

У той же час важливою є розробка комплексу питань щодо забезпечення ефективної міжнародної цифрової інформаційної безпеки, який би ґрунтувався на вивченні та аналізі актуальних експертних матеріалів, що стосуються сучасного комплексу питань міжнародної інформаційної безпеки. У тому числі, на звітних матеріалах авторитетних міжнародних компаній, які спеціалізуються як на проблематиці міжнародної цифрової інформаційної безпеки, так і на розробці відповідних технічних інструментів для її забезпечення.

Мета статті, завдання дослідження. Метою роботи є дослідження поточного стану, актуальних проблем та тенденцій міжнародної цифрової інформаційної безпеки на прикладі регіону Центральної та Східної Європи (ЦСЄ) для пошуку напрямів підвищення її ефективності.

Відповідно до мети дослідження в роботі були поставлені та вирішувалися наступні *завдання*:

– обробити та проаналізувати актуальну звітність, що стосується сучасного стану міжнародної цифрової інформаційної безпеки в регіоні ЦСЄ;

– дослідити ключові тенденції, виклики, проблеми та галузеві особливості цифрової інформаційної безпеки в ЦСЄ;

– проаналізувати підходи до оцінки поточного стану інформаційної безпеки міжнародних організацій регіону ЦСЄ та напрями її покращення.

Для вирішення поставлених завдань у даній роботі був проведений аналіз опублікованих результатів та висновків IT Cloud Security Survey [6], що стосуються дослідження поточної проблематики та стратегії інформаційної безпеки й кіберзахисту міжнародних організацій на основі опитування представників малого, середнього та великого біз-

несу, зокрема регіону Центральної і Східної Європи.

Основні результати дослідження. Дослідження, проведені компанією IT Cloud Security Survey у Центральній та Східній Європі за дорученням IDC та Microsoft дали можливість оцінити стан кібербезпеки та управління інформаційними ризиками в 1500 компаній у Польщі, Чехії, Угорщині, Румунії та Греції. У рамках дослідження були опитані IT-директори та IT-менеджери, фахівці з IT-безпеки, CISO та особи, які приймають бізнес-рішення.

Результати проведеного дослідження забезпечують можливість визначити поточний стан, виклики та погляди на тенденції цифрової інформаційної безпеки в ЦСЄ, вияснити існуючі способи оцінки поточних стратегій безпеки; ознайомитися з історіями успіху тих міжнародних компаній, які зміцнили свою інформаційну безпеку; перейняти ті рішення та рекомендації щодо забезпечення інформаційної безпеки, які можуть допомогти повторити ці успіхи іншим компаніям та установам.

Крім того, отримані відповіді дали можливість в цілому осмислити поточний ландшафт кібербезпеки, який розвивається відповідно до нових методик управління та роботи з інформацією, що вимагають підходів з поєднанням пильності та гнучкості цих процесів. При цьому одним з основних факторів управління ризиками інформаційної безпеки та кіберзахисту є розгортання інструментів і процесів, які дозволяють співробітникам залишатися зосередженими на роботі, а не турбуватися про безпеку. І це дозволяє командам інформаційної безпеки випереджати загрози, а не наздоганяти їх, ліквідовуючи потім ті чи інші негативні наслідки. Хмарні рішення будуть особливо актуальними для міжнародних компаній та установ, які прагнуть залишатися гнучкими у своєму підході щодо цифрової інформаційної безпеки.

Результати проведених досліджень свідчать про позитивний імпульс у правильному напрямку, оскільки багато міжнародних компаній прискорюють зосередження на зміцненні кібербезпеки. Хоча підтримка інформаційної безпеки – це завжди безперервний процес, і він не буде ефективним без комплексної стратегії [1]. Бізнес-лідери та управлінці, які є проактивними у своєму підході та тримають себе в курсі розвитку поточної ситуації щодо інформаційної безпеки, завжди матимуть найкращу підготовку, щоб залишатися попереду у цьому процесі.

Зростання складності інформаційних загроз. Як показує щорічний звіт Microsoft Digital Defense Report [3], кіберзагрози стають все більш складними. Протягом останнього року зловмисники швидко підвищили рівень витонченості, використовуючи методи, які ускладнюють виявлення інформаційних загроз навіть найбільш сучасними інструментами кіберзахисту. Якщо раніше кіберзлочинці зосереджувалися на атаках з використанням зловмисного програмного забезпечення, то тепер вони починають надавати перевагу фішинговим атакам (~70%), дедалі швидше видозмінюючи їх, щоб уникнути виявлення.

При цьому в більшості випадків метою фішингових атак є отримання облікових даних користувачів. Ці кібератаки можуть відбуватися звідки завгодно, що робить дану небезпеку глобальною загрозою, якій потрібно протистояти за допомогою глобального досвіду.

Виклики та проблеми цифрової інформаційної безпеки організацій ЦСЄ. Оскільки міжнародні компанії визнають неминучі інформаційні загрози, їхні страхи щодо інформаційної безпеки справедливо віддзеркалюють глобальний ландшафт кіберзагроз. Порушення безпеки є головним занепокоєнням для більшості підприємств, тоді як поведінка співробітників також викликає серйозне занепокоєння. Аналогічно як інформаційна безпека викликає занепокоєння серед всієї спільноти ЦСЄ, підприємства та установи цього регіону також продовжують сприймати кібербезпеку як складну проблему. Це вимагає від них чіткої орієнтації в системі управління інформаційними ризиками.

Багато організацій та підприємств у регіоні ЦСЄ вже з меншим оптимізмом дивляться в майбутнє, коли думають про кібербезпеку, оскільки понад дві третини міжнародних компаній вже зіткнулися з низкою проблем інформаційної безпеки. Крім потенційних фінансових втрат, слід виділити наступні найбільші актуальні проблеми кібербезпеки для регіону ЦСЄ:

– наслідки можливого порушення інформаційної безпеки (55%);

– погана поінформованість співробітників (50%);

– складність інформаційної безпеки (36%);

– атаки програм-вимагачів/шкідливих програм (38%);

– вартість охорони (25%);

– застарілі процеси та системи безпеки (30%);

– застосування узгоджених засобів контролю безпеки локально та в хмарі (27%);

– жодних проблем інформаційної безпеки не виявлено (23%).

Однак вражаючим є той факт, як існуюче занепокоєння та реальна поведінка щодо інформаційної безпеки суперечать одне одному. Незважаючи на визнання нависаючих кіберзагроз і проблем з інформаційною безпекою, результати досліджень показують, що більшість міжнародних компаній мають приголомшливий дисонанс між побоюваннями інформаційних загроз та діями свого керівництва:

– 58% підприємств не мають комплексної стратегії інформаційної безпеки;

– більшість загалом задоволені інформаційною безпекою своїх IT-систем (86%).

Що стосується базової гігієни кібербезпеки, то більше половини організацій ЦСЄ (54%) проводять тренінги з питань безпеки лише на разовій основі, а ще 15% – не проводять їх взагалі. При цьому 11% підприємств не оцінюють безпеку при розгляді нових ІТ-рішень, а 9% взагалі не мають визначеної стратегії інформаційної безпеки.

Наступною проблемою організацій ЦСЄ щодо забезпечення інформаційної безпеки є нехтування обізнаністю їх працівників про безпеку та кіберзахист. До того ж компанії, які прагнуть оновити свої стратегії безпеки, здебільшого планують інвестувати в нові технології, не звертаючи уваги на оптимізацію вже наявних процесів: 61% планують додати нові технології до свого арсеналу безпеки. Проте лише 38% планують провести кампанію з підвищення обізнаності співробітників щодо інформаційної безпеки.

Однак підприємствам слід використовувати техноцентричний підхід, лише якщо особи, які приймають рішення, чітко розуміють, яку цінність технологічні інвестиції можуть принести їхнім зусиллям у сфері безпеки. Найважливішим першим кроком у цьому процесі є проведення аудиту та оцінки ризиків, щоб виявити специфічні інформаційні проблеми. На основі цієї фундаментальної інформації можна побудувати стратегію інформаційної безпеки, яка охоплює всі основи – від впровадження нових технологій і автоматизації процесів до навчання співробітників.

Ще однією проблемою ефективного забезпечення інформаційної безпеки організацій в регіоні ЦСЄ є низький рівень залучення до цього процесу їх керівників. У той час як за останній рік 41% компаній збільшили свою прихильність до інформаційної безпеки, лише 36% відповідним чином збільшили свої бюджети безпеки, що свідчить про неспроможність у деяких випадках узгодити наміри з відповідними інвестиціями. Це може бути викликано тим фактом, що планування інформаційної безпеки в основному делеговано ІТ-спеціалістам і CISO, і лише 25% компаній та установ залучають до цього процесу осіб, які приймають управлінські рішення.

Однак чітке розуміння бізнес-цінності цифрової інформаційної безпеки на рівні менеджменту має вирішальне значення для забезпечення того, щоб команди, які зменшують інформаційні ризики, мали бюджет, необхідний для захисту організації та забезпечення безперервності бізнесу та управління.

Певні пріоритеті у забезпеченні цифрової інформаційної безпеки продовжує визначати віддалена робота. Починаючи з 2020 року бізнес-середовище та діяльність установ віртуалізувалися надзвичайно швидкими темпами, завдяки чому безпечна віддалена робота, керування доступом співробітників і внутрішні інформаційні загрози стали головними пріоритетами для організацій у всьому регіоні ЦСЄ. Оскільки країни об'єднали зусилля у боротьбі зі спалахом вірусу та запровадили загальнонаціональні карантинні заходи, компанії та установи були підштовхнуті до використання дистанційних або гібридних моделей роботи.

В даний час створення безпечного віддаленого робочого середовища залишається головним пріоритетом разом із постійною боротьбою зі шкідливими атаками зловмисного програмного забезпечення. Для розуміння важливості цих питань, наведемо основні пріоритети інформаційної безпеки для підприємств ЦСЄ на наступні 6-18 місяців:

– атаки шкідливого програмного забезпечення (67%);

– безпечна віддалена робота (65%);

– моніторинг кібербезпеки в реальному часі (57%);

– управління доступом співробітників (47%);

– виявлення внутрішньої загрози (46%).

При цьому, найбільш ефективними рішеннями цифрової інформаційної безпеки, які використовуються підприємствами ЦСЄ, є:

– безпечний віддалений доступ (79%);

– керування доступом (72%);

– захист кінцевої точки (69%).

Таким чином, безпечний віддалений доступ замінює вічний номер один – захист кінцевих точок – як найпоширеніше рішення інформаційної безпеки, яке безпосередньо відображає те, як організації долали виклики, створені глобальною пандемією. Природа найпопулярніших рішень безпеки свідчить про те, що організації в ЦСЄ визнали додаткові заходи безпеки, необхідні для розміщення робочих місць в Інтернеті, одночасно захищаючи свою цифрову власність.

Важливим аспектом у забезпеченні цифрової інформаційної безпеки організацій та установ залишається використання хмарних технологій. На запитання, чому хмарні рішення безпеки вважаються найбезпечнішими, представники компаній-користувачів такими технологіями вказали наступні їх переваги: наявність глобальної експертизи (64%), достатній позитивний досвід використання хмарних технологій (62%), доступність ефективних функцій безпеки (49%), сумісність хмарної та локальної інфраструктур (45%).

Локальні рішення існують уже понад 30 років, що пояснює, чому більшість міжнародних компаній та установ високо цінують сумісність інфраструктури, дотримуючись таких рішень. Проте все більше й більше організацій обирають саме хмарні рішення безпеки. Особливо тому, що вони надають їм доступ до глобального досвіду та досвіду великих провайдерів. Хоча компанії визнають, що як хмарні, так і локальні пропозиції забезпечують хорошу взаємодію з клієнтами, важливо пам'ятати, що безпека є

глобальною загрозою, і з нею потрібно боротися настільки ж далекосяжно.

Потреба у співпраці при забезпеченні інформаційної безпеки. Проведені дослідження встановили, що більше третини компаній ЦСЄ (36%) вважають питання цифрової інформаційної безпеки та її забезпечення надто складною темою. Серед уявних складнощів вказується, що кібербезпека – це технічний аспект, який вимагає спеціальний знань співробітників та ІТ-спеціалістів компанії і є занадто складним для ефективного планування та реалізації.

Однак, слід зазначити, що вирішення проблем забезпечення інформаційної безпеки значно спрощується, коли організація знайшла правильні інструменти та партнерів. Співпраця з зовнішніми постачальниками відповідних рішень щодо кіберзахисту може забезпечити організації глобальну експертизу з кібербезпеки, знайти найкращі рішення для інформаційних потреб, отримати консультаційну підтримку та відповідні вказівки щодо розробки та реалізації стратегії інформаційної безпеки організації.

Галузеві особливості щодо інформаційної безпеки в ЦСЄ. Підприємства та установи різних розмірів і сфер діяльності регіону ЦСЄ в цілому мають схоже сприйняття кіберзагроз та підходів до їх управління. Однак у галузевому порівнянні все ж висвітлюються деякі унікальні моменти. Серед таких особливих галузей виділяються сфера фінансових послуг, виробництво та роздрібна торгівля.

Так, характерним для галузі фінансових послуг є наступне:

– витрати на інформаційну безпеку потрапили до трійки найбільших викликів безпеці (27%);

– безпечна віддалена робота є основним пріоритетом на наступні 6-18 місяців (67%);

– на запитання про кроки, необхідні для підвищення інформаційної безпеки, розуміння його бізнес-цінності потрапило до трьох найпоширеніших відповідей (42%).

Щодо виробництва, то це галузь, де:

– компанії перевершили міжгалузеві середні показники, оскільки 33% з них посилили зобов'язання щодо інформаційної безпеки;

– 69% респондентів назвали навчання співробітників ключовим кроком у зміцненні інформаційної безпеки;

– атаки програм-вимагачів і шкідливих програм є найбільшою проблемою для інформаційної безпеки (39%).

Нарешті, для роздрібної торгівлі характерним виявилося наступне:

– більша довіра міжнародним хмарним провайдерам, ніж місцевим і регіональним компаніям, коли йдеться про інформаційну безпеку;

– 26% респондентів заявили, що не стикалися з проблемами безпеки протягом минулого року;

– 44% заявили, що планують використовувати гібридні хмарні рішення протягом наступних двох років.

Оцінка поточного стану та напрями покращення інформаційної безпеки міжнародної організації в регіоні ЦСЄ. Дозволити міжнародним компаніям безпечно розвиватися та захищати свої організації від кібератак є головним питанням спеціалістів з інформаційної безпеки та ІТ. Розуміння обсягу організаційних цифрових активів і встановлення основних правил є ключовими, оскільки часто відсутність елементарної гігієни безпеки в будь-якій даній екосистемі продовжує давати змогу кіберзлочинцям використовувати добре відомі вразливості або їх нові варіанти.

При цьому інформаційна безпека може створити цінність бізнесу. Тому для організації важливими є адекватна оцінка свого поточного стану інформаційної безпеки, визначення потенційних напрямів її покращення для вжиття ефективних заходів для створення та розгортання відповідної стратегії. Для того, щоб організація могла провести таку оцінку і визначити, де вона перебуває на шляху забезпечення інформаційної безпеки, і намітити наступні кроки в цьому напрямі, можна запропонувати наступний дієвий список контрольних питань [4]:

1. Чи використовує організація багатофакторну автентифікацію? Паролі співробітників можуть бути легко зламані. Запровадження другої форми автентифікації при вході в корпоративну інформаційну систему є одним із основних принципів кібергігієни для захисту організації.

2. Чи зберігає організація свої дані в безпеці? Втрата чи пошкодження даних може порушити роботу організації, тому вони повинні мати багаторівневий захист.

3. Чи створюється резервна копія важливих даних організації? Програмне забезпечення-вимагач є одним із найприбутковіших каналів доходу для кіберзлочинців, оскільки вони шифрують організаційні дані та просять гроші за їх розшифровку. Тому рекомендується зберігайте три резервні копії власних даних у двох різних типах сховищ і принаймні одну резервну копію за межами корпоративної системи.

4. Чи контролює організація доступ співробітників до інформації? Організація повинна захищати свою внутрішню мережу та контролювати доступ, оскільки співробітники використовують персональні пристрої для доступу до інформації компанії.

5. Ви автоматизована робота з адміністрування корпоративної інформаційної системи? Автоматизація є критично важливою для підтримки безпеки та ІТ-команд, оскільки забезпечує можливість оперативно виявляти інформаційні загрози та реагувати на них.

6. Чи регулярно організація оцінює свої заходи інформаційної безпеки? Якщо в організації є стра-

тегія безпеки, вона повинна регулярно переглядатися, щоб відповідні стратегії управління ризиками відповідали траєкторії зростання. Кожного разу, коли організація впроваджує нові технології чи робочі моделі або розширюєте свою команду, слід переконуватися, що заходи інформаційної безпеки охоплюють усі аспекти нового ландшафту.

7. Чи володіють співробітники організації питаннями інформаційної безпеки? Поєднання вбудованої інформаційної безпека з висококваліфікованими співробітниками є досить важливим. Як показали дослідження, програма інформаційної безпеки в Центральній та Східній Європі зосереджена на віддаленій роботі та пов'язаних із нею проблемах, виводячи цифрову поведінку співробітників організацій на перший план. Це викликано тим, що близько 50% підприємств найбільше занепокоєні як навмисними, так і ненавмисними людськими помилками, коли йдеться про загрози інформаційній безпеці. Одночасно справедливим є те, що оскільки компанії поспішають запроваджувати нові технології, вони стикаються з нестачею кваліфікації співробітників. Проведене опитування стану цифрових навичок у ЦСЄ показало, що на даний час лише 3,5% працівників компаній ЦСЄ повністю відповідають потребам у цих навичках [7].

Отже, питання підвищення кваліфікації співробітників є досить критичним. Підвищення кваліфікації – це не лише забезпечення безпеки функціонування компаній та установ. Адже гарантія того, що кожен співробітник компанії володіє необхідними цифровими навичками, дозволить її інвестиціям у технології реалізувати свій потенціал, підвищити продуктивність бізнесу та оптимізувати управлінські процеси. Підвищення кваліфікації співробітників після впровадження нових рішень є обов'язковим, щоб уникнути невідповідного використання технологій. Постійні навчальні програми щодо безпечних методів роботи допоможуть зменшити ризики, які виникають через помилки співробітників.

8. Чи приймаються зважені рішення щодо інформаційної безпеки? Незважаючи на те, що попередні питання дають змогу добре оцінити поточний стан безпеки та вжити певних заходів усередині організації, життєво важливо залучати зовнішніх експертів, коли йдеться про усунення складніших прогалин або оптимізацію існуючих процесів.

За результатами проведених досліджень можна визначити ключові напрями та плани покращення стану інформаційної безпеки організацій в регіоні ЦСЄ. В першу чергу, одним із основних кроків, які організації ЦСЄ можуть зробити для зменшення кіберризиків, є підвищення обізнаності співробітників щодо питань інформаційної безпеки. Понад дві третини (68%) планують запровадити ініціативи з навчання та підвищення кваліфікації своїх співробітників, тоді як 56 відсотків мають намір підвищити лише їх технічні знання.

Більшість компаній (83%) також визнають важливість оцінки інформаційної безпеки під час придбання нових IT-рішень. 36% компаній вже збільшили свій бюджет щодо забезпечення інформаційної безпеки за останні два роки. Нарешті, майже половина компаній (47%) планують створити власну стратегію інформаційної безпеки або розширити поточну.

Компанії, які готові зробити свою систему безпеки ефективнішою, одночасно зменшуючи операційні витрати та дозволяючи керівництву повернутися до досягнення своїх бізнес-цілей, можуть використовувати вбудовані інтелектуальні рішення безпеки від партнерів, які працюють в регіоні ЦСЄ і спеціалізуються на розробці відповідних технічних інструментів для захисту користувачів, даних, пристроїв та програм, забезпечуючи ефективне управління ризиками.

Висновки та перспективи подальших розробок. Проведені дослідження дали можливість виявити ключові тенденції цифрової інформаційної безпеки в Центральній та Східній Європі. Не дивлячись на очевидну стурбованість щодо зловмисного програмного забезпеченням, програмам-вимагачів та порушеннями інформаційної безпеки, більше половини організацій ЦСЄ не мають комплексної стратегії безпеки. Однак, незважаючи на це, 86% вказують на задоволення своїми заходами інформаційної безпеки. Помилкове відчуття безпеки часто призводить до відсутності ефективних захисних заходів, в той час як кібератаки стають все більш витонченими та швидко поширюються, залишаючи під загрозою будь-які компанії та установи незалежно від їхнього розміру та розташування. Інформаційна небезпека є глобальною загрозою, тому кіберризики слід розглядати як критичну загрозу, якою можна успішно керувати за допомогою належних розумних практик.

У цілому на основі проведених досліджень можна констатувати, що поточні стратегії інформаційної безпеки більшості організацій ЦСЄ не в змозі імітувати їхній зростаючий цифровий слід. У той же час, більшість організацій ЦСЄ прагнуть посилити свою інформаційну безпеку. Безпечна віддалена робота, поведінка працівників і можливі порушення ними безпеки тепер є головним пріоритетом для міжнародних компаній та установ разом із захистом від зловмисного програмного забезпечення.

Таким чином, результати та висновки даної статті, засновані на аналізі проблематики цифрової інформаційної безпеки на основі звітності щодо кіберзагроз в Центральній та Східній Європі, покликані сприяти пошуку ефективних і дієвих шляхів та інструменті для підвищення ефективності інформаційної безпеки в даному регіоні.

Основні напрямки подальших досліджень. У той час як компанії ЦСЄ прагнуть забезпечити стабільність та розвиток своєї діяльності, кіберзлочинці наполегливо продовжують свою підривну діяльність в даному регіоні й по всьому світу, захоплюючи як глобальних гравців, так і місцеві організації. У зв'язку з цим міжнародні компанії та установи вимушені оновлювати заходи цифрової інформаційної безпеки, щоб захистити свою діяльність від зловмисних атак сторонніх осіб або помилок власних співробітників. У зв'язку з цим актуальними є подальші дослідження щодо наступних ключових питань, які покликані забезпечити безперервність діяльності та зростання організацій Центральної та Східної Європи:

– забезпечення безперешкодного віддаленого доступу, щоб кожен співробітник міг безпечно працювати з будь-якого місця та на будь-якій платформі;

– використання повного набору хмарних рішень, уніфікованих для співробітників, пристроїв, програм і даних;

– розширення можливості команди співробітників організації шляхом її навчання для максимально ефективного використання наявних інструментів;

– залучення експертів для швидкого усунення прогалин в цифровій інформаційній безпеці.

СПИСОК ЛІТЕРАТУРИ

1. Лубенець С.В., Харченко І.М., Новікова Л.В. Проблеми побудови консолідованих стратегій управління корпоративною інформаційною безпекою в регіоні EMEA. *Вісник Харківського національного університету імені В.Н. Каразіна. Сер. «Міжнародні відносини. Економіка. Країнознавство. Туризм».* 2021. Вип. 14. С. 24–34. https://doi.org/10.26565/2310-9513-2021-14-03

2. Лубенець С.В., Харченко І.М., Павленко Є.П. Актуальні проблеми міжнародної інформаційної безпеки. *Вісник Харківського національного університету імені В.Н. Каразіна. Сер. «Міжнародні відносини. Економіка. Країнознавство. Туризм».* 2023. Вип. 17. С. 42–48. https://doi.org/10.26565/2310-9513-2023-17-04

3. 2023 Microsoft Digital Defense Report : web site. URL: https://www.microsoft.com/en-us/security/business/security-intelligence-report (date of the application: 13.02.2024).

4. Evaluate your Zero Trust security posture : web site. URL: https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard%3aprimaryr1 (date of the application: 13.02.2024).

5. Marek Grzegorczyk. A secure digital world: Protecting CEE's digital frontiers : web site. URL: https://emerging-europe-com.translate.goog/news/a-secure-digital-world-protecting-cees-digital-frontiers/?_x_tr_sl=en&_x_tr_tl=uk&_x_tr_hl=uk&_x_tr_pto=sc (date of the application: 13.02.2024).

6. The 2023 Cloud Security Survey : web site. URL: https://www.manageengine.com/log-management/cloud-security/2023-cloud-security-survey-report.html (date of the application: 13.02.2024).

7. Up-skilling is crucial to maintain digital transformation acceleration, a new Central and Eastern Europe survey finds : web site. URL: https://news.microsoft.com/europe/features/up-skilling-is-crucial-to-maintain-digital-transformation-acceleration-a-new-central-and-eastern-europe-survey-finds/ (date of the application: 13.02.2024).

Стаття надійшла до редакції 22.02.2024
Стаття рекомендована до друку 25.03.2024

Serhii Lubenets, Candidate of Technical Sciences (Ph. D.), Associate Professor, Associate Professor of the Department of International Relations, International Information and Security, V.N.Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, Ukraine, 61022, e-mail: s.lubenec@karazin.ua, Phone number: 097-361-55-09, ORCID: https://orcid.org/0000-0003-1061-8763

Igor Harchenko, Candidate of Technical Sciences (Ph. D.), Associate Professor, Associate Professor of the Department of International Relations, International Information and Security, V.N.Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, Ukraine, 61022, e-mail: kharchenko@karazin.ua, Phone number: 067-576-63-21, ORCID: https://orcid.org/0000-0002-1372-0408

Tetiana Shediakova, Associate Professor of the Department of the International Business and Economic Theory, V.N.Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, Ukraine, 61022, e-mail: shedyakova@karazin.ua, Phone number: 050-500-09-23, ORCID: https://orcid.org/0000-0001-6492-4542

TRENDS, CHALLENGES AND SOLUTIONS OF DIGITAL INFORMATION SECURITY IN CENTRAL AND EASTERN EUROPE

The problems and directions of ensuring effective international digital information security in Central and Eastern Europe (CEE) are considered, which are based on the analysis of the current state, key trends and challenges of information security in this region, using current reporting materials of international companies specializing in information security issues and development of appropriate complex tools for its provision. The subject of research in the article is the issue of ensuring international digital information security in the CEE. The goal is to study the current state, current problems and trends of international digital information security on the example of the region of Central and Eastern Europe in order to find ways to improve its effectiveness. Task: to process and analyze current reporting related to the current state of international digital information security in the CEE region; to explore the key trends, challenges, problems and industry specificities of digital information security in CEE; analyze approaches to assessing the current state of information security of international organizations in the CEE region and directions for its improvement. The general scientific method of system analysis is used - to determine the current state, key trends and challenges of digital information security, as well as to research promising directions for improving its effectiveness. The following results were obtained: based on the processing of reports concerning the current state of international digital information security in Central and Eastern Europe, key trends, challenges and problems of digital information security in the CEE region were investigated. The sectoral features of digital information security in the spheres of financial services, production and retail trade of this region have been determined. Effective approaches to assessing the current state of information security of international organizations in the CEE have been analyzed. Possible directions for its improvement and prospects for further scientific research on this topic are determined. Conclusions: the obtained results made it possible to understand the current landscape of cyber security in Central and Eastern Europe in general. Positive impulses have been identified in the focus of companies in the region on strengthening cyber security, which requires them to have a clear orientation in the information risk management system. The biggest current problems of CEE cyber security are highlighted. It has been established that the existing concern and actual behavior regarding information security in CEE contradict each other: most international companies have a significant dissonance between the fears of information threats and the actions of their management. It was determined that one of the biggest problems of CEE organizations in ensuring information security is the low level of involvement of their managers in this process, as well as the neglect of the awareness of the employees of the organizations about security and cyber protection. Establishing a secure remote work environment remains a top priority, along with the ongoing fight against malicious malware attacks. It was determined that the use of cloud technologies remains particularly relevant for international companies and CEE institutions. The need for cooperation between organizations and external suppliers of relevant solutions in ensuring the information security of the region was revealed. It has been established that there are some unique points regarding information security issues in the industry comparison; financial services, manufacturing and retail trade stand out among such CEE special industries. An effective list of control questions regarding an adequate assessment of the current state of the organization's information security to determine potential directions for its improvement is proposed. Plans for improving the effectiveness of digital information security of organizations in the CEE region are outlined.

Keywords: digital information security, cyber protection, cyber security, cyber threats, Central and Eastern Europe.

REFERENCES

1. Lubenets S., Harchenko I., Novikova L. (2021) Problemy pobudovy konsolidovanyh strategij upravlinnja korporatyvnoju informacijnoju bezpekoju v regioni EMEA [Problems of Building Consolidated Corporation Strategies for Corporate Information Security Management in the EMEA Region]. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations. Economics. Country Studies. Tourism*, vol. 14, 24–34. (in Ukrainian). https://doi.org/10.26565/2310-9513-2021-14-03

2. Lubenets S., Harchenko I., Pavlenko Y. (2023) Aktual'ni problemy mizhnarodnoi' informacijnoi' bezpeky [Current Problems of International Information Security]. *The Journal of V. N. Karazin Kharkiv National University. Series: International Relations.*

Economics. Country Studies. Tourism, vol. 17, 42–48. (in Ukrainian). https://doi.org/10.26565/2310-9513-2023-17-04

3. 2023 Microsoft Digital Defense Report. Available at: https://www.microsoft.com/en-us/security/business/security-intelligence-report (accessed 13.02.2024).

4. Evaluate your Zero Trust security posture. Available at: https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard%3aprimaryr1 (accessed 13.02.2024).

5. Marek Grzegorczyk. A secure digital world: Protecting CEE's digital frontiers. Available at: https://emerging--europe-com.translate.goog/news/a-secure-digital-world-protecting-cees-digital-frontiers/?_x_tr_sl=en&_x_tr_tl=uk&_x_tr_hl=uk&_x_tr_pto=sc (accessed 13.02.2024).

6. The 2023 Cloud Security Survey. Available at: https://www.manageengine.com/log-management/cloud-security/2023-cloud-security-survey-report.html (accessed 13.02.2024).

7. Up-skilling is crucial to maintain digital transformation acceleration, a new Central and Eastern Europe survey finds. Available at: https://news.microsoft.com/europe/features/up-skilling-is-crucial-to-maintain-digital-transformation-acceleration-a-new-central-and-eastern-europe-survey-finds/ (accessed 13.02.2024).

The article was received by the editors 22.02.2024
The article is recommended for printing 25.03.2024