Список використаних джерел:

1. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015.
2. Горбенко І. Д. Симетричний блоковий шифр «Калина» – новий національний стандарт України / І. Д. Горбенко, Р. В. Олійников, О. В. Казимиров, В. І. Руженцев, О. О. Кузнєцов, Ю. І. Горбенко, О. В. Дирда, В. І. Долгов, А. І. Пушкарьов, Р. І. Мордвінов // Радіотехніка. – 2015. – Вип. 181. – С. 5–22.
3. Ахмаметьєва Г.В., Бойко Н.В. Розробка алгоритму формування стеганографічного ключа для цифрових зображень. «Шляхи розвитку науки в сучасних кризових умовах»: матеріали І Міжнародної науково-практичної інтернет-конференції (Дніпро, 28-29 травня 2020 р.). / Дніпро, 2020. Т.1. 608 с. С.32-35.
4. Бойко Н.В. Удосконалення стеганографічного методу для цифрових зображень. Розробка алгоритму формування стеганографічного ключу: квал. роб. бак.: 122 Комп'ютерні науки. – Одеса 2020. – 67 с.
5. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22. May 15, 2001.
6. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness// http://www.stat.fsu.edu/pub/diehard/

Ключові слова: стеганографія, стеганографічний ключ, криптографія, S-блоки заміни, перемішування, статистичні характеристики
Keywords: steganography, steganographic key, cryptography, S-boxes, permutation, statistical characteristics

ВПЛИВ КІБЕРЗАГРОЗ НА ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

Пунченко Наталія

в.о. завідувача кафедри інформаційних технологій Одеського державного аграрного університету, кандидат технічних наук, доцент

Златова Марія

магістрант Одеського державного аграрного університету

У роботі розглядається важливий аспект у сучасному бізнес-середовищі. Аналізуючи зростання кіберзагроз і кібератак, у роботі досліджується, як ці інциденти впливають на загальну ефективність управління підприємством. Зокрема, розглядається втрата прибутку, вартість відновлення та зміни в стратегічному плануванні підприємства. Підкреслюється необхідність інтеграції ефективних стратегій кібербезпеки в систему управління підприєм-

ством і досліджується роль різних відділів, включаючи IT і вищого керівництва для забезпечення кіберстійкості. Крім того, робота рекомендує компаніям звернути увагу на інвестиції в кібербезпеку, враховуючи її важливість для довгострокового успіху та відновлення після потенційних кібератак [1].

У роботі дані посилання джерел, які пояснюють представлений матеріал.

The article considers an important aspect in the modern business environment. Analyzing the growth of cyber threats and cyber attacks, the article examines how these incidents affect the overall effectiveness of enterprise management. In particular, it considers the loss of profit, the cost of recovery and changes in the strategic planning of the enterprise.The article highlights the need to integrate effective cyber security strategies into the enterprise management system and examines the role of various departments, including IT and senior management, in ensuring cyber resilience.In addition, the article recommends that businesses pay attention to investments in cybersecurity, given its importance to long-term success and recovery from potential cyberattacks[1].

The work provides links to sources that explain the material presented.

Проблема впливу кіберзагроз на ефективність управління підприємством стає все більш актуальною в умовах цифрової трансформації бізнесу. Кібератаки можуть призвести до серйозних наслідків, таких як втрати конфіденційної інформації, переривання бізнес-процесів та пошкодження репутації підприємства.

Зростання кількості та складності кіберзагроз ставить під сумнів ефективність існуючих стратегій управління ризиками та кібербезпеки. Підприємства повинні усвідомити, що кіберзагрози не обмежуються лише технічними аспектами, але також мають важливий економічний вимір, впливаючи на фінансові показники та загальний відтік вартості бізнесу[2].

Поставлена проблема вимагає глибокого аналізу та розробки ефективних стратегій управління кіберризиками, які б враховували не лише технічні заходи забезпечення безпеки, а й економічні аспекти, такі як вартість відновлення, страхування та витрати на ефективні заходи кібербезпеки.

Аналіз останніх досліджень та публікацій показує, що за останні роки тема впливу кіберзагроз на управління підприємством привернула значну увагу в наукових дослідженнях. Її вивченням займались Арістова І.В., О. Криворучко, Ю.О. Черниш та багато інших науковців[4]. Їх дослідження акцентуються на розширенні кількості та складності кіберзагроз, оцінці економічних втрат від кібератак, а також розробці стратегій управління ризиками та кібербезпекою. Дослідники вивчали ефективність заходів кіберзахисту та їх вплив на бізнес-процеси та фінансові результати підприємства. Так, Шеломенцев В.П. особливу увагу приділив аспектам інтеграції кібербезпеки в за-

гальну стратегію управління підприємством, враховуючи зростання кількості та різноманітності кіберзагроз[4].

Виходячи з вищевикладеного можна визначити мету дослідження, яка полягає у аналізі комплексного впливу кіберзагроз на рівні аспекти функціонування підприємства та у визначенні стратегії, що спрямована на забезпечення стійкості та оптимальної ефективності у цифровому середовищі.

Сучасна дійсність свідчить про те, що кіберзагрози стрімко розвиваються: кіберзлочини стають більш вдосконаленими, краще координованими і мають транснаціональний характер. Це випливає з того, що Інтернет, цифрові послуги та інформаційно-комунікаційні технології (ІКТ) стали необхідною частиною світової економіки: від електронного обігу документів, інтернет-магазинів та онлайн-банкінгу до систем Інтернету речей та інтелектуальних систем управління підприємствами. За зростанням залежності від ІКТ у бізнесі та підприємництві також зростають кіберризики і кіберзагрози, що вимагає невідкладної реакції для їхнього уникнення або вирішення, а також збільшує необхідність обізнаності факторів ризику серед всіх зацікавлених сторін[3].

Система кібербезпеки має слугувати загальному інтересу як для постачальників послуг, так і для користувачів. Держава, яка виступає гарантом прав і свобод громадян, повинна взяти на себе відповідальність за забезпечення доступу до стабільного та безпечного цифрового простору, доступного для всіх громадян[2]. Відповідно, забезпечення належного рівня кібербезпеки стає необхідною умовою розвитку інформаційного суспільства.

Кібербезпека може не лише реагувати на інциденти, але й передбачати та запобігати атакам ще до їх виникнення. Для підвищення продуктивності підприємства, фахівці з кібербезпеки повинні акцентувати увагу не лише на технологіях, але й на тісній взаємодії з бізнес-командами. Співпраця повинна призвести до готовності відповідати на виклики кіберзловмисників і відбивати атаки з раніше невиданою ефективністю. Керівники підприємств все частіше звертаються до експертів з інформаційної безпеки для підвищення стійкості інформаційної системи та створення цінності захисту для бізнесу [3].

Однак за останні роки використання інформаційних технологій в гібридній війні породило нові вищого рівня кіберзагрози, спрямовані на національну та міжнародну безпеку. Збільшується кількість і потужність кібератак, мотивованих геополітичними інтересами окремих держав, груп та осіб, і вони вже не обмежуються поняттями фінансової ефективності чи рентабельності[1].

Нова епоха кібербезпеки вимагає повністю нових стратегій управління підприємством та його ресурсами, зокрема, інформаційними. Успішне впровадження таких змін в значній мірі залежить від гнучкості бізнес-процесів на підприємстві та ефективності інтеграції нових моделей та методів роботи.

Під час аналізу сучасного стану та тенденцій цифрових технологій, які визначають нову еру кібербезпеки, визначено ключові напрямки захисту підприємства від кіберзагроз.

Щодня стає все важливішим змінювати стереотипи в суспільстві щодо особистих даних, переконуючи, що вони є цінними. Відповідно, актуально проводити навчання фахівців з використання захищених протоколів передачі інформації та впровадження захищених інформаційних систем у роботу[2].

Ризик в сфері кібербезпеки для підприємства може бути пов'язаний із його партнерами та постачальниками. Захист IT-систем може бути посилений, але атаки хакерів можуть відбутися через отримання доступу до даних. Основною загрозою є те, що підприємства, намагаючись забезпечити сильний кіберзахист своїх інформаційних систем, мають труднощі у контролі дій всіх своїх партнерів та підрядників, яким надають доступ до своїх даних. Ці партнери та підрядники можуть виявитися менш кіберграмотними серед співробітників та мати менш ефективні рішення з кібербезпеки. І саме цими вразливостями користуються хакери, нападаючи на компанії-підрядники та отримуючи доступ до необхідних їм інформаційних систем[3].

Незалежно від причин виникнення, кіберінциденти завжди представляють загрозу для неперервної діяльності та сталого розвитку будь-якого підприємства. Основним інструментом для запобігання їм є система кіберзахисту, яка базується на наявних організаційних та технологічних ресурсах, фінансах, людських кадрах і нормативно-правовому базисі. Зазвичай системний адміністратор відповідає за створення цієї системи на локальному рівні. На великих підприємствах управління комплексом заходів протидії кіберзагрозам вже є управлінською задачею, для вирішення якої необхідно залучати кваліфікованих фахівців. Незалежно від конкретних інструментів, які планується використовувати, менеджмент безпеки виконується відповідно до таких принципів: локалізація людського фактору; розуміння критичних місць та джерел небезпеки; моніторинг ризиків; можливість оперативного реагування[4].

Висновки. Вплив кіберзагроз на ефективність управління підприємством вимагає комплексного підходу. Активне керівництво, розвиток культури безпеки та впровадження передових стратегій є важливими кроками у забезпеченні стійкості та успішної діяльності підприємства в умовах кіберзагроз.

Визначено, що для забезпечення кібербезпеки бізнесу є доцільним впровадження відповідних заходів, з основним акцентом на налагодженні потужного захисту інформаційних систем. Важливо враховувати, що загрози кібератак постійно еволюціонують, тому українському бізнесу важливо активно працювати над удосконаленням кіберзахисту. Це завдання зали-

шається стратегічно важливим як для державних установ, так і для приватного бізнесу.

Список використаних джерел:

1. Кібербезпека бізнесу в умовах нестабільності. URL: https://www.pwc.com/ua/uk/publications/2022/ cybersecurity-uncertainty-state.html. (дата звернення: 09.11.2023)
2. Майже половину кібератак СБУ виявляє у режимі «реального часу». URL: https://www.ukrinform.ua/ rubric-technology/3584942-majze-polovinu-kiberatak-sbu-viavlae-u-rezimi-realnogo-casu.html (дата звернення: 09.11.2023)
3. УПРАВЛІННЯ РИЗИКАМИ НА ПІДПРИЄМСТВІ. URL: http://dees.iei.od.ua/index.php/journal/article/view/218/204 (дата звернення: 10.11.2023)
4. КІБЕРБЕЗПЕКА УКРАЇНИ: АНАЛІЗ СУЧАСНОГО СТАНУ. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y (дата звернення: 10.11.2023)

Ключові слова: кібератака, кібербезпека, кіберзагроза, кіберінцидент.
Keywords: cyber attack, cyber security, cyber threats, cyber insident.

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

Кухаренко Сергій

доцент кафедри кібербезпеки факультету кібербезпеки і інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Кількість кіберзагроз з кожним роком швидко зростає. Розвиток кібератак, їх масштаби і можливі впливи на діяльність будь-яких організації спонукають останніх знаходити та приймати важливі рішення про те, як економічно ефективно управляти операціями щодо забезпечення безпеки.

Великі корпорації та організації всього світу такі, як JPMorgan Chase, IBM, Cisco, Amazon Web Services (AWS), Microsoft вже протягом багатьох років активно використовують Security Incident Event Management (SIEM) та Security Operations Center (SOC) у своїх стратегіях забезпечення інформаційної безпеки.

SOC – це спеціалізований центр (фізичний об'єкт всередині організації), що поєднує фахівці з інформаційної безпеки (команда аналітиків), які за допомогою спеціальних систем, процесів та технологій, призначених для безперервного моніторингу та реагування на події вирішують завдання з безпеки. Таких як контроль питань кібербезпеки, виявлення загроз, порушень та їх