Принципи стратегічного управління кібербезпекою підприємства

Далик Володимир Петрович[1], Максимів Іван Дмитрович[2],
Паськів Володимир Володимирович[3], Стасюк Петро Володимирович[4],
Паска Роман Петрович[5], Бутельський Ян Юрійович[6]

Опубліковано	Секція	УДК
08.11.2023	Економіка	004.056

DOI: https://doi.org/10.5281/zenodo.10117838

Анотація. У статті розглянуто ключові принципи стратегічного управління кібербезпекою підприємства в сучасному цифровому середовищі. З урахуванням важливості кібербезпеки для забезпечення нормального функціонування і стійкості підприємства в умовах загроз, узагальнено принципи, які визначають ефективність стратегічного управління кібербезпекою, включаючи підтримку керівництва, постійну оцінку ризиків, визначення мети та цілей, забезпечення необхідних ресурсів та навчання персоналу, відповідність стандартам безпеки, системний підхід та моніторинг результатів. За результатами проведеного дослідження наголошено на важливості підтримки ініціативи з кібербезпеки та виділення необхідних ресурсів для їх реалізації. Зазначено, що стратегія кібербезпеки має містити чітко сформульовану мету та конкретні цілі, а також бути підкріплена необхідними ресурсами, включаючи фінансові, людські та технічні для її впровадження.

Ключові слова: стратегічне управління, кібербезпека, підприємство, ризики, захист, цифрове середовище, стандарти безпеки, управління ресурсами.

Principles of strategic management of enterprise cyber security

Abstract. The modern business environment is undergoing transformation due to the rapid development of information technologies, leading to an increase in the volume and significance of digital information for enterprises across all sectors of the economy. In this context, ensuring the security of this information becomes a critical task for businesses. Cybersecurity is an essential aspect of information security, defined as a set of measures aimed at protecting information from unauthorized access, destruction, loss, or disclosure. Significant factors amplifying the importance of cybersecurity include the growth in the number and complexity of cyberattacks, the exploitation of digital information for business operations, and increased attention from social and regulatory structures on this matter.

[1]кандидат економічних наук, доцент, Національний університет «Львівська політехніка», https://orcid.org/0000-0003-0004-2270
[2]аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0009-0173-8588
[3]аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0008-2995-4840
[4]аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0000-2559-0770
[5]аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0005-7334-2508
[6]аспірант, ЗВО «Львівський університет бізнесу та права», https://orcid.org/0009-0007-8873-0620

However, despite the importance of cybersecurity for businesses, there are numerous challenges and issues related to its provision. This article explores the key principles of strategic enterprise cybersecurity management in the modern digital environment. Recognizing the importance of cybersecurity in ensuring normal enterprise functioning and resilience to threats, the article generalizes the principles that determine the effectiveness of strategic cybersecurity management. These principles include top management support, continuous risk assessment, goal and objective setting, provision of necessary resources and personnel training, compliance with security standards, a systemic approach, and result monitoring. The research emphasizes the significance of supporting cybersecurity initiatives and allocating necessary resources for their implementation. It highlights that a cybersecurity strategy should have a clearly defined purpose and specific objectives, supported by the required resources, including financial, human, and technical resources, for successful implementation. The strategy should adhere to regulatory requirements and security standards applicable to the enterprise, including compliance with relevant legislation and other requirements to ensure proper conformity. The strategy should be based on a systemic approach, being integrated and encompassing all aspects of the organization, including technology, processes, people, and partners. Moreover, the strategy should include a system for monitoring and analyzing results to assess its effectiveness and respond promptly to changes in the cyber environment.

Keywords: strategic management, cybersecurity, enterprise, risks, protection, digital environment, security standards, resource management.

Вступ

Сучасне бізнес-середовище переживає трансформацію через швидкий розвиток інформаційних технологій, що призводять до зростання обсягу цифрової інформації та її значущості для підприємств у всіх галузях економіки. У такому контексті гарантування безпеки цієї інформації стає критичним завданням для підприємств. Кібербезпека – це важливий аспект інформаційної безпеки, визначається як комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, руйнування, втрати чи розкриття. Вагомими факторами, що підсилюють важливість кібербезпеки, є зростання кількості та складності кібератак, зловживання цифровою інформацією для ділових операцій, а також підвищена увага соціальних та регуляторних структур до цього питання.

Незважаючи на важливість кібербезпеки для підприємств, на теоретичному рівні існують численні виклики та проблеми, пов'язані з її забезпеченням. Кібератаки стають більш досконалими та складними, і підприємства відчувають постійний потік нових загроз. Актуальність дослідження для сучасної економічної науки полягає в необхідності зрозуміти та вирішити ці проблеми, що надасть підприємствам інструменти та стратегії для ефективного управління кібербезпекою.

У дослідженнях останніх років закладено основи вирішення проблем стратегічного управління кібербезпекою підприємств. Наприклад, у своєму дослідженні Білявська Ю. та Шестак Я. запропонували рекомендації щодо утримання кібербезпеки та зазначили, що кібербезпека має стати запорукою успішного впровадження цифрових технологій, а також наголосили наскільки важливо дотримуватися кібергігієни в умовах війни особливо при переході на 5G-мережі та розвитку Суспільства 5.0. [1]. Краус К., Краус Н., Штепа О. також розглядають трансформаційні процеси кібербезпеки в умовах воєнного стану для суб'єктів господарювання. Науковці обговорюють необхідність захисту даних, розглядають загрози кібербезпеки та вказують на необхідність впровадження системи управління інформаційною безпекою ISO/IEC 27001:2013 для підвищення захисту інформаційних систем. Автори підкреслюють, що підприємство повинно

удосконалювати виробничі процеси технологічних лабораторій та боротися з такими загрозами, як Ramsomware, які можуть вплинути на їхню діяльність і безпеку даних [2].

У дослідженні Вітер С. та Світлишин І. визначено основні принципи та заходи для гарантування безпеки облікової інформації в контексті кібербезпеки, при цьому враховано постійне вдосконалення кіберзлочинності, а також автори наголосили на важливості створення програми заходів з кіберзахисту, які мають охоплювати не тільки технологічні, але і людські ресурси на підприємствах [3]. Хлапонін Ю., Кондакова С., Шабала Є., Юрчук П. та Делянчук П. розглядають тенденції кіберзлочинності та роль кібербезпеки в системі національної безпеки країни на основі дослідження стану систем захисту від кібератак у розвинених країнах, таких як Франція, Японія, Китай, Південна Корея та Велика Британія. У дослідженні підкреслюється важливість розробки національної стратегії кібербезпеки та постійного вдосконалення методів боротьби з кіберзлочинністю для подальшого розвитку суспільства [4].

З урахуванням наявних досліджень, метою цієї статті визначаємо аналіз та вивчення принципів стратегічного управління кібербезпекою підприємств з метою розробки ефективних стратегій та рекомендацій для підприємств у галузі кібербезпеки.

Результати

Стратегічне керівництво є важливою складовою сучасного управлінського процесу на підприємствах і полягає у систематичному плануванні, координації та прийнятті рішень та дій, спрямованих на досягнення довгострокових цілей і успішне функціонування підприємства в мінливих умовах.

Стратегічне управління виокремлюється через свою спрямованість на досягнення цілей, які визначаються на довгий термін та враховують головні завдання підприємства в контексті його місця на ринку та відповідності зовнішнім умовам. Основними елементами стратегічного управління є формулювання місії та візії підприємства, аналіз стану внутрішнього та зовнішнього середовища, визначення стратегічних цілей та завдань, розробка та вибір стратегій, а також контроль та оцінка їхньої ефективності.

Стратегічне управління відіграє важливу роль у підприємствах, оскільки допомагає спрямовувати ресурси та зусилля на досягнення головних цілей, забезпечує сприятливий клімат для прийняття важливих рішень та реагування на зміни в середовищі, а також сприяє визначенню конкурентних переваг підприємства та створенню стратегічної позиції на ринку, що відповідає його корпоративній місії та завданням. Стратегічне управління є важливим елементом процесу прийняття управлінських рішень та вимагає від керівництва підприємства великої уваги до аналізу та прогнозування подій, гнучкості в реагуванні на зміни та здатності до адаптації в нових умов. Таким чином, стратегічне управління є необхідною складовою для забезпечення стабільності, конкурентоздатності та успіху підприємства в сучасному бізнес-середовищі.

Кібербезпека підприємства є складним і багатодисциплінарним аспектом управління, що визначається як система стратегічних, організаційних, технічних та поведінкових заходів та політик, спрямованих на захист інформаційних ресурсів та ділових процесів підприємства від різноманітних загроз, що виникають в кіберпросторі.

Кібербезпека підприємства охоплює аспекти інформаційної безпеки та безпеки технологічних систем і мереж, що використовуються підприємством, передбачає застосування відповідних заходів для захисту конфіденційної, цінної та критично важливої інформації, яка обробляється і зберігається на підприємстві. Кібербезпека також забезпечує безперервність операцій та захист від кібератак, здатних заподіяти шкоду інформаційним активам, фінансовому стану, репутації та іншим важливим аспектам діяльності підприємства.

Кібербезпека підприємства є надзвичайно актуальною та важливою темою в сучасному світі, оскільки від інформаційної безпеки та захищеності технологічних інфраструктур залежить функціонування підприємства та його можливість зберігати конкурентну перевагу на ринку. В умовах загального зростання кількості та складності кіберзагроз, важливим стає не лише реагування на інциденти, а й передбачення та запобігання їх виникненню, що вимагає від підприємств системного та комплексного підходу до кібербезпеки (рис.1).

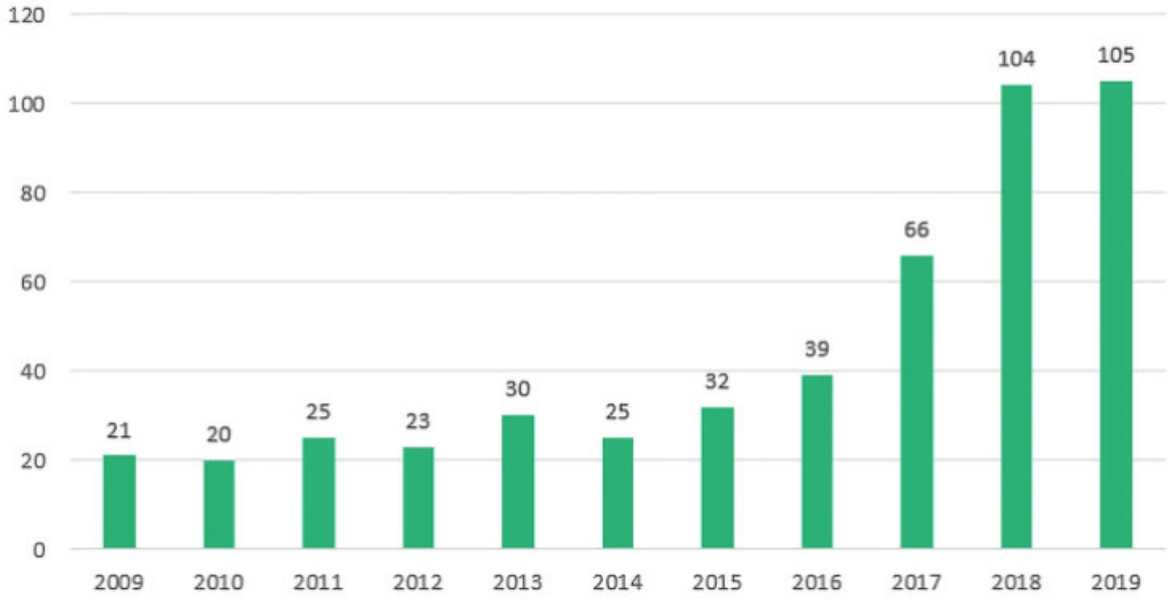

Рис. 1. Випадки кібератак, які завдали втрат на понад 1 млн. дол. США
Джерело: [1]

Переваги стратегічного підходу до кібербезпеки полягають у його спроможності забезпечити більш ефективний та комплексний захист інформаційних ресурсів та процесів підприємства в умовах зростаючого числа та складності кіберзагроз. Стратегічний підхід до кібербезпеки передбачає розгляд заходів та політик у ширшій перспективі, а не обмежується лише реагуванням на окремі події чи інциденти. На рис. 1 наведено деякі з основних переваг стратегічного підходу до кібербезпеки [5, 6]. Усі ці переваги роблять стратегічний підхід до кібербезпеки необхідним для підприємств, оскільки допомагають забезпечити ефективний та стійкий захист від кіберзагроз у сучасному інформаційному середовищі.

Вектори стратегічного управління кібербезпекою підприємства є важливими складовими в системі гарантування безпеки та захисту інформаційних ресурсів і процесів організації в цифрову епоху: ці напрямки визначаються як набір ключових фаз та дій, спрямованих на досягнення стратегічних цілей у галузі кібербезпеки; це система послідовних етапів, які охоплюють ідентифікацію загроз та ризиків, розробку відповідних стратегій, а також асигнування необхідних ресурсів та моніторинг їх впровадження для забезпечення ефективності та стійкості в сфері кібербезпеки [5].

Ідентифікація загроз та ризиків кібербезпеки є першим кроком у створенні стратегії, оскільки дозволяє підприємству ретельно аналізувати потенційні загрози, які можуть вплинути на його інформаційні активи та операції. Такий процес включає в себе ідентифікацію інформаційних активів, оцінку їх вартості та значущості, а також аналіз великої кількості загроз, включаючи зловживання, кібератаки та інші потенційні вектори атак [6].

Рис. 2. Стратегічні підходи до кібербезпеки

Узагальнено авторами

Перший етап стратегічного управління кібербезпекою підприємства передбачає ідентифікацію та аналіз потенційних загроз кібербезпеці, що впливають на інформаційні ресурси та операції організації. Зазначений процес включає в себе аналіз широкого спектру можливих кіберзагроз, таких як кібератаки, віруси, шкідливі програми, фішинг, кібершпигунство та інші. Для ефективного аналізу потенційних загроз необхідно враховувати як внутрішні, так і зовнішні загрози, а також їх еволюцію та появу нових видів атак в кіберпросторі.

Після ідентифікації потенційних загроз необхідно провести оцінку їхнього впливу на підприємство. Оцінка впливу передбачає аналіз можливих наслідків та шкідливого впливу, який мати кіберзагрози на інформаційні активи, фінансовий стан, репутацію та операційну діяльність підприємства. Такі дії допоможуть визначити, наскільки серйозними є потенційні загрози та які ресурси необхідно виділити для їхнього запобігання або відновлення після інциденту. Аналіз потенційних загроз та оцінка їхнього впливу є ключовими етапами у процесі ідентифікації загроз та ризиків кібербезпеки підприємства, оскільки надають підприємству можливість зорієнтувати свої зусилля та ресурси на найбільш критичні аспекти захисту та визначити стратегії для запобігання або мінімізації можливих кіберризиків.

Розробка стратегії кібербезпеки визначає стратегічні цілі та завдання підприємства у сфері захисту від кіберзагроз. Зазначений напрямок передбачає вибір стратегічних цілей, розробку планів дій та визначення необхідних ресурсів для реалізації цих стратегій. Ефективна стратегія кібербезпеки допомагає підприємству забезпечити захист інформаційних активів та процесів від потенційних загроз та зберегти їхню конфіденційність, цілісність та доступність.

Розробка стратегії кібербезпеки є ключовим етапом стратегічного управління кібербезпекою підприємства та передбачає визначення чіткої мети та цілей у галузі кібербезпеки. Мета стратегії кібербезпеки полягає в створенні ефективної системи захисту інформаційних ресурсів та операцій від кіберзагроз. Цілі стратегії визначають конкретні результати, які підприємство прагне досягти, такі як забезпечення

конфіденційності, цілісності та доступності інформації, мінімізація ризиків та втрат, забезпечення відповідності стандартам та регулюванням у галузі кібербезпеки.

Після визначення мети та цілей стратегії кібербезпеки, необхідно вибрати стратегічні напрямки для їхнього досягнення. Такий процес включає в себе розгляд різних можливих стратегій та методів захисту інформаційних активів та операцій. Стратегічні напрямки можуть включати в себе впровадження технологічних рішень, розробку політик та процедур, підвищення кібербезпеки персоналу та багато інших аспектів. Вибір стратегічних напрямків має враховувати унікальні потреби та характеристики підприємства, а також зміни у кіберзагрозах та технологічному середовищі. Оптимальні стратегії кібербезпеки повинні бути адаптованими, ефективними та спрямованими на досягнення мети та цілей, визначених на початку процесу розробки стратегії кібербезпеки підприємства.

Ресурси та інфраструктура для кібербезпеки передбачають виділення відповідних фінансових, технічних і людських ресурсів для впровадження та підтримки стратегії кібербезпеки, що включає інвестування в технології, навчання персоналу, створення захищеної інформаційної інфраструктури та інші аспекти, які забезпечують належний рівень захисту [7].

Людські ресурси відіграють важливу роль у сфері кібербезпеки підприємства і є фундаментальною складовою ефективної системи захисту від кіберзагроз. Спеціалісти з кібербезпеки, а також інші члени персоналу, які відповідають за інформаційну безпеку, відіграють критичну роль у виявленні, аналізі та запобіганні кібератакам. Ефективне управління кібербезпекою вимагає наявності кваліфікованих кадрів, які володіють глибокими знаннями в галузі кібербезпеки та можуть виявляти та реагувати на потенційні загрози. Крім того, організація повинна забезпечити постійне навчання та підвищення кваліфікації свого персоналу, оскільки кіберзагрози постійно змінюються та вдосконалюються.

Технології та обладнання є ще одною важливою складовою інфраструктури для забезпечення кібербезпеки підприємства, що включає в себе різноманітні технічні засоби, програмне забезпечення та обладнання, які допомагають виявляти, блокувати та реагувати на кібератаки. Сучасні технології для кібербезпеки включають в себе системи виявлення та запобігання вторгнень, антивірусне програмне забезпечення, системи криптографічного захисту, мережеві файерволи та інші інструменти, які забезпечують захист інформаційних ресурсів.

Важливо відзначити, що ефективність технологій та обладнання для кібербезпеки залежить від належних налаштувань, підтримки та інтеграції в існуючу інфраструктуру підприємства. Зазначимо, що технології мають постійно оновлюватися, оскільки кіберзагрози постійно еволюціонують.

Отже, ресурси та інфраструктура для кібербезпеки включають в себе як кваліфікований персонал, так і технологічні рішення, і обидва ці аспекти є незамінними в забезпеченні ефективного захисту інформаційних активів та операцій підприємства в кіберпросторі.

Впровадження та моніторинг стратегії охоплює фазу виконання планів та стратегій, а також систематичний моніторинг та оцінку їх ефективності. Такий напрямок дозволяє підприємству здійснювати контроль над реалізацією стратегії кібербезпеки, реагувати на зміни в кіберпросторі та вдосконалювати свої заходи захисту в реальному часі.

Аналізовані напрямки становлять основну структуру для розробки та впровадження стратегії кібербезпеки підприємства, що дозволяє досягти більшої стійкості та ефективності у сфері захисту інформаційних ресурсів та процесів.

Проаналізуймо основні чинники впливу стратегічного управління кібербезпекою на економічні показники підприємства: зменшення ризиків та витрат, збільшення довіри клієнтів та інвесторів, захист репутації та бренду підприємства, підвищення конкурентоспроможності та стійкості до кібератак [6,7].

Здійснення стратегічного управління кібербезпекою на підприємстві суттєво впливає на його економічні показники. Один з ключових аспектів цього впливу – це зменшення ризиків та витрат, пов'язаних з потенційними кіберзагрозами. Шляхом ідентифікації та запобігання потенційним кібератакам підприємство уникне значних фінансових втрат, пов'язаних з втратою конфіденційності даних, втратою доступу до систем, відшкодуванням збитків клієнтам та іншими наслідками кіберінцидентів. Наголосимо, що ефективне стратегічне управління кібербезпекою дозволяє підприємству знизити ризик втрати важливої інформації, яка може бути використана конкурентами або зловмисниками.

Ефективна стратегія кібербезпеки також сприяє збільшенню довіри клієнтів та інвесторів до підприємства. Клієнти та партнери більш схильні співпрацювати з підприємством, яке забезпечує високий рівень захисту особистих даних та конфіденційної інформації, здатне зберегти лояльність клієнтів і залучити нових інвесторів.

Підприємство має дбати про кібербезпеку, захищати свою репутацію та бренд від негативного впливу кіберінцидентів. Відомості про витоки даних, кібератаки та інші події значно пошкоджують репутацію підприємства та призводять до втрати довіри споживачів. Захист бренду є важливим економічним активом, і стратегічне управління кібербезпекою сприяє його збереженню.

Застосування стратегічного управління кібербезпекою підприємства сприяє підвищенню його конкурентоспроможності та стійкості до кібератак. Підприємство, яке ефективно забезпечує захист інформації та операцій від кіберзагроз, отримує конкурентну перевагу перед тими, хто не надає належної уваги кібербезпеці, сприяючи залученню нових клієнтів та збільшенню частки на ринку.

Успішна реалізація стратегій кібербезпеки на підприємствах може бути ілюстрована різними прикладами. Наведемо декілька прикладів успішних стратегій кібербезпеки [8; 9]:

1. JPMorgan Chase & Co.: У 2014 році банк JPMorgan Chase став жертвою однієї з найбільших кібератак в історії, але після інциденту вони інвестували значні ресурси в покращення своєї кібербезпеки: вдосконалили моніторинг, впровадили нові технології, покращили навчання персоналу та почали співпрацю з галузевими експертами. Зазначені заходи допомогли їм запобігти подібним інцидентам у майбутньому та підвищити довіру клієнтів.

2. Target: У 2013 році мережа магазинів Target стала жертвою масштабної кібератаки, внаслідок чого було втрачено багато конфіденційних даних клієнтів. Після цього інциденту компанія внесла значні зміни у свої стратегії кібербезпеки, зміцнила захист та інвестувала в моніторинг, навчання персоналу та технології. Такі дії дозволили їй покращити свою кібербезпеку та зберегти довіру споживачів.

3. Microsoft: Microsoft має довгу історію боротьби з кіберзагрозами, оскільки їхні продукти, такі як операційні системи Windows, є постійним об'єктом атак. Компанія активно веде дослідження в галузі кібербезпеки та надає регулярні оновлення та заходи безпеки для своїх користувачів. Компанія також співпрацює з експертами у сфері кібербезпеки, щоб виявляти та виправляти потенційні вразливості.

4. IBM: IBM активно розвиває свої рішення в галузі кібербезпеки та надає своїм клієнтам усіх рівнів захисту, також ведуть дослідження у сфері кібербезпеки та

аналізують загрози. Компанія практикує принцип "реагуй та запобігай", що дозволяє їй ефективно захищати свої інтереси та ресурси.

Наведені приклади демонструють, як підприємства можуть вдосконалювати свої стратегії кібербезпеки та досягати успішних результатів у цій сфері. Важливо розуміти, що кібербезпека є невід'ємною частиною бізнес-стратегії та вимагає постійного вдосконалення та адаптації до нових загроз.

Перешкоди та виклики в реалізації стратегічного управління кібербезпекою є фундаментальними аспектами сучасного підприємницького середовища, які вимагають глибокого аналізу та ефективних стратегічних відповідей (рис. 3). Кібербезпека стає надзвичайно актуальною у зв'язку з постійним розвитком цифрових технологій та зростанням загроз у кіберпросторі. У зазначеному контексті розглядаються основні перешкоди та виклики, які ускладнюють реалізацію стратегічного управління кібербезпекою підприємств [1; 3; 6].

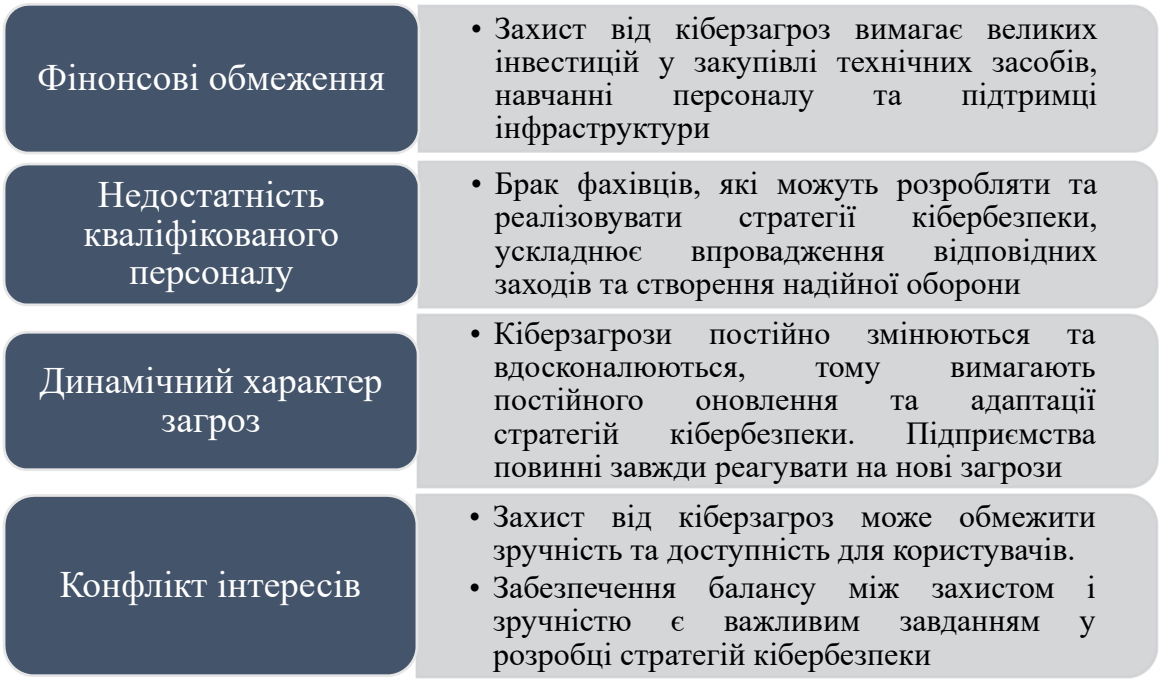

Рис. 3. Перешкоди та виклики в реалізації стратегічного управління кібербезпекою

Узагальнено авторами

Всі зазначені перешкоди та виклики потребують серйозної уваги та розв'язання. Ефективне стратегічне управління кібербезпекою включає в себе розробку стратегій, які враховують ці аспекти та забезпечують надійний захист підприємства в цифровому середовищі.

Висновки

Ефективність та успішність стратегічного управління кібербезпекою підприємства засновується на урахуванні низки ключових принципів. За результатами дослідження визначено декілька ключових принципів стратегічного управління кібербезпекою підприємства: підтримка керівництва, постійна оцінка ризиків, визначення мети та цілей, забезпечення належного ресурсу та навчання персоналу, забезпечення відповідності стандартам безпеки, системний підхід, моніторинг та аналіз результатів.

Керівництво підприємства повинно активно підтримувати ініціативи з кібербезпеки та виділяти необхідні ресурси для їх реалізації, оскільки від активної участі вищого рівня залежить успіх стратегії. Підприємство має реально оцінювати кіберзагрози та ризики на основі визначення об'єктів та інформації, що потребують захисту. Стратегія має містити чітко сформульовану мету та конкретні цілі, адже це допомагає визначити, що саме підприємство намагається досягти в області кібербезпеки.

Підприємство повинно забезпечити необхідні ресурси, включаючи фінансові, людські та технічні для впровадження стратегії кібербезпеки. Регулярне навчання персоналу важливе для підвищення компетентності та усвідомленості в галузі кібербезпеки. Щодо забезпечення відповідності, то стратегія повинна відповідати регуляторним вимогам та стандартам безпеки, що стосуються підприємства, зокрема дотримуватися відповідного законодавства та інших вимог для забезпечення належної відповідності.

Стратегія повинна базуватися на системному підході, бути інтегрованою, охоплюючи всі аспекти організації, включаючи технології, процеси, людей та партнерів. Також стратегія повинна передбачати систему моніторингу та аналізу результатів, щоб перевіряти її ефективність та вчасно реагувати на зміни в кіберсередовищі.

Зазначені принципи допоможуть підприємствам створити надійну та ефективну стратегію кібербезпеки, яка дозволить захищати їх від потенційних кіберзагроз і забезпечити стійкість у цифровому середовищі.

Список використаних джерел

1. 8 Huge Cybersecurity Trends (2023). URL: https://explodingtopics.com/blog/cybersecurity-trends
2. Білявська, Ю., Шестак, Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. Commodities· and· markets. 2022. № 43(3), С. 47-59.
3. Краус, К. М., Краус, Н. М., Штепа, О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. Innovation and Sustainability. 2022. № 3: 26-37.
4. Вітер, С. А., Витер, С. А., Світлишин, І. І., Светлишин, И. И. Захист облікової інформації та кібербезпека підприємства. Економіка і суспільство.2017. № 11. С.497-502
5. Хлапонін, Ю. І., Кондакова, С. В., Шабала, Є. Є., Юрчук, П. П., & Делянчук, П. С. Аналіз стану кібербезпеки в провідних країнах світу. Кібербезпека: освіта, наука, техніка. 2019. № 4.С. 6-13.
6. Діордіца, І. В. Система забезпечення кібербезпеки: сутність та призначення. Підприємництво, господарство і право. 2017. № 7, 109-116.
7. Десятко А.М. Кібергігієна. Кібербезпека. Безпека держави: матеріали наукових семінарів. Київ: КНТЕУ. 2020. 101 с.
8. Краус Н.М. Інноваційна економіка в глобалізованому світі: інституціональний базис формування та траєкторія розвитку: монографія. К.: Аграр Медіа Груп. 2019. 420 с.
9. Страшні історії кіберсвіту: 5 найбільших витоків даних десятиліття. https://www.eset.com/ua/about/newsroom/blog/data-protection/strashnyye-istorii-kibermira-5-krupneyshikh-utechek-dannykh-desyatiletiya/
10. Банк JP Morgan повідомив про найбільшу крадіжку клієнтських даних. https://www.epravda.com.ua/news/2014/10/3/495462/