DOI: https://doi.org/10.32782/2524-0072/2024-68-20

УДК 004:658 (477)

ОСОБЛИВОСТІ ФОРМУВАННЯ ЦИФРОВОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

FEATURES OF FORMING DIGITAL SECURITY AT THE ENTERPRISE

Обрамич Орест Сергійович
аспірант,
Національний університет «Львівська політехніка»
ORCID: https://orcid.org/0009-0006-2280-5549

Obramych Orest
Lviv Polytechnic National University

Стаття присвячена особливостям формування системи цифрової безпеки підприємств. У сучасному цифровому середовищі формування системи цифрової безпеки на підприємстві є надзвичайно важливим процесом, що забезпечує захист інформаційних активів від різноманітних загроз. Основними елементами цієї системи є об'єкти, такі як технологічна інфраструктура, та суб'єкти, до яких належать співробітники і IT-фахівці. Спільна робота цих елементів створює цілісну систему, яка захищає дані. Система цифрової безпеки включає методологічне, правове та ресурсне забезпечення, які під впливом управлінських рішень забезпечують уникнення загроз та створення сприятливих для функціонування підприємства умов використання, обробки та зберігання інформації. Стратегічно, вона підвищує довіру клієнтів і забезпечує відповідність нормативним вимогам. Тактично ж, система дозволяє оперативно реагувати на загрози, зменшуючи ризики збитків від кібератак. Отже, формування системи цифрової безпеки є ключовим для сталого розвитку підприємства, сприяючи його успішній адаптації до викликів цифрового світу.

Ключові слова: цифрова безпека, система, підприємство, методологічне забезпечення, правове забезпечення, ресурсне забезпечення.

The article is devoted to the peculiarities of the formation of the digital security system of enterprises. In the modern digital environment, the formation of a digital security system at an enterprise is a critically important process that ensures the protection of information assets from various threats. The main subjects of this system are employees, IT specialists and the management of the enterprise, who play a key role in the implementation of security policies. The objects of the system are information assets, technological infrastructure and business processes that need protection. Methodological support of the system includes the development of strategies, policies and procedures that regulate risk management, detection of threats and response to incidents. As part of the methodological support, basic principles such as integrity, confidentiality and availability are highlighted, as well as specific methods, including encryption, authentication and access control. System functions include risk management, staff training, incident response and monitoring. Legal protection provides for compliance with legislation and standards in the field of data protection. Resource provisioning includes the technical means, software and human resources required to implement security policies. The strategic importance of the system lies in increasing the trust of customers and partners, which contributes to business development. The tactical importance of a digital security system is the ability to quickly respond to threats, which helps to avoid financial losses and ensure the continuity of business processes. Therefore, the formation of a digital security system is the basis for the stable functioning of the enterprise, ensuring its successful adaptation to new challenges in the dynamic digital world. This system is not only a means of protection, but also an important strategic tool that determines the success of the enterprise in conditions of constant changes.

Keywords: digital security, system, enterprise, methodological support, legal support, resource support.

Постановка проблеми. Актуальність дослідження механізму формування цифрової безпеки на підприємстві зростає з кожним роком, адже світ стає все більш цифровим і технологічно складним. Сьогодні компанії стикаються з новими викликами, пов'язаними з кіберзагрозами, які можуть мати серйозні наслідки для їхньої діяльності.

Перш за все, варто зазначити, що кіберзлочини, такі як атаки з використанням шкідли-

вого програмного забезпечення або фішинг, стають дедалі більш витонченими. У сучасному бізнесі дані клієнтів, фінансова інформація та інтелектуальна власність стали стратегічними активами. Втрата чи компрометація таких даних може призвести не лише до фінансових збитків, а й до шкоди репутації компанії. Крім того, зростає кількість регуляторних вимог щодо захисту інформації. Наприклад, закони на зразок GDPR [1] вимагають від підприємств впровадження належних заходів для забезпечення безпеки даних. Невиконання цих вимог може призвести до значних штрафів і втрати довіри з боку клієнтів.

Технології також не стоять на місці. Інтернет речей, хмарні обчислення та штучний інтелект відкривають нові можливості, але водночас створюють нові виклики для забезпечення безпеки. Важливо досліджувати, як інтегрувати ці технології в підприємства таким чином, щоб не ставити під загрозу їхню безпеку.

Не менш важливою є культура безпеки в самих компаніях. З підвищенням обізнаності менеджменту та працівників щодо важливості цифрової безпеки, необхідно розробляти ефективні стратегії і політики. Це не лише зменшить ризики, а й створить середовище, де кожен співробітник усвідомлює свою роль у забезпеченні безпеки. Дослідження механізмів формування цифрової безпеки на підприємстві є критично важливим у сучасному світі. Це допомагає підприємствам не лише захистити свої активи, а й зміцнити свою позицію на ринку, забезпечуючи стабільність і конкурентоспроможність.

Аналіз останніх досліджень і публікацій. Охоплення цифровізацією всіх сфер суспільних та економічних відносин спонукало розвиток досліджень у цій сфері. Найбільш досліджуваними є питання сутності та значення цифровізації в розвитку галузей та підприємств. Розвиток цифровізації поряд з перевагами створює і ризики, які зумовлюють необхідність формування цифрової безпеки на підприємства задля забезпечення захисту його інформації та інтересів. Відтак, в економічній та юридичній літературі дедалі частіше відстежуються управлінські питання щодо забезпечення цифрової безпеки. Зокрема, К. Краус та ін. [2], досліджуючи особливості діджиталізації на мікрорівні, пропонують реалізовувати окремі функції менеджменту для забезпечення цифрової безпеки на підприємстві. Передерій Т. [3] важливу роль в забезпеченні цифрової безпеки підприємства розглядає через необхідність запровадження стратегічного підходу до її управління. Пропонує застосовувати системний підхід до управління цифровою безпекою П. Пасенчук [4], акцентуючи увагу на забезпеченні інструментів та процедур, якими повинен володіти персонал підприємства. Таким чином, досліджуються окремі напрями, методи, функції управління цифровою безпекою на підприємствах.

Виділення невирішених раніше частин загальної проблеми. Розглядаючи комплексний підхід до побудови системи цифрової безпеки на підприємстві, Н. В. Касьянова та ін [5] пропонують реалізовувати концептуальну, математичну та функціональну моделі. Найбільш повною для цілей даного дослідження є концептуальна модель, яка відображає ризики та джерела загроз, перелік процедур, принципів, потенційних загроз та інформаційних ресурсів, які в найбільшій мірі піддаються таким загрозам та потребують захисту. При цьому, не достатньо визначені конкретні інструменти забезпечення цифрової безпеки та функцій, які реалізують цифрову безпеку на підприємствах.

Пропонуючи механізм комплексного забезпечення цифрової безпеки промислового підприємства, Аванесова Н. Е. та ін.[6], виходячи із системного підходу, детально розглядають об’єкти та суб’єктів, мету, завдання, принципи, функції, методи, ресурси, функціональні складові, які забезпечують вибір стратегії цифрової безпеки промислового підприємства. Таким чином, автори відводять першочергове значення стратегічному управлінню цифровою безпекою підприємства, проте не розглянуто особливості формування цифрової безпеки.

Формування цифрової безпеки на підприємстві в умовах зростання залежності багатьох напрямів діяльності підприємств в сучасних умовах та процесів від використовуваних інформаційних технологій та інформації, потребує комплексного концептуального підходу.

Формулювання цілей статті (постановка завдання). Зважаючи на викладене вище, метою даної статті є дослідження особливостей формування цифрової безпеки на підприємстві.

Виклад основного матеріалу дослідження. Розглядаючи цифрову безпеку підприємства, як сукупність «інформаційної безпеки та кібербезпеки, які тісно взаємоді-

ють між собою та направлені на запобігання виникненню, протидію ризикам та загрозам, а також на мінімізацію втрат в разі їх виникнення в сфері інформаційного забезпечення діяльності підприємства та техніко-технологічного забезпечення використання інформації» [7], доцільно визначити основні параметри формування цифрової безпеки на підприємстві.

Варто погодитись із Аванесовою Н. Е та ін. [6], що цифрова безпека на підприємстві повинна носити системний характер, її забезпечення – бути загальною системою, складовою систем управління підприємством. Відтак, доцільно охарактеризувати основні елементи такої системи.

Насамперед, варто відзначити притаманні будь-якій системі, характерних об'єктів та суб'єктів системи цифрової безпеки підприємства.

Під об'єктами системи цифрової безпеки розглядаємо ті елементи інформаційного забезпечення діяльності підприємств, які потребують захисту від загроз і атак для забезпечення їх цілісності, конфіденційності та доступності. До основних об'єктів системи цифрової безпеки підприємства відносимо інформаційні активи, технологічну інфраструктуру, а також процеси і процедури.

Основними об'єктами системи цифрової безпеки є її інформаційні активи, тобто дані, які підприємство збирає, зберігає і обробляє. Це можуть бути фінансові звіти, клієнтські бази даних, конфіденційна інформація про продукти чи технології. Захист цих активів – пріоритет номер один. До технологічної інфраструктури відносяться всі апаратні та програмні засоби, що використовуються на підприємстві. Сервери, комп'ютери, мережеве обладнання, програмне забезпечення – всі ці елементи повинні бути захищені від кібератак і зловмисних дій. Процеси і процедури – це визначені алгоритми і методи, які підприємство використовує для управління інформаційною безпекою. Сюди входять регулярні аудит-інвентаризації, моніторинг доступу до даних, а також процедури реагування на інциденти.

Суб'єкти системи цифрової безпеки підприємства – це фізичні та юридичні особи, які беруть участь у забезпеченні інформаційної безпеки, включаючи співробітників, IT-фахівців, керівництво та зовнішніх партнерів, які спільно відповідають за захист інформаційних ресурсів підприємства.

Насамперед, серед суб'єктів системи цифрової безпеки доцільно виділити співробітників підприємства, які є найважливішим елементом системи безпеки. Від їхньої обізнаності та дотримання встановлених політик залежить успіх у захисті інформаційних активів. Регулярні тренінги та навчання допомагають формувати культуру безпеки в організації. Також важливо виокремити IT-відділ, який відповідає за впровадження і підтримку технологій захисту. Фахівці з інформаційної безпеки, системні адміністратори та технічні експерти працюють над забезпеченням безпеки системи, оновленням програмного забезпечення та моніторингом мережевої активності. Керівництво підприємства має стратегічну роль у формуванні цифрової безпеки. Вони визначають політику безпеки, затверджують бюджети на її реалізацію та забезпечують необхідні ресурси для ефективної роботи системи.

Нарешті, зовнішні партнери компанії, які є постачальниками програмного забезпечення, консультантами з безпеки або компанії, що спеціалізуються на кіберзахисті, тощо забезпечують отримання підприємством доступ до новітніх технологій та експертиз.

Система цифрової безпеки повинна бути побудована на тісній взаємодії між суб'єктами та об'єктами. Співробітники виконують політики, розроблені керівництвом, а IT-відділ забезпечує необхідні технології. Зовнішні партнери додають експертизу, яка допомагає підприємству залишатися на передовій в умовах постійно змінюваного цифрового середовища.

Система цифрової безпеки підприємства є складним і багатогранним механізмом, який охоплює різні аспекти захисту інформаційних активів. Методологічне забезпечення системи цифрової безпеки підприємства є основою для формування ефективних стратегій захисту інформаційних активів. Тут доцільно виділити загальні принципи забезпечення цифрової безпеки, а також методи та функції її реалізації.

Основні принципи забезпечення цифрової безпеки на підприємстві складають фундамент для ефективної системи захисту інформаційних активів. Ці принципи формують стратегічний підхід, що дозволяє адаптуватися до сучасних викликів у сфері кіберзахисту.

1. Конфіденційність. Цей принцип передбачає, що інформація повинна бути доступною лише для тих осіб, які мають на це відповідні права. Забезпечення конфіденційності передбачає використання методів шифрування, контроль доступу і політики обмеження інформації. Це не тільки захищає чутливі дані, але й підвищує довіру клієнтів та партнерів.

2. Цілісність. Цілісність інформації означає, що дані мають залишатися незмінними і точними під час зберігання і передачі. Підприємства реалізують заходи, які дозволяють виявляти несанкціоновані зміни, зокрема за допомогою хешування і систем контролю версій. Цей принцип допомагає запобігти маніпуляціям з даними, які можуть завдати шкоди бізнесу.

3. Доступність. Доступність забезпечує, щоб користувачі мали можливість отримувати доступ до інформаційних систем і даних у будь-який час. Це передбачає реалізацію заходів для запобігання простоїв, таких як резервне копіювання даних, відновлення після збоїв і належне управління ресурсами. Забезпечення доступності є критично важливим для безперервності бізнес-процесів.

4. Відповідальність. Кожен співробітник підприємства повинен чітко розуміти свою роль у забезпеченні цифрової безпеки. Визначення відповідальності допомагає створити культуру безпеки, де всі учасники активно беруть участь у захисті інформації. Це включає навчання та підвищення обізнаності про загрози, що існують, і необхідність дотримання політик безпеки.

5. Адаптивність. Система цифрової безпеки повинна бути гнучкою і готовою до змін. Нові технології та методи атак постійно з'являються, тому підприємство має бути готовим адаптувати свої стратегії та інструменти. Регулярне оновлення політик, аудит систем безпеки та навчання персоналу є важливими елементами цього принципу.

6. Прозорість – вимагає відкритого обміну інформацією про політики та процедури безпеки як всередині підприємства, так і з зовнішніми партнерами. Це допомагає створити довіру і забезпечити всіма учасниками необхідну інформацію для дотримання стандартів безпеки.

Дотримання цих основних принципів забезпечує комплексний підхід до цифрової безпеки на підприємстві, дозволяючи захистити інформаційні активи від загроз і забезпечити безперервність бізнесу.

Також методологічний підхід передбачає створення процедур, що визначають конкретні дії у разі виявлення загроз чи інцидентів. Наприклад, у разі кібератаки, процедури можуть регламентувати, хто відповідає за реагування, які кроки потрібно здійснити для мінімізації збитків і як повідомити відповідні органи. Такі чіткі інструкції допомагають уникнути плутанини та зменшити час реакції на загрози.

Методологічне забезпечення також включає регулярний моніторинг та оновлення політик у відповідь на нові виклики. У сучасному світі, де технології швидко розвиваються, підприємства повинні постійно адаптувати свої стратегії, щоб залишатися на передовій в боротьбі з кіберзлочинцями. Це передбачає проведення тренінгів для співробітників, щоб підвищити їхню обізнаність про актуальні загрози, а також тестування готовності через симуляції інцидентів.

Методи забезпечення цифрової безпеки підприємства є основними інструментами, які використовуються для захисту інформаційних активів від різноманітних загроз. Кожен з цих методів виконує свою специфічну роль у створенні багатошарового захисту, що дозволяє ефективно реагувати на сучасні виклики у сфері кібербезпеки.

1. Шифрування є ключовим методом, який перетворює дані на незрозумілий формат, що робить їх недоступними для сторонніх осіб. Цей метод особливо важливий для захисту чутливої інформації, такої як фінансові дані або особисті дані клієнтів. Використовуючи різні алгоритми шифрування, підприємства можуть гарантувати, що навіть якщо дані потраплять до зловмисників, їх не вдасться прочитати без відповідного ключа. Шифрування може застосовуватися як до даних на стаціонарних носіях, так і до інформації, що передається через мережу.

2. Аутентифікація забезпечує підтвердження особи або системи, що намагається отримати доступ до інформаційних ресурсів. Вона включає в себе використання паролів, PIN-кодів, а також більш сучасних методів, таких як двофакторна аутентифікація (2FA) або біометричні дані (відбитки пальців, розпізнавання обличчя). Цей метод допомагає переконатися, що доступ до системи отримують лише авторизовані користувачі, знижуючи ризик несанкціонованого доступу.

3. Контроль доступу регулює, хто і які ресурси може використовувати в інформаційній системі. Це може бути реалізовано через політики, які визначають права доступу на основі ролей користувачів, а також за допомогою технологій, які обмежують доступ до чутливої інформації. Цей метод допомагає запобігти витокам даних та зловживанням, гарантуючи, що лише уповноважені особи можуть отримувати доступ до специфічної інформації.

4. Моніторинг і аудит – це процеси, які передбачають постійне спостереження за активністю в інформаційних системах та перевірку дотримання політик безпеки. Цей метод включає використання систем виявлення вторгнень (IDS) і журналів доступу для виявлення аномалій або підозрілої активності. Регулярний аудит дозволяє виявляти вразливості, аналізувати інциденти безпеки та забезпечувати постійне вдосконалення системи захисту.

5. Резервне копіювання є важливим методом, що забезпечує захист даних від втрати внаслідок збоїв, атак або людських помилок. Регулярне створення резервних копій дозволяє швидко відновити інформацію в разі її втрати, мінімізуючи збитки і зупинку бізнес-процесів. Системи резервного копіювання можуть бути автоматизованими та інтегрованими в загальну стратегію безпеки підприємства.

6. Пенетраційне тестування. Цей метод включає контрольоване проведення атак на інформаційні системи з метою виявлення їх вразливостей. Пенетраційні тестування дозволяють підприємствам зрозуміти, наскільки ефективно працює їхня система безпеки, та визначити слабкі місця, які потребують покращення. Це важливий етап в управлінні ризиками, оскільки дозволяє вжити превентивні заходи до того, як зловмисники зможуть скористатися вразливостями.

Наведені методи забезпечення цифрової безпеки формують основний каркас захисту підприємства, який дозволяє йому ефективно управляти ризиками, захищати інформацію та підтримувати стабільність бізнес-процесів у сучасному цифровому середовищі.

Таким чином, методологічне забезпечення створює основу для комплексного підходу до цифрової безпеки, що дозволяє підприємствам ефективно управляти ризиками, виявляти загрози та адекватно реагувати на інциденти, забезпечуючи стабільність і захист інформаційних ресурсів.

Функції забезпечення цифрової безпеки на підприємстві є невід'ємною частиною комплексного підходу до захисту інформаційних активів. Вони дозволяють не лише реалізувати заходи безпеки, а й організувати процеси, що забезпечують надійний захист у сучасному цифровому середовищі.

Одна з основних функцій цифрової безпеки полягає в управлінні ризиками. Це включає в себе систематичний підхід до ідентифікації, оцінки та реагування на потенційні загрози. Підприємство має оцінити, які дані і системи є найбільш вразливими, а також визначити можливі наслідки у разі їх компрометації. На основі цього аналізу розробляються стратегії для зменшення ризиків, що дозволяє адаптувати заходи безпеки відповідно до специфіки бізнесу.

Функція реагування на інциденти є критично важливою для забезпечення безпеки. У разі виникнення інциденту, наприклад, кібератаки або витоку даних, підприємство повинно мати чіткий план дій. Цей план охоплює виявлення інциденту, оцінку його масштабів, реагування на загрозу та відновлення нормальної роботи систем. Наявність такого плану дозволяє знизити негативні наслідки і швидше повернутися до звичайної діяльності.

Підвищення обізнаності співробітників є важливою функцією, оскільки людський фактор часто стає найбільш вразливим місцем у системі безпеки. Регулярні тренінги та навчальні програми допомагають співробітникам зрозуміти загрози, такі як фішинг або соціальна інженерія, а також навчають їх правильному використанню технологій. Чим обізнаніші співробітники, тим менше шансів на успіх атак, що використовують людські помилки.

Ця функція охоплює регулювання змін в інформаційних системах та технологіях. Кожне оновлення програмного забезпечення, зміна конфігурації системи або впровадження нових технологій повинні проходити через процедури безпеки. Це допомагає забезпечити, що зміни не створять нових вразливостей і не порушать існуючі механізми захисту.

Функція відповідності нормативам передбачає дотримання всіх вимог, які регулюють захист даних і інформаційної безпеки. Це можуть бути як національні закони, так і міжнародні стандарти, такі як GDPR або ISO 27001. Забезпечення відповідності не лише захищає підприємство від юридичних наслідків, але й підвищує його репутацію в очах партнерів і клієнтів.

Моніторинг і аудит є постійними функціями, які забезпечують контроль над дотриманням політик безпеки. Моніторинг активності в системах дозволяє виявляти аномалії та потенційні загрози в режимі реального часу, тоді як аудит дозволяє регулярно перевіряти ефективність реалізованих заходів. Ця функція сприяє постійному вдосконаленню системи безпеки і своєчасному виявленню слабких місць.

Функції забезпечення цифрової безпеки на підприємстві складають комплексний меха-

нізм, який дозволяє не лише захищати інформаційні активи, а й підтримувати їх цілісність, конфіденційність та доступність. Вони забезпечують системний підхід до управління безпекою, що є критично важливим для успішної діяльності в умовах постійно змінюваного кіберсередовища.

Не менш важливим є правове забезпечення цифрової безпеки. Це охоплює дотримання національних і міжнародних нормативних актів, законів про захист даних і приватності, а також стандартів кібербезпеки. Правова база забезпечує законність дій підприємства у сфері збору, обробки та зберігання інформації, а також захищає права користувачів та співробітників, формуючи довіру до системи безпеки.

Ресурсне забезпечення складається з усіх необхідних матеріальних, технічних і людських ресурсів, які потрібні для реалізації політик безпеки. Це включає в себе інвестиції в апаратне і програмне забезпечення, навчання співробітників, а також залучення зовнішніх експертів. Наявність достатніх ресурсів дозволяє підприємству ефективно реалізовувати заходи щодо захисту інформації.

Систему цифрової безпеки також слід розглядати через призму управлінських рішень та процесів. Це стосується організаційної структури, відповідальності та ролей всіх учасників процесу забезпечення безпеки. Управлінські рішення визначають, як реалізуються політики безпеки на практиці, хто відповідає за контроль і моніторинг, а також як відбувається комунікація в разі виникнення інцидентів.

Формування системи цифрової безпеки підприємства необхідно для захисту інформаційних активів від різноманітних загроз, які можуть поставити під загрозу цілісність, конфіденційність і доступність даних. У сучасному світі, де інформація стала одним із найцінніших ресурсів, підприємства стикаються з численними викликами, від кібератак до внутрішніх ризиків, і саме система цифрової безпеки забезпечує їх ефективний захист.

Система цифрової безпеки повинна забезпечити збереження конкурентоспроможності підприємства, адже надійна система захисту інформації підвищує довіру клієнтів і партнерів; є важливим елементом для виконання нормативних вимог; повинна допомогти уникнути фінансових втрат, пов'язаних з кібератаками. Витрати на відновлення після атаки, штрафи за порушення законодавства в сфері захисту даних та втрати через зупинку бізнес-процесів можуть бути значними. Наявність ефективної системи захисту допомагає зменшити ці ризики і забезпечити стабільність фінансових показників підприємства.

Необхідність формування системи цифрової безпеки підприємства пов’язана з її здатноістю захищати інформаційні активи, підтримувати довіру клієнтів, уникати фінансових ризиків і дотримуватися нормативних вимог. Це не лише засіб захисту, а й стратегічний інструмент, який допомагає підприємствам процвітати в умовах швидко змінюваного цифрового середовища.

Висновки. Формування системи цифрової безпеки на підприємстві є надзвичайно важливим процесом, що впливає на стабільність і ефективність діяльності в умовах сучасного цифрового середовища. Важливою складовою цієї системи є об'єкти і суб'єкти, які беруть участь у забезпеченні безпеки. Об'єкти – це інформаційні активи, технологічна інфраструктура та бізнес-процеси, що потребують захисту. Суб'єкти – це співробітники, IT-фахівці та керівництво, які реалізують політики безпеки.

Крім того, система цифрової безпеки складається з різноманітних елементів забезпечення: методологічного, правового та ресурсного, пов’язані реалізацією управлінських рішень. Методи забезпечують захист інформації від несанкціонованого доступу. Функції управління ризиками, реагування на інциденти і навчання персоналу підвищують готовність підприємства до можливих загроз. Завдяки комплексному підходу підприємства можуть створити багатошарову оборону, яка захищає від різноманітних атак.

З точки зору стратегічного значення, система цифрової безпеки формує основи для сталого розвитку підприємства. Коли інформаційні активи надійно захищені, це підвищує довіру клієнтів і партнерів, що може призвести до залучення нових клієнтів та розширення ринку. Наявність ефективної системи безпеки забезпечує відповідність нормативним вимогам, що допомагає уникнути ризиків, пов’язаних із юридичними наслідками.

Тактичне значення системи цифрової безпеки полягає в тому, що вона дозволяє підприємству оперативно реагувати на загрози, зменшуючи ймовірність збитків від кібератак або витоків даних. Регулярний моніторинг і аудит системи забезпечують можливість виявлення вразливостей та вдосконалення заходів захисту, що дозволяє постійно адаптуватися до нових викликів.

Формування системи цифрової безпеки на підприємстві є критично важливим не лише для захисту даних, але й для стратегіч-

ного розвитку та успішної адаптації в умовах швидко змінюваного цифрового середовища. Це складний процес, що включає всі рівні організації та вимагає активного залучення всіх співробітників, адже саме це визначає успіх підприємства в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) №2016/679. UDP: https://zakon.rada.gov.ua/laws/card/984_008-16 (Дата звернення 20.09.2024)

2. Краус К., Краус Н., Штепа О. (2022). Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. № 3. С. 26–37.

3. Передерій Т. (2019). Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України*. № 2 (37). С. 201–204.

4. Пасенчук П. В. (2023). Складові цифрової безпеки підприємства*. Інформаційні технології та цифрова економіка*: матеріали Міжнародної науково-практичної конференції. М-во освіти і науки України; Державний університет інфраструктури та технологій. Київ : Видавничий центр ДУІТ. С. 245–247.

5. Касьянова Н. В., Біличенко М. М., Севериненко А. О. (2023). Моделювання цифрової безпеки підприємства. *Електронне наукове фахове видання з економічних наук «Modern Economics».* № 39. С. 54–61.

6. Аванесова Н. Е., Мордовцев О. С., Колодяжна Т. В. (2020). Формування механізму комплексного забезпечення цифрової безпеки промислового підприємства України. *Вісник НТУ «ХПІ» (економічні науки)*. Вип. 3. С. 9–14.

7. Дуляба, Н., & Обрамич, О. (2023). Теоретичні засади дослідження сутності цифрової безпеки. *Економіка та суспільство*, (55). https://doi.org/10.32782/2524-0072/2023-55-66 (дата звернення 20.09.2024)

REFERENCES:

1. Rehlament Yevropeiskoho Parlamentu i Rady (IeS) 2016/679 vid 27 kvitnia 2016 roku pro zakhyst fizychnykh osib u zviazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh, ta pro skasuvannia Dyrektyvy 95/46/IeS (Zahalnyi rehlament pro zakhyst danykh) № 2016/679. Available at: https://zakon.rada.gov.ua/laws/card/984_008-16 (accessed September 20, 2024)

2. Kraus, K., Kraus, N. & Shtepa, O. (2022). Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu. [Digital transformation of cyber security at the micro level in martial law]. *Innovation and Sustainability*. 3. 26–37. [in Ukrainian].

3. Perederij, T. (2019). Stratehiia tsyfrovoi bezpeky pidpryiemstva yak draiver tsyfrovoi transformatsii ekonomiky Ukrainy [The digital security strategy of the enterprise as a driver of the digital transformation of the economy of Ukraine]. *Herald of economic science of Ukraine.* Vup. 2 (37). P. 201–204. [in Ukrainian].

4. Pasenchuk P. V. (2023). Skladovi tsyfrovoi bezpeky pidpryiemstva. [Components of digital security of the enterprise]. *Informatsiini tekhnolohii ta tsyfrova ekonomika*: materialy Mizhnarodnoi naukovo-praktychnoi konferentsii. M-vo osvity i nauky Ukrainy; Derzhavnyi universytet infrastruktury ta tekhnolohii. Kyiv: Vydavnychyi tsentr DUIT. S. 245–247. [in Ukrainian].

5. Kasianova N. V., Bilychenko M. M., Severynenko A.O. (2023). Modeliuvannia tsyfrovoi bezpeky pidpryiemstva. [Modeling the digital security of the enterprise]. *Elektronne naukove fakhove vydannia z ekonomichnykh nauk «Modern Economics».* Vup. 39. P. 54–61. [in Ukrainian].

6. Avanesova N. E., Mordovtsev O. C., Kolodiazhna T. V. (2020). Formuvannia mekhanizmu kompleksnoho zabezpechennia tsyfrovoi bezpeky promyslovoho pidpryiemstva Ukrainy. Visnyk NTU «KhPI» (ekonomichni nauky). Vyp. 3. P. 9–14. [in Ukrainian].

7. Duliaba, N., & Obramych, O. (2023). Teoretychni zasady doslidzhennia sutnosti tsyfrovoi bezpeky. [Theoretical foundations of the study of the essence of digital security]. *Ekonomika ta suspilstvo*, (55). https://doi.org/10.32782/2524-0072/2023-55-66 (accessed September 20, 2024)