Anna Krymska
Candidate of Technical Sciences,
Associate Professor at the Department of Management,
Marketing and International Logistics
Chernivtsi Institute of Trade and Economics
of State University of Trade and Economics

Кримська А.О.
кандидат технічних наук, доцент кафедри менеджменту,
маркетингу і міжнародної логістики
Чернівецького торговельно-економічного інституту
Державного торговельно-економічного університету

DOI: https://doi.org/10.30525/978-9934-26-501-3-29

THE ROLE OF CYBERSECURITY IN IMPLEMENTING DIGITAL STRATEGIES IN ENTERPRISE MANAGEMENT

РОЛЬ КІБЕРБЕЗПЕКИ У ВПРОВАДЖЕННІ ЦИФРОВИХ СТРАТЕГІЙ В УПРАВЛІННІ ПІДПРИЄМСТВОМ

Цифровізація управління підприємством створює нові можливості для підвищення ефективності та адаптивності бізнес-процесів, однак водночас посилює загрозу кіберризиків. У сучасних умовах кібербезпека стає невід'ємною складовою цифрових стратегій, адже без належного захисту інформаційні системи підприємств залишаються вразливими до атак, що може призвести до втрат конфіденційних даних, фінансових збитків та репутаційних втрат. Відтак, інтеграція кібербезпеки в цифрові стратегії є необхідною умовою забезпечення стабільного функціонування та сталого розвитку підприємств. Наукова значущість цієї проблеми полягає в потребі розробки адаптивних моделей кіберзахисту, здатних оперативно реагувати на динамічні загрози у кіберпросторі. Практична ж цінність полягає у визначенні ефективних рішень, що мінімізують кіберризики і підтримують надійність цифрової інфраструктури управління.

Метою дослідження є визначення ключових підходів та механізмів інтеграції кібербезпеки в цифрові стратегії управління підприємствами, що дозволить мінімізувати кіберризики, забезпечити захист конфіденційної інформації та підвищити стійкість цифрової інфраструктури підприємства до сучасних загроз.

Аналіз основних кіберзагроз, пов'язаних з впровадженням цифрових стратегій в управлінні підприємствами, свідчить про зростання ризиків, які безпосередньо впливають на безпеку та стабільність цифрових систем. Поширеність інформаційних технологій створює додаткові можливості для здійснення кіберзлочинів, таких як несанкціонований доступ до конфіденційних даних, крадіжка особистої або фінансової інформації, атаки на корпоративні мережі та системи управління, що призводить до значних фінансових і репутаційних втрат. Однією з найбільш актуальних загроз є фішинг, що використовує соціальну інженерію для введення користувачів в оману та отримання доступу до особистих облікових даних. Такі атаки стають особливо небезпечними у великих компаніях, де інформаційні системи мають багато користувачів, а помилка однієї людини може створити серйозну загрозу для всієї організації.

Впровадження цифрових стратегій також збільшує ризики деструктивного впливу шкідливого програмного забезпечення, зокрема вірусів, троянів та програм-вимагачів.

Зростання складності та взаємозалежності інформаційних систем підвищує вразливість до атак типу «відмова в обслуговуванні» (DDoS), коли кіберзловмисники паралізують роботу цифрових платформ, перевантажуючи їх запитами, що унеможливлює доступ користувачів до системи. Особливої уваги вимагають загрози, пов'язані з порушенням цілісності та доступності даних, що може мати катастрофічні наслідки для підприємств, залежних від точності й оперативності інформації [1].

Сучасні методи та інструменти кібербезпеки, інтегровані в цифрові системи управління, стають важливим компонентом захисту підприємств від динамічних кіберзагроз. Одним із ключових підходів є багатофакторна аутентифікація, що мінімізує ризик несанкціонованого доступу. Наприклад, компанія Google активно використовує цей метод для захисту своїх ресурсів, поєднуючи декілька рівнів перевірки, таких як паролі, мобільні пристрої та біометричні дані. Шифрування даних є ще одним критично важливим інструментом, який гарантує збереження конфіденційної інформації у разі її перехоплення. Так, Facebook впроваджує комплексне шифрування, що дозволяє зберігати персональні дані користувачів у безпеці.

Засоби виявлення та реагування на загрози (EDR) набули популярності завдяки здатності відслідковувати аномальну активність у режимі реального часу. Microsoft, наприклад, активно застосовує EDR для захисту своїх цифрових платформ, що дає змогу своєчасно реагувати на кіберзагрози та запобігати потенційним атакам. Централізована обробка даних та аналіз інцидентів можливі завдяки системам управління інформаційною безпекою (SIEM). IBM інтегрує такі системи у свою кібербезпекову інфраструктуру, що забезпечує аналіз потенційних загроз і дозволяє оперативно локалізувати порушення, створюючи тим самим комплексний підхід до кібербезпеки [2].

Управління ризиками також відіграє важливу роль, оскільки дозволяє підприємствам оцінювати рівень кіберзагроз та приймати стратегічні рішення щодо захисних заходів. Amazon використовує методику управління ризиками для захисту своєї цифрової інфраструктури, забезпечуючи безперервний моніторинг загроз та розробку відповідних запобіжних заходів. У свою чергу, Tesla застосовує штучний інтелект і алгоритми машинного навчання для аналізу великих обсягів даних з метою прогнозування можливих атак і автоматизації процесу виявлення аномалій [3]. Адаптація кіберзахисних підходів до динамічних умов кіберсередовища потребує інтеграції гнучких стратегій, що реагують на нові загрози в режимі реального часу [4]. Ключовим аспектом є створення адаптивної системи кіберзахисту з моніторингом загроз та використанням штучного інтелекту для прогнозування атак на основі поведінкових моделей, що дозволяє не лише реагувати, але й передбачати можливі атаки. Проактивний підхід включає навчання співробітників з метою підвищення кіберграмотності, зменшуючи ризик фішингових атак та витоків інформації. Гнучка політика доступу з багаторівневою аутентифікацією підвищує захист конфіденційних даних, а регулярний аудит безпеки допомагає виявляти вразливості й оперативно їх усувати, підтримуючи стійкість інформаційних систем до нових кіберзагроз.

Запропонована модель інтеграції кібербезпеки покликана вирішити цю проблему завдяки багаторівневій адаптивній структурі, яка поєднує різні методи захисту, аналізу та кризового управління. Унікальність моделі полягає в її здатності не лише реагувати на поточні загрози, а й передбачати потенційні загрози, що дає змогу підприємствам своєчасно адаптувати захисні заходи та мінімізувати ризики для цифрової інфраструктури. Завдяки комплексному підходу модель забезпечує надійність і безперервність роботи цифрових систем, що є критично важливим для стійкого розвитку бізнесу (рис. 1).

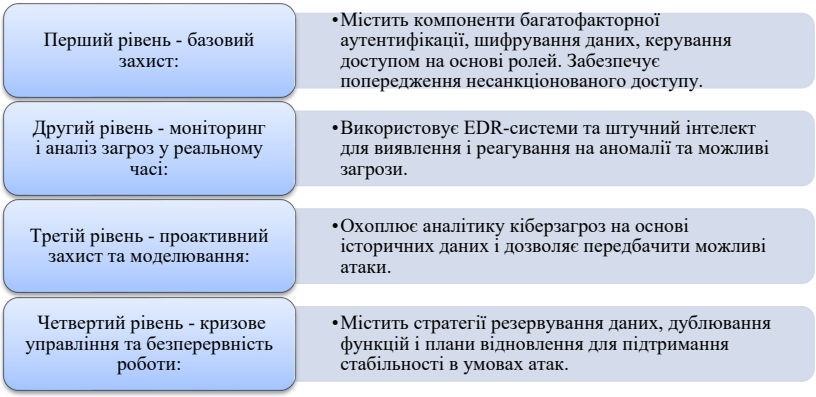

Рис. 1. Модель інтеграції кібербезпеки в цифрові стратегії управління

Джерело: власна розробка автора

На першому рівні впроваджується базовий захист, що охоплює багатофакторну аутентифікацію, шифрування даних і керування доступом на основі ролей. Цей рівень покликаний забезпечити фундаментальний рівень безпеки цифрових систем, знижуючи ймовірність несанкціонованого доступу та витоку конфіденційної інформації. Другий рівень системи фокусується на моніторингу та аналізі загроз у режимі реального часу за допомогою систем виявлення та реагування, а також технологій штучного інтелекту, що дозволяє виявляти аномалії в поведінці користувачів і своєчасно реагувати на можливі загрози. Це значно скорочує час реагування на кіберінциденти і підвищує загальну ефективність захисних заходів. Третій рівень інтегрує проактивний підхід до кібербезпеки, спрямований на аналіз історичних даних і поведінкових моделей для моделювання можливих атак. Це дозволяє передбачати загрози та завчасно вживати превентивних заходів, що знижує ризик серйозних інцидентів. Четвертий рівень акцентує увагу на кризовому управлінні та забезпеченні безперервності роботи, передбачаючи впровадження стратегій резервування даних, дублювання функцій та регулярне тестування планів відновлення після кіберінцидентів. Завдяки цьому навіть у разі серйозних загроз цифрові системи підприємства можуть підтримувати стабільність роботи та мінімізувати можливі збитки.

Встановлено, що ефективна інтеграція кібербезпеки є критичною складовою цифрових стратегій управління підприємствами у контексті сучасних кіберзагроз. Недостатня адаптивність традиційних систем безпеки до динамічних загроз ускладнює забезпечення безперервності бізнес-процесів під час кіберінцидентів. Основними ризиками залишаються фішинг, шкідливе програмне забезпечення, порушення цілісності даних та атаки типу «відмова в обслуговуванні». Рекомендовано впроваджувати адаптивну багаторівневу модель захисту, яка поєднує багатофакторну аутентифікацію, шифрування даних, активний моніторинг та проактивні заходи, зокрема навчання персоналу. Подальші дослідження повинні зосереджуватися на адаптивних моделях кіберзахисту з використанням штучного інтелекту для прогнозування загроз та підвищення кіберграмотності співробітників.

Література:

1. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *International Scientific-Practical Journal Commodities and Markets.* 2022. № 43(3). С. 47–59. DOI: https://doi.org/10.31617/2.2022(43)04

2. Далик В.П., Максимів І.Д., Паськів В.В., Стасюк П.В., Паска Р.П., Бутельський Я.Ю. Принципи стратегічного управління кібербезпекою підприємства. *Академічні візії.* 2023. № 25. DOI: https://doi.org/10.5281/zenodo.10117838

3. Ciekanowski M., Gudanowska A., Koperna M., Niziński S. Strategies for Effective Cybersecurity Management in Organizations. *European Research Studies Journal.* 2024. Vol. 27(1). P. 365–379.

4. Judijanto L., Rasmanto M., Wahyudi D. Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks. *International Journal Software Engineering and Computer Science.* 2023. № 3(3). С. 386–396.