Фещук Дмитро Васильович
аспірант,
Приватний вищий навчальний заклад
«Європейський університет»
ORCID: https://orcid.org/0009-0009-0470-9643

DOI: https://doi.org/10.36059/978-966-397-481-1-48

РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ПІД ЧАС ВОЄННОГО СТАНУ

У сучасних умовах воєнного стану питання інформаційної безпеки підприємств набуває критичного значення. Зростає кількість кібератак, спроб несанкціонованого доступу до даних та інших загроз, що можуть вплинути на функціонування бізнесу. Надійний захист інформаційних ресурсів стає необхідною умовою стабільної роботи підприємства, що визначає актуальність даного дослідження. Особливу роль відіграють міжнародні стандарти, які допомагають вибудовувати ефективну систему управління інформаційною безпекою.

Дослідженням питань інформаційної безпеки займалися такі науковці, як: В.І. Андреєв [4], який досліджував основи інформаційної безпеки та управління ризиками; В.О. Хорошко [4], що аналізував формування загроз інформаційній безпеці та організаційні заходи кіберзахисту; Є. Живило [5], який вивчав методи оцінки кіберризиків на об'єктах критичної інформаційної інфраструктури.

Ризиками інформаційної безпеки є загрози, що можуть призвести до втрати, витоку чи несанкціонованого використання даних підприємства. Основними факторами ризику є кібератаки, фізичне знищення носіїв інформації, збої в роботі систем та внутрішні загрози. Для мінімізації ризиків важливо дотримуватися стандартів ISO 27001, які забезпечують системний підхід до управління інформаційною безпекою.

Головною метою інформаційної безпеки у воєнний час є захист критично важливої інформації підприємства. Військові дії посилюють важливість як зовнішньої, так і внутрішньої інформації. Зовнішня інформація допомагає аналізувати ситуацію на ринку, оцінювати ризики та адаптувати бізнес-стратегію. Внутрішня інформація забезпечує стабільність операційних процесів, управління персоналом і збереження ноу-хау компанії. Одним із ключових підходів до захисту інформації є розміщення критично важливих даних за межами країни, де відбувається війна, що унеможливлює їх захоплення ворогом та використання у злочинних цілях.

До основних ризиків інформаційної безпеки у воєнний час відносяться:

1) Кібератаки – хакерські атаки, фішинг, DDoS-атаки;

2) Фізичні загрози – знищення серверного обладнання, втрати носіїв інформації;

3) Внутрішні загрози – витік даних через персонал, шпигунство;

4) Збої у функціонуванні інформаційних систем – втрата даних через перебої електропостачання, нестабільність мережевих з'єднань;

5) Фінансові ризики – втрати через крадіжку або компрометацію даних.

Для запобігання ризикам та загрозам у воєнний час, вітчизняним підприємствам слід використовувати комплексний підхід до оцінки ризиків та впровадження ефективних заходів безпеки, що дозволить мінімізувати загрози та забезпечити безперервну роботу підприємств навіть у кризових умовах. Нами пропонується найбільш ефективний, на наш погляд, ряд рекомендацій, які посилять безпеку інформації підприємствам, а саме:

1) Впровадження сучасних технологій кіберзахисту: багатофакторної аутентифікації, VPN, резервного копіювання;

2) Організація політики безпеки: контроль доступу до інформаційних систем, навчання персоналу;

3) Регулярний аудит безпеки та тестування систем на стійкість до атак;

4) Використання резервних майданчиків для збереження критично важливих даних за межами країни конфлікту;

5) Дотримання міжнародних стандартів інформаційної безпеки, таких як ISO 27001, для комплексного захисту інформації.

Захист інформації, під час воєнного періоду, є ключовим чинником стабільної діяльності та стратегічного розвитку підприємства у майбутньому. Своєчасне використання комплексу дій та заходів безпеки інформації, є запорукою зменшення наслідків дій негативних факторів. Особливу увагу слід приділити фізичному розміщенню критичних даних за межами країни, де тривають бойові дії, для запобігання їх втрати, пошкодження або потрапляння до рук супротивника, а також додержуватись норм міжнародних стандартів інформаційної безпеки.

Література:

1. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. URL: https://www.iso.org/standard/27001
2. ISO/IEC 27002:2022. Code of Practice for Information Security Controls. URL: https://www.iso.org/standard/75652.html
3. Державна служба спеціального зв’язку та захисту інформації України. Стратегія кібербезпеки України, 2022. URL: https://cip.gov.ua
4. Андреєв В.І., Хорошко В.О. Основи інформаційної безпеки. Львів : Національний університет «Львівська політехніка», 2023. URL: https://directory.lpnu.ua/majors/subject/ikta/6.125.00.00/8/2023/ua/full/1/15704
5. Живило Є. Оцінка кіберризиків на об'єктах критичної інформаційної інфраструктури організаційно-технічних моделей кіберзахисту. ResearchGate, 2023. URL: https://www.researchgate.net/publication/380909071