Co-funded by the Erasmus+ Programme of the European Union

ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСІ РЕАЛІЗАЦІЇ ПРОЄКТІВ

Романенков Юрій,
д.т.н., професор, професор кафедри економічної кібернетики та управління економічною безпекою
Харківський національний університет радіоелектроніки,
м. Харків, Україна
ORCID: https://orcid.org/0000-0002-6544-5348
Полозова Олена,
здобувач першого (бакалаврського) рівня вищої освіти
Харківський національний університет радіоелектроніки,
м. Харків, Україна
ORCID: https://orcid.org/0009-0009-4235-7511

У сучасних умовах швидкого розвитку технологій та цифровізації всі аспекти реалізації проєктів, від планування до впровадження, потребують особливої уваги до забезпечення інформаційної безпеки. Інформаційні ресурси є ключовим активом для будь-якої організації, і їх втрата чи компрометація можуть призвести до серйозних наслідків, як фінансових, так і репутаційних. Відповідно, забезпечення захисту інформації під час реалізації проєктів стає невід'ємною частиною управління ризиками. Захист інформаційних ресурсів стає пріоритетом на кожному етапі життєвого циклу проєкту: від його планування до впровадження та експлуатації.

Теоретичним і практичним аспектам забезпечення інформаційної безпеки та, зокрема, в процесі реалізації проєктів присвячено роботи багатьох науковців, серед яких Ю. Романенков, Т. Зейнієв [1], А. Ясінська [2], В. Ходаков, Г. Райко [3] та інші.

Інформаційна безпека в широкому сенсі – це сукупність технічних і організаційних заходів, а також розроблених документів, основна мета яких полягає в захисті та збереженні інформації, що належить компанії. Водночас, інформаційна безпека є частиною кібербезпеки, яка охоплює не лише захист інформації та даних, а й захист систем, мереж та інших компонентів.

До основних завдань інформаційної безпеки належить також створення бізнес-процесів, що забезпечують захист інформаційних активів незалежно від формату інформації чи її стану (під час передачі, обробки та зберігання в базах даних) [1].

Особливо важливо забезпечити ці процеси під час реалізації проєктів, адже будь-яка вразливість може призвести до витоку або втрати важливої інформації, що негативно вплине на діяльність компанії та її репутацію.

Процес захисту інформації має починатися з оцінки ризиків та загроз, і надалі включати контроль доступу, шифрування даних, регулярний моніторинг

та аудит, а також дотримання правових та нормативних вимог. Кожен з цих елементів відіграє важливу роль у побудові стійкої системи безпеки, яка дозволяє захищати критично важливу інформацію та забезпечувати безперервність проєкту навіть у разі інцидентів або атак. Основні складові інформаційної безпеки в процесі реалізації проєктів представлені в таблиці 1.

Таблиця 1. Класифікація та характеристика складових інформаційної безпеки в процесі реалізації проєктів

Складова	Характеристика
Оцінка ризиків та загроз	Це початковий етап, на якому проводиться аналіз потенційних ризиків і загроз для інформаційних активів. Враховуються можливі сценарії кібератак, внутрішні та зовнішні ризики, а також оцінюється ймовірність витоку даних або компрометації систем. Важливо розуміти, які активи є найбільш критичними для проєкту, і на основі цього визначати пріоритети захисту
Контроль доступу	Забезпечення того, що доступ до інформації мають лише уповноважені особи. Це включає в себе політики автентифікації, використання двофакторної або багатофакторної автентифікації, обмеження прав доступу залежно від ролі та повноважень співробітників. Таким чином, знижується ризик несанкціонованого доступу до критично важливих даних
Шифрування даних	Шифрування є ключовою технологією, що дозволяє захистити інформацію під час її передачі по мережі або при зберіганні в базах даних. Використання сильних алгоритмів шифрування гарантує, що навіть у разі перехоплення або доступу до даних зловмисники не зможуть прочитати або використовувати їх
Моніторинг і аудит	Регулярний моніторинг та аудит систем і процесів інформаційної безпеки дозволяє виявляти можливі порушення або спроби несанкціонованого доступу в реальному часі. Це включає використання систем виявлення вторгнень (IDS/IPS), аналітичних інструментів для аналізу подій, а також впровадження механізмів швидкого реагування на інциденти безпеки
Політики резервного копіювання і відновлення	Забезпечення безперервного функціонування проєкту у випадку збоїв або кібератак є критичним. Регулярне резервне копіювання інформації та наявність планів відновлення після аварій (Disaster Recovery Plan) допоможуть мінімізувати втрати у разі непередбачених ситуацій. Збереження резервних копій у безпечних місцях, віддалених від основної інфраструктури, підвищує рівень захисту
Правові та нормативні вимоги	Проєкти мають відповідати законодавчим і нормативним вимогам у сфері захисту інформації, таким як GDPR, ISO/IEC 27001, NIST, SOC тощо. Це включає управління персональними даними, дотримання стандартів безпеки, а також документування заходів, що застосовуються для забезпечення захисту інформаційних активів

Джерело: розроблено автором на основі [1-3]

Таким чином, для забезпечення ефективної інформаційної безпеки під час реалізації проєктів необхідно впроваджувати комплексні заходи, які

враховують всі ключові складові захисту інформаційних активів. Їх застосування дозволяє забезпечити комплексний підхід до інформаційної безпеки, знизити ризики та гарантувати безпеку інформаційних активів протягом усього життєвого циклу проєкту. Дотримання законодавчих і нормативних вимог інформаційної безпеки має першочергове значення, особливо в галузях із суворими стандартами відповідності. Компанії повинні переконатися, що їхні цифрові ініціативи відповідають чинним законам і нормам для вдалої реалізації проєкту.

У сучасному цифровому середовищі, яке швидко розвивається, підприємства, що не адаптуються до цифрових технологій, ризикують відстати. Успішна адаптація потребує стратегічного міждисциплінарного підходу з акцентом на клієнтоорієнтованість, використання даних і гнучкість. Крім того, бути в курсі нових технологій і використовувати інновації є ключовими для підтримки конкурентоспроможності в цифровому ландшафті, що постійно розвивається.

Швидкий розвиток цифрових технологій та активна діджиталізація бізнес-процесів значно впливають на формування інформаційного середовища сучасних підприємств. Інформація сьогодні розглядається як один із ключових активів бізнесу, і боротьба за доступ до неї стає новим напрямом діяльності. Вибір щодо впровадження систем захисту інформації залишається за кожною організацією, однак, для забезпечення безпеки бізнесу, збереження його унікальності та конкурентних переваг, вкрай важливо вживати заходи щодо забезпечення інформаційної безпеки.

Таким чином, інформаційна безпека підприємства вимагає комплексного підходу в процесі планування та реалізації будь-якого проєкту. Для ефективного захисту даних необхідно постійно моніторити інформаційні системи, регулярно оновлювати програмне забезпечення, а також не чекати, виникнення загрози, а відразу впроваджувати нові технології. Цифровий світ швидко змінюється, і загрози інформаційній безпеці еволюціонують разом із ним. Тому необхідно постійно адаптувати свої стратегії захисту даних, враховуючи нові виклики. Система інформаційної безпеки має бути гнучкою та динамічною, здатною швидко реагувати на зміни зовнішнього та внутрішнього середовища бізнес-структур.

Список використаних джерел:

1. Романенков Ю.О., Зєйнієв Т.Г. Завдання контуру стратегічного управління ефективністю бізнес-процесів в організації. *Системні дослідження та інформаційні технології*. 2015. № 3. С. 43–47.

2. Ясінська А.І. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство*. 2023. Випуск № 56. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3056/2977 (дата звернення 03.10.2024)

3. Застосування інформаційних технологій в економіці, освіті та управлінні проектами: колект. монографія / [В. Є. Ходаков та ін.]; за заг. ред. канд. техн. наук, доц. Райко Галини Олександрівни; Херсон. нац. техн. ун-т. Херсон: Вишемирський В. С., 2018. 201 с.