Лекція: Кібербезпека та управління ризиками в цифровому середовищі управління проєктами

Вступ

У сучасному цифровому середовищі управління проєктами кібербезпека стала однією з ключових складових ефективного функціонування організацій. Використання інформаційних технологій, хмарних сервісів та віддаленого доступу до даних створює значні ризики, пов'язані із загрозами кібербезпеки. Захист інформації, управління доступом, впровадження політик безпеки та відповідність міжнародним стандартам є критично важливими для запобігання кібератакам та мінімізації ризиків. У цій лекції ми розглянемо основні загрози кібербезпеки у сфері управління проєктами, методи захисту даних, вплив цифрових загроз на управління ризиками та міжнародні політики й стандарти у сфері кібербезпеки.

1. Основні загрози кібербезпеки у сфері управління проєктами

Кіберзагрози в управлінні проєктами можуть мати серйозні наслідки, включаючи витік конфіденційної інформації, фінансові втрати, порушення термінів та репутаційні ризики. З розвитком цифрових технологій зростає кількість атак на інформаційні системи, а проєктні команди стають потенційними цілями для зловмисників. Основні загрози можна класифікувати за їхнім впливом і характером.

Фішингові атаки та соціальна інженерія

Фішинг – це один із найпоширеніших методів атак, який використовується для викрадення облікових даних користувачів. Зловмисники надсилають шахрайські електронні листи або повідомлення, що імітують довірені джерела, з метою отримання конфіденційної інформації. Соціальна інженерія, у свою чергу, базується на маніпулюванні людьми для отримання доступу до критичних систем. Це може включати телефонні дзвінки, підроблені документи або навіть використання фізичних методів проникнення в організацію.

Витік даних та несанкціонований доступ

Ненадійне зберігання або передача конфіденційної інформації може призвести до її витоку. Часто причиною є недостатньо налаштовані системи безпеки, вразливості в програмному забезпеченні або недбалість

співробітників. У проєктному управлінні, де використовується велика кількість документів та ресурсів, цей ризик є особливо актуальним.

Шкідливе програмне забезпечення (Malware, Ransomware)

Шкідливі програми (malware) можуть бути впроваджені в інформаційні системи з метою крадіжки даних або завдання шкоди. Один із найнебезпечніших видів таких атак – програми-вимагачі (ransomware), які блокують доступ до файлів або систем і вимагають викуп за їхнє розблокування. Це може повністю зупинити роботу проєктної команди та призвести до значних фінансових витрат.

Інсайдерські загрози

Ризики можуть походити не лише від зовнішніх атак, але й від внутрішніх учасників організації. Співробітники або партнери, які мають доступ до конфіденційних даних, можуть навмисно або випадково спричинити їхній витік. Інсайдерські загрози включають шкідливі дії, недбалість та несанкціоноване використання ресурсів.

DDoS-атаки та загрози для онлайн-платформ

Атаки типу "відмова в обслуговуванні" (DDoS) спрямовані на перевантаження серверів або систем, що може вивести їх з ладу. У сфері управління проєктами такі атаки можуть завадити доступу до критичних сервісів, затримати виконання завдань та спричинити серйозні втрати для організації.

Атаки на хмарні сервіси

Сучасні проєкти часто використовують хмарні платформи для зберігання даних та спільної роботи над документами. Проте недостатній рівень захисту хмарних сервісів може зробити їх легкою мішенню для атак. Загрози включають несанкціонований доступ, вразливості у програмному забезпеченні провайдерів та зловживання привілеями користувачів.

Використання незахищених мереж і пристроїв

Віддалена робота та використання особистих пристроїв у проєктному управлінні створюють додаткові ризики. Підключення до незахищених Wi-Fi-мереж, відсутність оновлень безпеки та використання ненадійного програмного забезпечення можуть стати причиною витоку конфіденційної інформації.

Невідповідність нормативним вимогам та стандартам

Багато організацій працюють у межах міжнародних стандартів кібербезпеки, таких як ISO 27001 або GDPR. Невідповідність вимогам може призвести до юридичних наслідків, штрафів та втрати довіри клієнтів і партнерів.

Кібербезпека в управлінні проєктами потребує постійної уваги та оновлення підходів до захисту інформації. Розуміння основних загроз та їхнього потенційного впливу допоможе організаціям впроваджувати ефективні

заходи безпеки, запобігати втратам і мінімізувати ризики в цифровому середовищі.

Ці загрози можуть призвести до втрати контролю над проєктами, зупинки роботи, а також значних фінансових і репутаційних втрат.

2. Методи захисту даних та управління доступом

Захист даних та ефективне управління доступом є ключовими аспектами кібербезпеки в цифровому середовищі управління проєктами. Сучасні технології та методи забезпечення інформаційної безпеки допомагають зменшити ризики витоку даних, несанкціонованого доступу та інших загроз.

Шифрування та контроль безпеки даних

Шифрування є одним із найефективніших методів захисту даних. Воно дозволяє зробити інформацію недоступною для сторонніх осіб навіть у разі її перехоплення. Основні типи шифрування включають симетричне та асиметричне шифрування, а також використання SSL/TLS для безпечної передачі даних через мережу. Крім того, важливо впроваджувати контроль безпеки даних, що включає:

- Класифікацію даних за рівнями конфіденційності.
- Політики збереження та знищення даних.
- Використання механізмів цифрового підпису для автентифікації документів.

Управління ідентифікацією та доступом (IAM)

Системи IAM (Identity and Access Management) забезпечують контроль над тим, хто має доступ до інформаційних систем і на якому рівні. Основні компоненти IAM включають:

- **Двофакторну автентифікацію (2FA)** – додатковий рівень захисту при вході в систему.
- **Мультифакторну автентифікацію (MFA)** – комбінацію різних методів перевірки особи.
- **Принцип найменших привілеїв (PoLP)** – обмеження доступу тільки тими правами, які необхідні для виконання завдань.
- **Single Sign-On (SSO)** – єдиний доступ до кількох систем за допомогою однієї автентифікації.

Моніторинг активності та аудит

Постійний моніторинг активності користувачів дозволяє виявляти підозрілі дії, що можуть свідчити про загрози безпеці. Інструменти для моніторингу та аудиту включають:

- **Системи виявлення вторгнень (IDS/IPS)** – автоматичний аналіз мережевого трафіку для виявлення аномалій.

- **Журнали подій (SIEM)** – централізоване зберігання та аналіз логів систем безпеки.
- **Контроль змін у конфігураціях** – автоматичний аудит змін у критичних системах.

Політики управління доступом та безпеки

Важливим аспектом кібербезпеки є створення чітких політик управління доступом, які включають:

- Впровадження ролевої моделі доступу (RBAC).
- Регулярний перегляд та оновлення прав доступу користувачів.
- Автоматизацію процесів надання та відкликання доступу.
- Захист від витоків даних шляхом моніторингу використання конфіденційної інформації.

Захист кінцевих пристроїв

Віддалена робота та використання особистих пристроїв у проєктному управлінні створюють додаткові ризики, тому важливо забезпечити:

- Використання корпоративного антивірусного програмного забезпечення.
- Контроль оновлень операційних систем і застосунків.
- Використання VPN для захищеного з'єднання.
- Автоматичне блокування пристроїв у разі тривалого простою.

Резервне копіювання та відновлення даних

Для мінімізації наслідків атак (наприклад, програм-вимагачів) необхідно впроваджувати стратегії резервного копіювання, що включають:

- Регулярне створення резервних копій у кількох незалежних локаціях.
- Використання методів шифрування для резервних даних.
- Автоматизоване тестування процесів відновлення інформації.
- Використання "золотих копій" (immutable backups), які не можуть бути змінені навіть у разі атаки.

Захист даних та управління доступом є фундаментальними аспектами кібербезпеки, які допомагають мінімізувати ризики втрати або компрометації інформації. Впровадження ефективних методів захисту дозволяє організаціям забезпечити надійне функціонування інформаційних систем у цифровому середовищі.

Для мінімізації кіберризиків в управлінні проєктами необхідно впроваджувати сучасні методи захисту даних і управління доступом:

- **Шифрування даних** – використання сучасних криптографічних алгоритмів для захисту переданих і збережених даних.
- **Двофакторна автентифікація (2FA)** – додатковий рівень безпеки при вході в системи управління проєктами.

- **Розмежування доступу** – обмеження прав користувачів відповідно до їхніх посадових обов'язків (принцип найменших привілеїв).
- **Моніторинг та аудит** – регулярний аналіз активності користувачів для виявлення аномальної поведінки.
- **Резервне копіювання** – створення резервних копій критичних даних для захисту від атак програм-вимагачів.
- **Навчання персоналу** – підвищення обізнаності співробітників щодо кіберзагроз та способів їх запобігання.

Ефективне управління доступом і захист інформації допомагає зменшити ризики несанкціонованого доступу до даних і запобігти втратам інформації.

3. Вплив цифрових загроз на управління ризиками

Кіберзагрози безпосередньо впливають на процес управління ризиками в проєктах, змінюючи підходи до оцінки ймовірності та наслідків загроз. Основні аспекти впливу цифрових загроз на управління ризиками включають:

- **Підвищення рівня невизначеності** – складність прогнозування нових типів атак та їхніх наслідків.
- **Необхідність оперативного реагування** – важливість швидкого виявлення та нейтралізації загроз.
- **Фінансові ризики** – витрати на ліквідацію наслідків кібератак, штрафи за порушення нормативних вимог.
- **Зміни в методах управління ризиками** – перехід від реактивних до проактивних стратегій захисту.
- **Адаптація політик безпеки** – необхідність регулярного оновлення стандартів кібербезпеки відповідно до нових загроз.

Проактивне управління кіберризиками включає впровадження систем виявлення загроз, тестування на проникнення, створення планів реагування на інциденти та впровадження політик інформаційної безпеки.

Цифровізація поступово трансформує суспільні економічні відносини. Сучасні підприємства все частіше використовують прогресивні цифрові бізнес-моделі. Екосистемна модель є найскладнішою, втім має значні можливості. Цифровою екосистемою є соціально-технічна система, у якій постачальники та споживачі активів взаємодіють на базі цифрової платформи. Платформи дозволяють масштабувати діяльність, прискорювати та оптимізувати бізнес-процеси, знижувати витрати, отримувати позитивні мережеві ефекти. Завдяки цим конкурентним властивостям екосистемна модель руйнує традиційні підприємницькі структури та реформує економіку, перетворюючи її на платформну або економіку екосистем. Умови діяльності підприємств у

цифрових екосистемах характеризуються не лише більшими вигодами, але й новими специфічними ризиками. Цифрове середовище вимагає удосконалення інструментів ризик-менеджменту

В разі переорієнтації бізнесу на екосистемну модель у підприємства зростає рівень інформаційних ризиків. Вони набувають нових характеристик і стають значущими для стійкості бізнесу. До них відносять ризики інформаційних систем, інформаційно-комунікаційних технологій, шахрайства в кіберпросторі, кіберзагрози, некоректність обробки даних, порушення інтелектуальної власності, виток приватної або конфіденційної інформації тощо. До особливих ризиків екосистеми належать ризики, пов'язані з діяльністю компанії-організатора екосистеми, яку називають оркестратором. У наукових дослідженнях екосистему часто представляють як спільноту учасників, що вільно взаємодіють між собою без ієрархічного управління. Проте управління екосистемою здійснює оркестратор. Саме він встановлює правила доступу та співпраці в екосистемі, умови й алгоритми роботи. Оркестратор має доступ до всієї інформації, що використовують і генерують учасники, він врегульовує скарги, стежить за функціонуванням екосистеми. Його мета – це прибуток. Компанії-платформи, що є оркестраторами екосистем, можуть становити значні небезпеки для бізнеса. Чим більше платформа стає основним інструментом в операційних процесах, тим вище у підприємства ризики контрагента, пов'язані з безперервністю функціонування платформи та інформацією, що на ній зберігається. Існують ризики використання оркестратором інформаційних даних учасників екосистем для власних цілей, а також ризики дискримінації бізнесу з боку платформи. Дискримінація може проявлятися в технологічних або інформаційних проблемах цифрового обслуговування, виражатися в невигідних або непрозорих умовах партнерства.

4. Політики та стандарти кібербезпеки у міжнародному контексті

Міжнародні стандарти та політики відіграють ключову роль у забезпеченні кібербезпеки в управлінні проєктами. Найважливіші з них включають:

- **ISO/IEC 27001** – стандарт управління інформаційною безпекою, що визначає вимоги до захисту даних і процесів.
- **NIST Cybersecurity Framework** – набір рекомендацій для побудови надійної системи кібербезпеки.
- **GDPR (General Data Protection Regulation)** – регламент Європейського Союзу, що регулює захист персональних даних.
- **CIS Controls** – набір найкращих практик з кібербезпеки для захисту цифрових активів.
- **COBIT (Control Objectives for Information and Related Technologies)** – фреймворк управління IT-ризиками та безпекою.

Ці стандарти забезпечують базу для розробки ефективних політик кібербезпеки, які допомагають організаціям відповідати вимогам регуляторів, захищати інформацію та мінімізувати ризики.

З метою забезпечення належного функціонування внутрішнього ринку з одночасним прагненням досягнути високого рівня кібербезпеки, кіберстійкості та довіри в межах Союзу, цей Регламент встановлює: (a) цілі, завдання та організаційні питання, що стосуються ENISA (Агентства Європейського Союзу з питань мережевої та інформаційної безпеки); та рамки для створення європейських схем сертифікації кібербезпеки з метою забезпечення належного рівня кібербезпеки для продуктів ІКТ, послуг ІКТ та процесів ІКТ в Союзі, а також з метою уникнення фрагментації внутрішнього ринку стосовно схем сертифікації кібербезпеки в Союзі. Рамки, зазначені в пункті (b) першого підпараграфа, застосовують без обмежень до спеціальних положень в інших правових актах Союзу, що стосуються добровільної або обов'язкової сертифікації.

Висновки

Кібербезпека в управлінні проєктами є критично важливим аспектом для збереження конфіденційності, доступності та цілісності даних. Основні загрози включають фішингові атаки, шкідливе ПЗ, витоки даних та DDoS-атаки. Захист інформації забезпечується шифруванням, автентифікацією, моніторингом та резервним копіюванням. Вплив цифрових загроз на управління ризиками вимагає впровадження проактивних стратегій, а відповідність міжнародним стандартам допомагає організаціям підвищити рівень кіберзахисту. Сучасний світ вимагає постійної уваги до питань безпеки, і ефективне управління кіберризиками є важливою складовою успішного виконання проєктів.

Література

1. Kerzner H. Project Management Next Generation: The Pillars for Organizational Excellence. Hoboken, NJ: John Wiley & Sons, 2022. 512 p.

2. Шинкарук Л. В., Дєліні М. М., Суханова А. В., Алексєєва К. А. Управління бізнес-проєктами: навч. посіб. Київ: НУБіП України, 2021. 324 с.

3. Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK Guide). 7th ed. Newton Square, PA: Project Management Institute, 2021. 370 p.

4. Duggal J. S. The DNA of Strategy Execution: Next Generation Project Management and PMO. Plantation, FL: J. Ross Publishing, 2018. 312 p. 13.

5. Morales A. A., Abreu A. Digital Transformation in Project Management: A Case Study in a Public Organization // Journal of Modern Project Management. 2020. Vol. 8, No. 1. P. 120–133.