

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ РИЗИК В ІТ ПРОЕКТАХ

Демченко Д.О.¹; Петрова Р.В., доц., к.т.н.²

^{1,2} Харківський національний університет радіоелектроніки

^{1,2} Україна, Харків

¹ dmytro.demchenko3@nure.ua; ² roksana.petrova@nure.ua

Анотація. Під час дослідження розроблено підходи до оцінки кіберризиків у великих ІТ проектах, зокрема в розподілених системах та комп'ютерних мережах. Експериментально підтверджено ефективність проактивного моніторингу загроз. Запропоновані методи можуть бути практично застосовані для підвищення рівня безпеки в корпоративній і хмарній інфраструктурі.

Ключові слова: кібербезпека; кіберризики; кіберзагрози; управління ризиками.

Вступна частина. У сучасному світі цифровізація процесів у великих ІТ проектах призводить до зростання кіберзагроз, що негативно впливає на конфіденційність, цілісність та доступність даних. Це безумовно стосується розподілених систем та хмарних платформ, які надають можливості для розвитку, але в той же час є цілями для зловмисників. З кожним роком кількість кібератак зростає, а їхні особливості дещо ускладнюють звичайні методи виявлення загроз, що використовуються в більшості організацій.

Існуючі методи боротьби з кіберзагрозами часто сфокусовані на реактивних підходах, а саме: виявленні і виправленні вразливостей вже після атак. Однак такі методи не завжди ефективні, особливо в умовах складної ІТ інфраструктури. Проблема вимагає проактивного підходу, який передбачає інтеграцію безпеки ще на стадії проектування та постійний моніторинг ризиків [2].

Метою дослідження є розробка підходів до проактивного управління кіберризиками у великих ІТ проектах, з акцентом на безпеку розподілених систем і мереж.

Основна частина. Основні кіберризики можна класифікувати за трьома ключовими критеріями: конфіденційність, цілісність та доступність даних. Порушення одного з цих елементів може призвести до критичних наслідків для ІТ проекту, таких як втрата даних або несанкціонований доступ до конфіденційної інформації [3]. Наприклад, атаки DDoS можуть серйозно порушити доступність сервісів, що особливо небезпечно для великих компаній, які надають критичні послуги через інтернет.

Однією з причин зростання кіберзагроз є збільшення використання хмарних технологій та віддаленої роботи, що відкриває нові горизонти та можливості для атак. Цифрова трансформація, хоч і забезпечує нові можливості для розвитку бізнесу, але вона також збільшує вразливість ІТ систем через більшу кількість точок доступу [1]. Особливо це стосується великих розподілених систем, де контроль за доступом та захистом даних є дещо ускладненим через використання віддалених серверів та персоналу.

Для ефективного управління кіберризиками в великих ІТ проектах необхідно впроваджувати проактивні стратегії, такі як "Security by Design". Це означає, що заходи безпеки повинні бути інтегровані на всіх етапах розробки проекту, починаючи від планування та закінчуючи впровадженням. Такий підхід дозволяє знизити ймовірність успішних атак шляхом попередження потенційних загроз ще до їх виникнення. Експериментальні дослідження показали, що використання методів тестування і постійного

моніторингу допомагає виявляти вразливості в системах ще до їхнього використання злоумисниками.

Управління кіберризиками включає як технічні, так і організаційні аспекти. Технічні методи, такі як шифрування даних, двофакторна аутентифікація та сегментація мережі, забезпечують фізичний захист даних від зовнішніх атак. Проте без належної організаційної підтримки вони можуть бути недостатньо ефективними. Організаційні підходи, такі як навчання співробітників та регулярне проведення аудитів безпеки, також є критично важливими для мінімізації ризиків. Це дозволяє зменшити можливості для людських помилок, які залишаються одним із найбільших джерел кіберризиків.

Ключовим компонентом стратегії кібербезпеки у великих ІТ проектах є інцидентний менеджмент. Це процес, який дозволяє організаціям швидко реагувати на загрози та мінімізувати шкоду. Важливим елементом інцидентного менеджменту є наявність чіткого плану дій при виникненні загрози, що включає в себе певну команду швидкого реагування на інциденти та готовність до відносно швидкого відновлення операцій. Використання автоматизованих систем моніторингу та швидкого сповіщення про підозрілу активність однозначно підвищує ефективність таких заходів, дозволяючи виявляти атаки на дуже ранніх етапах розробки ІТ проектів.

Оцінка кіберризиків є невід'ємною частиною управління безпекою у великих ІТ проектах. Важливою складовою цього процесу є використання моделей оцінки ризиків, які допомагають визначити ймовірність загроз і їхні потенційні наслідки для системи. Одним із таких підходів є метод, який дозволяє пріоритезувати ризики залежно від їхнього впливу на проект. Застосування цих методів дозволяє компаніям ефективно розподіляти ресурси для управління ризиками, зосереджуючи увагу на найнебезпечніших загрозах, причому водночас звертаючи увагу і на менш небезпечні потенційні проблеми.

Таким чином, проактивне управління кіберризиками, підтримане технічними та організаційними заходами, дозволяє зменшити ймовірність атак, покращити стійкість систем до інцидентів і знизити потенційні втрати від кіберзагроз.

Останнім десятиліттям сталося стрімке зростання впливу цифрової трансформації на рівень кіберризиків у великих ІТ проектах. Впровадження таких технологій, як хмарні сервіси та штучний інтелект, сприяє підвищенню ефективності та гнучкості бізнес-процесів. Однак це також значно збільшує вразливість інфраструктури до атак, оскільки кожен новий компонент є потенційним носієм шкідливого програмного забезпечення. Масова цифровізація створює комплексні мережі з численними точками доступу, що ускладнює управління безпекою [2]. Відсутність належного захисту таких відносно новітніх елементів може призвести до серйозних наслідків, включаючи витік даних та збої в роботі критично важливих систем.

Висновки. Під час дослідження розроблено підходи до оцінки та управління кіберризиками у великих ІТ проектах. Визначено основні типи загроз, такі як атаки на конфіденційність і доступність даних, та розроблено стратегії для мінімізації ризиків через впровадження методів "Security by Design". Експериментально підтверджено, що постійний моніторинг і активні методи безпеки дозволяють значно зменшити кількість успішних кібератак. Практичне застосування цих підходів може бути корисним для великих організацій та хмарних платформ, що працюють з критичними даними та інфраструктурою будь-якого масштабу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press.
- [2] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- [3] Wheeler, E., & Sutton, D. (2011). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Syngress.

Demchenko D.O., Petrova R.V.

Cyber security as a key risk in IT projects

Abstract. During the research, approaches were developed to assess cyber risks in large IT projects, in particular in distributed systems and computer networks. The effectiveness of proactive threat monitoring has been experimentally confirmed. The proposed methods can be practically applied to increase the level of security in corporate and cloud infrastructures.

Keywords: Cyber security; cyber risks; cyber threats; risk management.