DOI: https://doi.org/10.32782/2524-0072/2024-67-79

УДК 007.2

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЄКТНОМУ УПРАВЛІННІ

PROBLEMS OF INFORMATION SECURITY IN PROJECT MANAGEMENT

Супруненко Світлана Анатоліївна
кандидат економічних наук, доцент,
Національна академія статистики, обліку та аудиту
ORCID: https://orcid.org/0000-0002-4585-3440

Suprunenko Svitlana
National Academy of Statistics, Accounting and Auditing

У статті розглядаються основні проблеми забезпечення інформаційної безпеки в контексті проєктного управління. Автори аналізують сучасні виклики, пов'язані з кіберзагрозами, дезінформацією та кібератаками на критичну інфраструктуру. Особлива увага приділяється питанням конфіденційності, цілісності та доступності інформації в умовах зростаючої ролі технологій та інформаційних мереж. Запропоновані напрями вирішення проблем базуються на створенні ефективних механізмів кіберзахисту, підвищенні кіберграмотності команди проєкту та розвитку співпраці між учасниками проєкту, замовником, партнерами. Стаття підкреслює важливість системного підходу до забезпечення інформаційної безпеки та активної ролі учасників проєкту у розробці та впровадженні стратегічних заходів у цій сфері. Зроблені висновки, що кібербезпека в управлінні проєктами охоплює захист даних, контроль доступу, безпеку мережі, управління вразливістю, реагування на інциденти та дотримання стандартів, таких як ISO 27001.

Ключові слова: проєктне управління, управління проєктами, інформаційна безпека, кібербезпека.

The article considers the main problems of ensuring information security in the context of project management. The authors analyze today's challenges related to cyber threats, disinformation and cyber attacks on critical infrastructure. Particular attention is paid to issues of confidentiality, integrity and availability of information in the context of the growing role of technologies and information networks. The proposed areas of problem solving are based on the creation of effective cyber protection mechanisms, the improvement of cyber literacy of the project team and the development of cooperation between project participants, the customer, and partners. The article emphasizes the importance of a systematic approach to ensuring information security and the active role of project participants in the development and implementation of strategic measures in this area. It is concluded that cybersecurity in project management encompasses data protection, access control, network security, vulnerability management, incident response, and compliance with standards such as ISO 27001. In summary, cybersecurity in project management encompasses data protection, access control, network security, vulnerability management, incident response and compliance with standards such as ISO 27001. Effective cyber security includes the implementation of practices, protocols and measures to protect data, systems and assets from cyber threats. Aspects such as data protection, access control, network security, vulnerability management and incident response are discussed. The importance of the ISO 27001 standard for ensuring information security during the entire project life cycle is emphasized. Implementation of the standard helps to protect documents, databases and other assets of the project from threats. The article emphasizes the need to integrate information security and privacy into the project management methodology, which allows for effective identification, assessment and management of information security risks in any type of project. Information security and privacy should be integrated into the project management methodology to identify, assess and manage risks at all stages of the project.

Keywords: project management, project management, information security, cyber security.

Постановка проблеми. Безпека не входить до стандартного процесу запуску проєкту, однак керівники проєктів повинні приділяти їй увагу. Ігнорування питань інформаційної безпеки та конфіденційності часто призводить до затримок у запуску або введенні в експлуатацію, а іноді навіть до запуску нової інформаційної системи без належного контролю. Це підвищує ризики, такі як розкриття інформації; несанкціонований доступ до систем та

даних; порушення законодавчих вимог, відповідно основною метою безпеки проєкту є захист конфіденційності проєкту, захист артефактів та корпоративних даних.

Інформаційна безпека є критично важливою для бізнесу з кількох причин, серед яких необхідність захисту даних, дотримання законодавства, запобігання кібератакам, необхідність збереження довіри клієнтів, безперервність бізнесу.

Компанії зберігають велику кількість конфіденційної інформації, включаючи дані клієнтів, фінансові записи та комерційні таємниці. Втрата або розкриття цих даних може призвести до серйозних фінансових та репутаційних втрат. В свою чергу, багато країн мають суворі закони та регуляції щодо захисту даних, а недотримання цих вимог може призвести до штрафів та юридичних наслідків. Кібератаки, такі як фішинг, зловмисне програмне забезпечення та DDoS-атаки, можуть паралізувати бізнес-операції. Інформаційна безпека допомагає захистити системи від таких загроз. Клієнти бізнесу очікують, що їхні дані будуть захищені, а порушення безпеки може призвести до втрати довіри та відтоку клієнтів. Надійні заходи безпеки допомагають забезпечити безперервність бізнес-операцій навіть у разі інцидентів, таких як зломи або природні катастрофи.

Отже, проблема інформаційної безпеки в проєктному управлінні є надзвичайно актуальною для дослідження темою.

Аналіз останніх досліджень і публікацій. Питання проблем інформаційної безпеки в проєктному управлінні розглядаються в багатьох сучасних дослідженнях. Так, В.Редзюк і Н. Редзюк, зокрема розглядають актуальні проблеми інформаційної безпеки в Україні, включаючи кіберзагрози, дезінформацію та кібератаки на критичну інфраструктуру. Запропоновані ними напрями розв'язання проблем базуються на створенні ефективних механізмів кіберзахисту та підвищенні кіберграмотності населення [3, с. 59-65]. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління розглядає А. Форос [4, с. 222-226]. Роботи К. Захаренка присвячені аналізу міжнародних та національних нормативно-правових актів, що стосуються інформаційної безпеки, та їх розвитку у сучасних умовах [1].

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значну кількість наукових досліджень з питань забезпечення інформаційної безпеки в проєктному управлінні, практичні аспекти є надзвичайно важливими для забезпечення захисту даних та інформаційних систем, що потребує поглиблення наукового пошуку в цій темі.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження проблеми інформаційної безпеки в проєктному управлінні.

Виклад основного матеріалу дослідження. Функціонування кожної компанії визначається постійним виконанням проєктів в короткостроковій, середньостроковій і довгостроковій перспективі (внутрішні проєкти по підтримці структури організації, і зовнішні проєкти по наданню послуг клієнтам).

Проєкти вимагають збору та обробки даних та генерації інформації. Вони стають все більш залежними від інформаційних систем, які зазвичай містять вразливості та недоліки безпеки. Коли використовуються вразливості, це може негативно вплинути на успіх проєктів. Від рівня інформаційної безпеки в управлінні проєктами залежить, наскільки безпечним буде проєкт. Щоб максимізувати довгострокову рентабельність інвестицій (ROI) при реалізації проєкту, важливо враховувати інформаційну безпеку з усіма аспектами.

Але коли проєкт розглядається в організації, то зазвичай не враховується, що він повинен вестися відповідно до принципів управління проєктами інформаційної безпеки. Однак інформаційна безпека є важливою для кожного проєкту з кількох ключових причин:

1. Захист конфіденційної інформації: Проєкти часто включають роботу з чутливою інформацією, такою як комерційні таємниці, дані клієнтів та інші важливі дані. Захист цієї інформації є критичним для запобігання її несанкціонованому доступу та розкриттю [5].

2. Зменшення ризиків: Інформаційна безпека допомагає виявляти та усувати потенційні загрози, що можуть вплинути на успішність проєкту. Це включає захист від кібератак, зловмисного програмного забезпечення та інших загроз [5].

3. Дотримання нормативних вимог: Багато проєктів підпадають під дію законодавчих та регуляторних вимог щодо захисту даних. Недотримання цих вимог може призвести до штрафів та інших юридичних наслідків [6].

4. Захист репутації: Порушення безпеки може серйозно вплинути на репутацію організації. Забезпечення належного рівня безпеки допомагає зберегти довіру клієнтів та партнерів [5].

5. Збереження активів проєкту: Інформаційна безпека гарантує, що всі ресурси та дані проєкту захищені від втрат або пошкоджень [6]

6. Підтримка безперервності бізнесу: Надійні заходи безпеки допомагають забезпечити безперервність бізнес-операцій навіть у разі інцидентів, таких як зломи або природні катастрофи [6].

І це в основному те, що вимагає ISO 27001 у додатку A.5.8 Інформаційна безпека в управлінні проєктами: Інформаційна безпека повинна вирішуватися в управлінні проєктами, незалежно від типу проєкту. Цей контроль може бути застосований до всіх видів проєктів, від незначного впровадження IT до великого проєкту зі зміни бізнесу. Інформаційна безпека повинна бути частиною «звичайного бізнесу», тому ризики та цілі інформаційної безпеки повинні враховуватися на початку кожного проєкту [7].

Всі проєкти в основному потребують ресурсів, активностей для розвитку та встановлених часових цілей. Інформаційна безпека в управлінні проєктами може бути інтегрована декількома способами (рис. 1).

Отже, інтеграція інформаційної безпеки в управлінні проєктами відповідно до ISO 27001 передбачає виявлення ризиків і впровадження заходів безпеки через навчання команди проєкту політикам та засобам контролю інформаційної безпеки, щоб підвищити обізнаність та компетентність, та зменшити кількість інцидентів та невідповідностей [2].

Для забезпечення інформаційної безпеки проєкту також доцільно укласти угоди про конфіденційність з постачальниками, які працюють над проєктом, та інформувати їх про відповідні політики та процедури. Якщо проєкт співпрацює з постачальником, необхідно налаштувати заплановані перевірки доступу з командою постачальників, проводити огляди та аудити для вимірювання ефективності впровадження, аналізувати результати та за потреби вживати коригувальних заходів або заходів для вдосконалення.

На завершальному етапі проєктів збереження усіх даних та документів повинно відбувати з належними заходами безпеки та перевіркою прав доступу членів команди. Коли ці дії виконуються неналежним чином, це може стати каталізатором несанкціонованого розголошення конфіденційної та безцінної ділової інформації. Особливо важливо (незалежно від розміру організації) включати інформаційну безпеку в проєктну діяльність тих проєктів, які стосуються або націлені на цілісність, доступність і конфіденційність інформації.

Ефективне управління проєктами з точки зору їх кібербезпеки включає кілька ключових компонентів для забезпечення успішного впровадження заходів інформаційної безпеки та захисту пов’язаних із проєктом даних

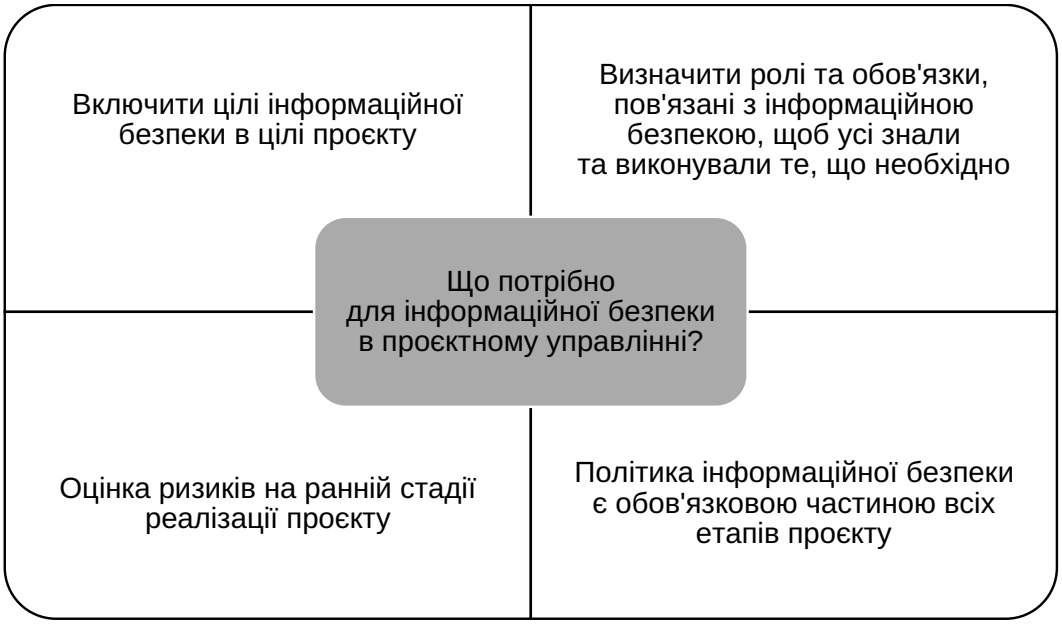

Рис. 1. Інтеграція інформаційної безпеки в управлінні проєктами відповідно до ISO 27001

Джерело: адаптовано авторкою за [6]

і активів. Деякі з ключових компонентів включають (табл. 1).

Впроваджуючи ці ключові компоненти в практику управління проєктами кібербезпеки, організації можуть ефективно зменшувати ризики кібербезпеки, захищати активи проєкту та забезпечувати успішну реалізацію проєктів у безпечному середовищі.

Висновки. Таким чином, інформаційна безпека завжди буде складовою управління будь-яким проєктом в організації. Кібербезпека в управлінні проєктами стосується практик, протоколів і заходів, які впроваджуються для захисту пов'язаних із проєктом даних, систем і активів від кіберзагроз і атак. Це передбачає виявлення, оцінку та пом'якшення ризиків кібербезпеки протягом життєвого циклу проєкту, щоб забезпечити конфіденційність, цілісність і доступність інформації та ресурсів проєкту.

Кібербезпека в управлінні проєктами охоплює різні аспекти, включаючи захист даних, контроль доступу, безпеку мережі, управління вразливістю, реагування на інциденти та дотримання відповідних правил і стандартів. Ефективні заходи кібербезпеки допомагають захистити конфіденційні дані проєкту, пом'якшити вплив порушень безпеки та забезпечити успішну реалізацію проєктів у безпечному середовищі.

Стандарт якості ISO 27001 допомагає керувати інформаційною безпекою проєктів. Від ініціації проєкту до захисту від різних загроз, таких як витоки даних та кібератаки, компанії можуть передбачати ризики, відповідним чином реагувати та захищати свою

Таблиця 1

Ключові компоненти кібербезпеки

Компонента	Сутність заходів
1. Оцінка ризику	Проведення комплексної оцінки ризиків для виявлення потенційних загроз кібербезпеці, вразливостей і ризиків, пов'язаних з проєктом. Це передбачає оцінку ймовірності та потенційного впливу різних інцидентів безпеки на цілі та результати проєкту.
2. Політика та процедури безпеки	Встановлення чітких і надійних політик безпеки, процедур і вказівок, які визначають ролі та обов'язки, окреслюють прийнятне використання ресурсів проєкту та вказують засоби контролю безпеки та заходи для захисту даних і активів проєкту.
3. Безпечна інфраструктура	Впровадження захищеної IT-інфраструктури, мережевої архітектури та систем, які включають передовий досвід галузі та стандарти безпеки для запобігання несанкціонованому доступу, витоку даних і кібератакам. Це може включати впровадження брандмауерів, шифрування, контролю доступу та систем виявлення вторгнень.
4. Контроль доступу	Застосування жорстких заходів контролю доступу, щоб гарантувати, що лише авторизовані особи мають доступ до ресурсів проєкту, даних і систем. Це передбачає впровадження механізмів автентифікації користувачів, керування доступом на основі ролей (RBAC), принципів найменших привілеїв і багатофакторної автентифікації (MFA), де це можливо.
5. Навчання з питань безпеки	Проведення постійного тренінгу з кібербезпеки та навчання для членів команди проєкту та зацікавлених сторін, щоб покращити їхнє розуміння ризиків кібербезпеки, передового досвіду та процедур. Це сприяє розвитку культури усвідомлення безпеки та відповідальності протягом усього життєвого циклу проєкту.
6. План реагування на інциденти	Розробка та впровадження плану реагування на інциденти, в якому описано процедури виявлення, реагування та відновлення після інцидентів і порушень безпеки. Це включає створення груп реагування на інциденти, визначення процедур ескалації та проведення регулярних тренувань і навчань реагування на інциденти.
7. Постійний моніторинг і вдосконалення	Впровадження механізмів постійного моніторингу для проактивного виявлення та реагування на загрози безпеці та вразливості в режимі реального часу. Крім того, регулярно переглядайте та оновлюйте політику, процедури та засоби контролю кібербезпеки на основі нових загроз, технологій і нормативних вимог.

Джерело: узагальнено авторкою за [5]

інформацію. Документи, бази даних, пристрої, хмарні сервери тощо залишаються в безпеці в рамках проєкту, який стає стійким завдяки впровадженню ISO 27001.

Безпека проєкту передбачає перевірку того, що всі артефакти проєкту мають належні протоколи доступу. Протокол доступу визначає, як користувач отримує доступ до певних ресурсів. Процес безпеки проєкту забезпечує, що члени команди мають доступ до необхідної інформації. Цей контроль також допомагає забезпечити більшу значимість і присутність інформаційної безпеки в управлінні проєктами організації, що завжди позитивно для даного сектора, так як розглядається не як проста вимога стандарту, а як критичний параметр при зверненні і реалізації будь-якого проєкту в організації.

Інформаційна безпека та конфіденційність повинні бути інтегровані в методологію управління проєктами організації. Це дозволяє виявляти, оцінювати, усувати та керувати ризиками інформаційної безпеки та конфіденційності в рамках проєкту. Такий підхід можна застосовувати до будь-якого проєкту, незалежно від його типу, будь то основний бізнес-процес, IT, управління обладнанням чи інші допоміжні процеси.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Захаренко К. Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток. Київ : Вид-во НПУ імені М.П. Драгоманова, 2017. 389 с.

2. Лазученков Д., Тоцький Р. Оцінка відповідності та впровадження системи управління інформаційною безпекою за стандартом ISO 27001. URL: https://www.ey.com/uk_ua/consulting/compliance-assessment-and-implementation-of-the-information-secu (дата звернення: 18.09.2024)

3. Редзюк В., Редзюк Н. Сучасні проблеми інформаційної безпеки України та напрями їх вирішення. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2023. № 3. С. 59–65. DOI: https://doi.org/10.31470/2786-6246-2023-3-59-65

4. Форос А.В. Інформаційна безпека як складова національної безпеки України. *Правова держава*. 2009. № 11. С. 222–226.

5. Cybersecurity in Project Management With Practical Examples. URL: https://bakkah.com/knowledge-center/cybersecurity-in-pm (дата звернення: 16.09.2024)

6. How to manage security in project management according to ISO 27001 A.5.8. URL: https://advisera.com/27001academy/how-to-manage-information-security-according-to-iso-27001/ (дата звернення: 16.09.2024)

7. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/en/standard/27001#promo (дата звернення: 16.09.2024)

REFERENCES:

1. Zakharenko K. (2017) Politychni instytuty informatsiinoi bezpeky Ukrainy: transformatsiia, modernizatsiia, rozvytok [Political institutions of information security of Ukraine: transformation, modernization, development]. Kyiv: Vyd-vo NPU imeni M.P. Drahomanova. 389 p. (in Ukrainian)

2. Lazuchenkov D., Totskyi R. Otsinka vidpovidnosti ta vprovadzhennia systemy upravlinnia informatsiinoiu bezpekoiu za standartom ISO 27001. [Compliance assessment and implementation of the information security management system according to the ISO 27001 standard]. Available at: https://www.ey.com/uk_ua/consulting/compliance-assessment-and-implementation-of-the-information-secu (accessed: 18.08.2024)

3. Redziuk, V., & Redziuk, N. (2023). Suchasni problemy informatsiinoi bezpeky Ukrainy ta napriamy yikh vyrishennia. [Modern problems of information security of Ukraine and ways to solve them]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia – Public administration: concepts, paradigm, development, improvement*, (3), 59–65. DOI: https://doi.org/10.31470/2786-6246-2023-3-59-65

4. Foros A.V. (2009) Informatsiina bezpeka yak skladova natsionalnoi bezpeky Ukrainy [Information security as a component of national security of Ukraine]. *Pravova derzhava – The Rule of Law*, 11, 222–226.

5. Cybersecurity in Project Management With Practical Examples. Available at: https://bakkah.com/knowledge-center/cybersecurity-in-pm (accessed: 16.09.2024)

6. How to manage security in project management according to ISO 27001 A.5.8. Available at: https://advisera.com/27001academy/how-to-manage-information-security-according-to-iso-27001/ (accessed: 16.08.2024)

7. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Available at: https://www.iso.org/en/standard/27001#promo (accessed: 16.08.2024)