Список використаних джерел:

1. Острога М.М., Юрченко А.О., Коровай А.О. Інформаційна гігієна та інформаційний шум. Академічні Візії, 2023. № 22. DOI: https://doi.org/10.5281/zenodo.8252019

2. Boichenko E., Martynovych N. Investment attractiveness of Territories in the context of restoring and stimulating the development of the post-war economy of Ukraine. Modern trends in the development of financial and innovation-investment processes in Ukraine. Materials of the VI International Scientific and Practical Conference March 2-3, 2023: a collection of scientific papers, Vinnytsia: VNTU, 2023, 445 p.

3. Аналітики пояснили подорожчання нафти і дали прогноз. Офіційний сайт РБК Україна. URL: https://www.rbc.ua/ukr/news/analitiki-obyasnili-podorozhanie-nefti-dali-1613465367.html (дата звернення 11.09.2024).

4. У 2014 році іноземні інвестиції в Україну впали на $12,2 млрд – аналітики. Офіційний сайт «КореспонденТ» URL: https://ua.korrespondent.net/business/ economics/3492829-u-2014-rotsi-inozemni-investytsii-v-ukrainu-vpaly-na-122-mlrd-analityky (дата звернення 11.09.2024).

Мащенко М.А.,
доктор економічних наук, професор,
завідувач кафедри економічної теорії та економічної політики,
Іпполітов Є.М.,
здобувач PhD,
Національний технічний університет України
«Харківський політехнічний інститут»

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС СПІВПРАЦІ ТА КОМУНІКАЦІЇ В ПРОЄКТНОМУ УПРАВЛІННІ

Під час управління проєктами захист інформації є критично важливим, оскільки проєкти все частіше залежать від цифрових технологій та хмарних сервісів, що робить їх вразливими до кіберзагроз. Незахищена інформація та

несанкціонований витік інформації може призвести до фінансових втрат, втрати довіри клієнтів та компрометації конфіденційних даних. Тому забезпечення безпеки даних стає обов'язковою умовою успішної реалізації проєктів, особливо в умовах глобалізації та віддаленої роботи проєктної команди.

Основні аспекти забезпечення та управління інформаційною безпекою підприємства розглянуто у працях [1, 2], що дозволяє визначити що ж являє собою інформаційна безпека. В загальному розумінні, це сукупність заходів, спрямованих на захист інформації від несанкціонованого доступу, розкриття, модифікації або знищення, з метою забезпечення її конфіденційності, цілісності та доступності. Крім того, можна погодитися з визначенням Велігури А.В., за яким, інформаційна безпека – комплекс заходів та засобів щодо забезпечення збереження інформації, що знаходиться в системі інформаційного забезпечення діяльності підприємства, переданої, оброблюваної, а також тієї, що зберігається та надається системою [3].

Деталізуємо це визначення до процесу управління проєктами. Забезпечення інформаційної безпеки в управлінні проєктами полягає у впровадженні комплексних технічних, організаційних та адміністративних заходів, які захищають проєктні дані від витоку, несанкціонованого доступу та інших кіберзагроз. Це включає, в сою чергу, використання сучасних технологій захисту, таких як шифрування, багатофакторна автентифікація, VPN, а також розробку політик безпеки, навчання співробітників (членів проєктної команди) та управління доступом до конфіденційної інформації. Такі заходи є необхідними для захисту проєктної інформації та збереження її конфіденційності, цілісності та доступності на всіх етапах проєкту.

Значна частина процесів автоматизується завдяки цифровим інструментам, таким як: системи управління проектами, хмарні платформи та засоби для командної співпраці. Ці технології дозволяють значно підвищити ефективність, полегшуючи обмін даними та комунікацію між учасниками проекту, незалежно від їхнього місцезнаходження. Однак зростання залежності

від цих технологій також збільшує ризики, пов’язані з кіберзагрозами та безпекою конфіденційної інформації.

Крім того, інформаційні потоки у проєктному управлінні є ключовим елементом координації між учасниками проєкту. Вони включають передачу планів, технічних вимог, фінансових даних, аналітичних звітів та іншої конфіденційної інформації, необхідної для успішної реалізації завдань. Ці потоки проходять через різні канали комунікації: електронну пошту, месенджери, системи управління проєктами, відеоконференції, хмарні сховища тощо [2].

Однією з важливих особливостей проєктного управління є значна кількість учасників з різним рівнем доступу до проєктних даних, що вимагає чіткого контролю за правами доступу. Дистанційна робота та співпраця з міжнародними командами підвищують складність управління інформаційними потоками, оскільки необхідно враховувати різні часові пояси, мовні бар'єри та технологічну інфраструктуру.

Основні загрози інформаційної безпеки в проєктному управлінні можна розділити на кілька категорій.

1. Кіберзагрози, основними серед яких можуть бути фішинг, шкідливе програмне забезпечення (ПЗ) та злом систем. Фішинг є однією з найпоширеніших загроз, коли зловмисники через підроблені електронні листи або вебсайти намагаються отримати конфіденційні дані користувачів, такі як паролі або банківські реквізити. Шкідливе ПЗ може поширюватися через заражені файли або програми та використовуватися для крадіжки інформації або порушення роботи систем. Злом систем, зазвичай, спрямований на отримання несанкціонованого доступу до внутрішніх баз даних або проєктних документів, що може призвести до втрати критично важливої інформації.

2. Витік конфіденційної інформації – може відбуватися через слабку систему захисту або неправильне налаштування доступу до проєктних даних. Це може призвести до потрапляння внутрішньої інформації до сторонніх осіб

або конкурентів. Часто витік інформації відбувається через недбалість, коли важливі документи передаються через незахищені канали або зберігаються на небезпечних серверах.

Основні канали витоку інформації (КВІ) наведено у табл.1 [3].

Таблиця 1

Види каналів витоку інформації

Класифікаційна ознака	Приклад КВІ
Форма проявлення інформації	засоби контролю акустичної (мовної) інформації; засоби контролю аналого-цифрової сигнальної інформації; засоби контролю об’ємно-видової сигнальної інформації
Технологія використання	внесені й швидко встановлювані спеціальні пристрої; заздалегідь установлювані заставні пристрої; засоби дистанційного контролю
Схеми й способи використання енергії	активні (випромінюючі) пристрої; пасивні (перевипромінюючі) пристрої; природні КВІ
Тип КВІ	оптичний (візуальний); провідний; бездротовий (радіо); що візуально контролюється (спостереження); акустичний (звуковий); електромагнітний; матеріально-речовинний

Розглянемо наступну групу ризиків, які можуть вплинути на інформаційну безпеку під час управління проєктами.

3. Ризики, пов'язані з людським фактором

Людський фактор є одним із найбільших ризиків для інформаційної безпеки. Недбалість співробітників, через використання слабких паролів, залишення незаблокованих пристроїв без нагляду або передача інформації через незахищені мережі, може стати причиною витоку даних. Помилки співробітників через випадкове видалення важливих файлів або надсилання документів не тому адресату, також є потенційною загрозою. Відсутність належного навчання з питань кібербезпеки підвищує ймовірність таких інцидентів.

Крім того, серед основних організаційних каналів також можуть бути такі: влаштування зловмисника на роботу у фірму, як правило, на технічну, допоміжну або другорядну посаду; установлення зловмисником довірчих взаємин зі співробітником фірми або особами, що мають право вільного доступу в даній фірмі; кримінальний, силовий доступ до інформації, тобто крадіжка документів, справ, дискет, дисків, комп'ютерів, шантаж до співробітництва окремих працівників, підкуп працівників, інсценування екстремальних ситуацій; одержання інформації з випадкового каналу [4].

Наведені загрози можуть мати серйозні наслідки для проєктів, включно з фінансовими втратами, репутаційними ризиками та порушенням контрактних зобов'язань.

Саме тому, захист інформації від витоку технічними каналами в проєктному управлінні потребує комплексного підходу, що включає розробку та реалізацію організаційних, первинних технічних та основних технічних заходів з використанням засобів технічного захисту інформації (ТЗІ).

Організаційні заходи, які спрямовані на встановлення чітких правил та процедур, які регулюють доступ до інформації та її обробку. Первинні технічні заходи, спрямовані на виявлення та запобігання можливим технічним шляхам витоку інформації. Основні технічні заходи, включають використання засобів ТЗІ, що забезпечують безпеку інформації через використання спеціалізованих засобів.

Отже, реалізація цих заходів дозволяє створити багаторівневу систему захисту інформації від витоків через технічні канали, забезпечуючи безпеку на кожному етапі роботи з проєктними даними.

Список використаних джерел:

1. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека». Уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.

2. Рач В.А. Проблеми захисту інформації в управлінні проектами в епоху економіки знань. *Управління проектами та розвиток виробництва: зб.наук.пр*. Луганськ: вид-во СНУ ім. В.Даля. 2009. № 2 (30). С. 156-160. URL: http://www.pmdp.org.ua/images/Journal/30/09rvaeez.pdf

3. Велігура А.В. Оцінювання стану інформаційної безпеки підприємства. *Управління проектами та розвиток виробництва*. 2014. № 4(52), С. 28-39.

4. Кавун С. В. Классификатор видов информации и форм документов. *Науковий вісник Полтавського університету споживчої кооперації України*. Сер. Економічні науки : наук. журнал. Полтава : РВВ ПУСКУ, 2009. № 5(36). С. 69–75.

Мірошниченко І.С.,
кандидат економічних наук,
доцент кафедри менеджменту авіаційної діяльності,
Сажіна А.В.,
здобувач вищої освіти,
Льотна академія Національного авіаційного університету

РОЛЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УПРАВЛІННІ ПРОЄКТАМИ

Програмне забезпечення (ПЗ) відіграє ключову роль у сучасному управлінні проєктами, значно підвищує ефективність використання ресурсів та забезпечує кращу координацію, контроль і прозорість у виконанні завдань.

ПЗ для управління проєктами — це набір інструментів, які допомагають керувати проєктами, планувати завдання, координувати роботу команди, контролювати прогрес та ефективно розподіляти ресурси [1].

Основні задачі ПЗ в управлінні проєктами:

1. Ефективне управління ресурсами, за допомогою ПЗ раціонально розподіляються ресурси, такі як: час, працівників, фінанси та матеріали. ПЗ допомагає відстежувати використання ресурсів, визначати їх наявність і планувати майбутні потреби.