3.10. Ensuring information security in the process of development and implementation of startup projects

Забезпечення інформаційної безпеки в процесі розробки та імплементації стартап-проєктів

В умовах цифрової трансформації бізнесу стартап-проєкти активно використовують інноваційні технології і це робить їх вразливими до кіберзагроз. Невеликі стартап-проєкти часто обмежені фінансовими та людськими ресурси, тому безпека часто відходить на другий план, що створює ризики для збереження конфіденційної інформації та інтелектуальної власності. Саме хакерські атаки, витоки даних, маніпуляції з цифровою репутацією та копіювання продукції конкурентами можуть критично вплинути на довіру інвесторів і потенційних клієнтів. Через фінансові обмеження багато стартапів використовують хмарні сервіси, відкритий код та сторонні API, що збільшує ризики несанкціонованого доступу до даних. Також важливим викликом є соціальна інженерія, коли зловмисники використовують методи психологічного впливу для отримання конфіденційної інформації, використовуючи сучасні можливості AI. Відсутність належної політики кібербезпеки може призвести до фінансових втрат і навіть закриття проєкту. Водночас дотримання сучасних стандартів інформаційної безпеки допомагає стартапам зберегти конкурентоспроможність і мінімізувати ризики. Особливо актуальним є питання захисту персональних даних користувачів відповідно до міжнародних регуляцій, таких як GDPR (Бачинський, 2025). Інвестори та партнери все більше звертають увагу на рівень безпеки, що робить цей аспект важливим для подальшого розвитку компанії, яка ініціює стартап-проєкти. Саме тому дослідження питання забезпечення інформаційної безпеки в стартап-проєктах є критично необхідним для їхнього сталого зростання та успішної імплементації

на ринку. Проблеми захисту інформації в системи управління підприємством досліджувалися українськими науковцями, серед яких можна відзначити таких науковців як: Кицюк В. М., Пупинін О. С., які розглядали теоретичні аспекти інформаційної безпеки (Кицюк, & Пупинін, 2024), Ясінську А. І., яка, в свою чергу, визначила концептуальні засади захисту інформації (Ясинська, 2023), Легенчук С. Ф., Назаренко Т. П. та Царук І. М. визначили принципи захисту даних у системі обліку (Легенчук та ін., 2021), Якименко Ю. М., Савченко В. А., Легомінова С. В. провели системний аналіз інформаційної безпеки (Якименко та ін., 2022). Проте деякі аспекти забезпечення високого рівня інформаційної безпеки в контексті імплементації стартап-проєктів потребують подальшого розвитку та уточнення.

Метою цієї роботи є визначення чинників забезпечення інформаційної безпеки в процесі розробки та імплементації стартап-проєктів.

За словами Прохорової В. В. та Чобіток В. І., діяльність стартапів зосереджена на створенні тимчасової, невеликої організації, метою якої є пошук масштабованої, повторюваної та прибуткової бізнес-моделі в умовах невизначеності. Вони характеризуються міжнародною спрямованістю, незалежністю, відкритістю та здатністю виходити за межі традиційних організаційних структур (Прохорова, & Чобіток, 2023). Скорик Г. І., Недошитко А. А. зазначають, що проблеми та ризики, пов’язані з реалізацією стартапів, а також їхня важлива роль у розвитку сучасної інноваційної економіки, зумовлюють необхідність їхньої системної підтримки. Вони пропонують виділити такі основні напрямки: «розвиток культури підприємництва за сприяння закладів освіти; створення сприятливого інвестиційного клімату, насамперед, на засадах стабільності економічної політики; створення законодавчих засад, що регламентують правові, економічні, соціальні аспекти стартапів; інформаційна підтримка, підтримка участі у міжнародних проектах; надання фінансової підтримки з метою

активізації підприємництва; посилення соціальної спрямованості стартап-проектів» (Скорик, & Недошитко, 2021). Як можна побачити, що одним із факторів є інформаційна підтримка, яка, в свою чергу, повинна бути розглянута комплексно і всебічно.

Таким чином, стартапи завжди відрізняються високим рівнем невизначеності, оскільки вони часто реалізуються у нових або недостатньо розвинених (досліджених) ринкових нішах. Це означає, що стратегія, бізнес-модель і технологічні рішення можуть швидко змінюватися залежно від реакції ринку, поведінки конкурентів та зворотного зв'язку від користувачів. Така динамічність призводить до того, що питання інформаційної безпеки можуть вважатися не першочерговими завданнями, які потребують вирішення, адже основна увага приділяється розробці продукту, залученню інвестицій та виходу на ринок. Прискорений темп розвитку також створює ризик впровадження неперевірених рішень, які можуть містити вразливості або не відповідати сучасним стандартам безпеки. Крім того, можливі зміни командних гравців (прихід нових співробітників, залучення фрілансерів), що може збільшувати ймовірність витоку конфіденційних даних або неналежного керування доступами.

Також більшість стартапів на початковій стадії мають обмежене фінансування, що змушує їх економити на всіх можливих витратах, включаючи заходи кібербезпеки. Витрати на спеціалізоване програмне забезпечення для захисту даних, залучення фахівців з інформаційної безпеки або аудит кіберзахисту часто сприймаються як вторинні у порівнянні з розробкою мінімально життєздатного продукту (MVP) чи маркетинговими кампаніями. У стартапах може бути обмежена команда, тому відповідальність за безпеку покладається на розробників, які не завжди мають достатню експертизу в цій сфері. Це може призводити до використання слабких паролів, неналежного керування ключами API, недостатнього шифрування або відсутності резервного

копіювання даних. Як наслідок, стартапи стають легкою мішенню для хакерських атак, які можуть призвести до серйозних фінансових та репутаційних втрат.

Стартапи часто використовують сторонні технології, такі як хмарні сервіси (AWS, Google Cloud, Azure), бібліотеки з відкритим кодом та API для прискорення розробки продукту. Це дозволяє значно скоротити час на створення власних рішень, але водночас створює потенційні ризики для безпеки. Так, у відкритому коді можуть міститися вразливості, які стануть точкою входу для атак на стартап-проєкт. Крім того, стартапи не завжди регулярно оновлюють залежності, що підвищує ризик експлуатації відомих уразливостей. Використання сторонніх API може також нести загрозу витоку даних, якщо немає належного контролю за тим, як передається та зберігається інформація. У разі неправильного налаштування хмарних сервісів конфіденційні дані можуть опинитися у відкритому доступі, що часто трапляється через недостатню кваліфікацію розробників або поспіх у процесі розробки. Тому, особливості стартап-проєктів як об’єкту уваги, створюють значні виклики для інформаційної безпеки, які потребують системного підходу та ретельного контролю з перших етапів розвитку компанії.

На початкових стадіях стартапи є особливо вразливими до кіберзагроз через обмежені ресурси та низьку пріоритетність заходів кібербезпеки. Молоді компанії та засновники стартап проєктів часто використовують швидкі та недорогі технологічні рішення, які можуть містити вразливості. Це може бути і неналежний захист веб-додатків, і слабкі паролі або незахищені бази даних, які можуть стати точками входу для атак. Хакери можуть скористатися недостатньо захищеною інфраструктурою для крадіжки даних, маніпуляцій із вихідним кодом або навіть вимагання викупу, за допомогою атак програм-вимагачів. Окрім цього, стартапи можуть стати жертвами DDoS-атак, які виводять з ладу їхні сервіси, що критично для компаній, які реалізуют спартапи

та працюють у сфері SaaS або онлайн-торгівлі. Через відсутність резервних копій або стратегій реагування на кіберінциденти такі атаки можуть призвести до серйозних фінансових втрат і навіть закриття проєкту.

Важливого значення набуває витік конфіденційної інформації, бо вона є одним із найцінніших активів стартапу, особливо коли йдеться про інтелектуальну власність, бізнес-стратегію або фінансові дані. Витік даних може статися як через зловмисні дії шляхом атаки з боку конкурентів або хакерів, так і через внутрішню недбалість (відсутність контролю доступу, використання незахищених каналів передачі інформації, людські помилки). Витоки можуть поставити під загрозу відносини з інвесторами, які прагнуть гарантій безпеки своїх вкладень. Якщо стартап не може захистити свої дані, це може знизити довіру партнерів і потенційних клієнтів, а також поставити під загрозу його майбутнє фінансування. Особливо небезпечно, коли витік зачіпає персональні дані користувачів, оскільки це може спричинити юридичні проблеми та штрафи згідно з міжнародними регламентами, такими як GDPR або CCPA (California Consumer Privacy Act) (Гуменюк, 2025).

Крім того, стартапи та їх засновники часто стають мішенню фішингових атак, коли зловмисники намагаються отримати доступ до важливих облікових записів через підроблені електронні листи або вебсайти. Недосвідчені співробітники можуть випадково надати свої облікові дані або завантажити шкідливі файли, що відкриє доступ до корпоративної інформації. Соціальна інженерія також є серйозною загрозою, оскільки шахраї можуть видавати себе за потенційних інвесторів, партнерів або навіть співробітників компанії, щоб маніпулювати людьми та отримувати доступ до критичних даних. Ще одна загроза – атаки на цифрову репутацію, коли хакери або конкуренти розповсюджують неправдиву інформацію, підроблені відгуки або компрометуючі матеріали, щоб підірвати довіру клієнтів та інвесторів. Оскільки репутація є ключовим фактором успіху для молодих компаній, подібні атаки

можуть мати довготривалі негативні наслідки. Стартапи повинні усвідомлювати ці загрози та впроваджувати ефективні стратегії захисту, щоб мінімізувати ризики та забезпечити стабільний розвиток.

Що стосується захисту інформації, то шифрування є одним із найефективніших способів захисту конфіденційних даних стартапу, особливо коли йдеться про особисту інформацію клієнтів, фінансові транзакції та внутрішню документацію. Використання сучасних криптографічних методів, таких як AES-256 для збережених даних та TLS (Transport Layer Security) для передачі інформації, значно знижує ризик несанкціонованого доступу. Стартапи, що працюють у сфері фінтеху, охорони здоров'я або e-commerce, повинні впроваджувати шифрування на рівні баз даних, резервних копій та внутрішніх комунікацій. Також важливо використовувати двофакторну автентифікацію (2FA) та апаратні ключі безпеки для захисту доступу до критичних систем. Окрім цього, рекомендується регулярно оновлювати політики управління ключами шифрування та перевіряти систему на наявність вразливостей.

Стартапи повинні не лише технічно захищати свої дані, а й застосовувати юридичні інструменти, які допоможуть запобігти витоку конфіденційної інформації. Одним із найпоширеніших методів є угода про нерозголошення (NDA – Non-Disclosure Agreement), яка забезпечує юридичну відповідальність працівників, підрядників, партнерів та потенційних інвесторів за розголошення комерційних таємниць. У NDA слід чітко визначати, які саме дані є конфіденційними, як вони мають зберігатися та якими будуть наслідки за порушення угоди. Крім NDA, варто укладати угоди про захист інтелектуальної власності (IP Protection Agreements) із розробниками програмного забезпечення та дизайнерами, щоб уникнути можливих конфліктів щодо прав на код чи унікальні технологічні рішення. Додатково, реєстрація патентів, товарних

знаків або авторських прав допоможе захистити ключові напрацювання стартапу від копіювання та недобросовісної конкуренції.

Наступним фактором є ефективне управління зберіганням та передачею даних. Цей процес є критично важливим для мінімізації ризику їхнього витоку або компрометації. Стартапи повинні використовувати надійні хмарні сервіси, які відповідають міжнародним стандартам безпеки (наприклад, ISO 27001, SOC 2) (ISO/IEC 27001:2022, 2022), та забезпечувати регулярне резервне копіювання даних у зашифрованому вигляді. Важливо також контролювати рівні доступу, застосовуючи принцип мінімальних привілеїв, щоб запобігти витоку інформації через недбалість або внутрішні загрози. Передача конфіденційних даних між співробітниками та партнерами повинна здійснюватися лише через захищені канали, наприклад, за допомогою VPN, зашифрованих месенджерів або протокол SFTP (Secure File Transfer Protocol), який шифрує не тільки управляючі команди, але й дані, що передаються. Використання механізмів контрольованого доступу (RBAC – Role-Based Access Control) дозволяє обмежити можливість отримання даних тими, хто не має на це відповідних прав.

Отже, захист інтелектуальної власності та конфіденційної інформації вимагає комплексного підходу, який включає як технологічні, так і юридичні заходи. Впровадження цих рішень допоможе стартапу мінімізувати ризики втрати критичних даних та забезпечити довіру інвесторів і клієнтів.

Так як, інформаційна безпека є критично важливим елементом функціонування стартапів, особливо в умовах цифрової економіки, то необхідно визначити ключові фактори забезпечення інформаційної безпеки, які допоможуть стартапам мінімізувати ризики кіберзагроз. До ключових факторів можно віднести такі: впровадження політик інформаційної безпеки; технологічні рішення для захисту даних; кібергігієна та підготовка персоналу.

Розглянемо більш детально кожну складову та узагальнимо основні елементи політики інформаційної безпеки у Таблиці 1.

Таблиця 1

Фактори, що забезпечують дотримання інформації безпеки в стартап проєктах

Політики інформаційної безпеки (основні елементи)	Технологічні рішення для захисту даних	Кібергігієна та підготовка персоналу
1) управління доступом; 2) парольна політика; 3) резервне копіювання; 4) політика використання пристроїв; 5) реагування на інциденти	1) шифрування даних; 2) використання VPN та захищені з'єднання; 3) захист веб-додатків моніторинг загроз; 4) антивірусне ПЗ та виявлення й реагування на кінцеві точки (Endpoint Detection and Response (EDR); 5) автоматизовані оновлення операційних систем	1) навчання персоналу; 2) безпечне поводження з паролями; 3) обережність із зовнішніми носіями інформації; 4) контроль доступу; 5) симуляції атак

Джерело: власна розробка авторів

Політики інформаційної безпеки – це набір правил і процедур, які визначають підходи компанії до захисту інформації, контролю доступу, обробки та зберігання даних. Для стартапів особливо важливо розробити гнучкі, але водночас ефективні політики, які будуть відповідати їхнім бізнес-процесам і можливостям. Технологічні заходи є основою інформаційної безпеки в будь-якій компанії. Стартапи можуть використовувати сучасні інструменти, які забезпечують захист від атак, витоків даних та інших кіберзагроз. Людський фактор залишається однією з головних причин витоків інформації та успішних хакерських атак. Навіть найкращі технологічні рішення не принесуть результатів, якщо співробітники не розумітимуть основ безпеки та не будуть дотримуватися правил кібергігієни.

Отже, стартапи повинні документувати політики інформаційної безпеки та проводити регулярний аудит їх дотримання. Це може значно знизити ризик втрати даних та фінансових збитків у разі кібератаки. Стартапи повинні

будувати культуру кібербезпеки з перших днів роботи компанії, оскільки це допоможе мінімізувати ризики та захистити критично важливу інформацію. Практичне забезпечення інформаційної безпеки вимагає комплексного підходу, який включає впровадження політик, використання технологічних рішень та навчання персоналу. Стартапи, які приділяють увагу цим аспектам, значно підвищують свої шанси на успіх, знижують ризики фінансових та репутаційних втрат і створюють довгострокову довіру серед клієнтів, партнерів та інвесторів.

Далі розглянемо певні аспекти забезпечення інформаційної безпека на етапі імплементації стартап-проєктів. Після успішного запуску стартап-проєкту компанія стикається з новими викликами, пов’язаними з безпекою. Масштабування бізнесу, зростання користувацької бази та збільшення кількості інтеграцій із зовнішніми сервісами підвищують ризики кіберзагроз. На цьому етапі критично важливо впроваджувати ефективні механізми захисту IT-інфраструктури, проводити моніторинг інформаційної безпеки та бути готовими до можливих інцидентів. З розширенням стартапу змінюється його IT-інфраструктура: з’являються нові сервери, бази даних, API, інтеграції з хмарними платформами та сторонніми сервісами. Це створює додаткові вразливості, які можуть використати кіберзлочинці.

Основні заходи захисту під час масштабування стартапу наведено в Таблиці 2.

Для забезпечення безперервного захисту необхідно впроваджувати системи моніторингу, які в реальному часі аналізують активність у мережі та виявляють підозрілі дії. Основні компоненти моніторингу інформаційної безпеки груповано та розглянуто у Таблиці 3.

Таким чином, аудит інформаційної безпеки повинен проводитися щонайменше раз на квартал, а звітність за результатами моніторингу допоможе швидко реагувати на нові загрози.

Таблиця 2

Розроблення заходів захисту під час масштабування стартапу

(узагальнено авторами)

Назва	Сутність
1. Безпечна хмарна інфраструктура	використання захищених серверів, які відповідають міжнародним стандартам безпеки (AWS, Google Cloud або Azure із сертифікатами ISO 27001);
2. Мережева безпека	налаштування VPN, мережевих екранів (firewalls), віртуальних приватних хмар (VPC) та систем виявлення вторгнень (IDS/IPS);
3. Автоматизація безпеки	використання DevSecOps-підходу, при якому заходи безпеки впроваджуються на всіх етапах розробки та розгортання програмного забезпечення;
4. Захист API	обмеження доступу до API за допомогою токенів автентифікації (OAuth, JWT), шифрування запитів і налаштування rate limiting для запобігання DDoS-атакам;
5. Резервне копіювання	створення зашифрованих резервних копій даних із можливістю швидкого відновлення у разі втрати чи атаки програм-вимагачів;
6. Проведення регулярного тестування на проникнення	перевірка безпеки системи перед її масштабуванням

Проте, незважаючи на всі заходи безпеки, жодна система не є абсолютно захищеною від атак. Тому стартапу необхідно мати чіткий план реагування на інциденти (Incident Response Plan, IRP) та план аварійного відновлення (Disaster Recovery Plan, DRP).

На Рис. 1 наведено основні етапи реагування на інциденти для стартап-проєктів.

На першому етапі визначаються загрози, шляхом швидкої ідентифікації ознак кібератаки або витоку даних за допомогою SIEM та інших систем моніторингу. Далі оцінюється масштабу через аналіз впливу інциденту на роботу стартапу та прояв потенційних ризиків. На третьому етапі відбувається локалізація проблеми за допомогою ізоляції скомпрометованих систем, з метою запобігання поширення атаки. Четвертий етап спрямовано на відновлення безпеки шляхом усунення вразливостей, відновлення роботи сервісів та оновлення безпекових політик. Обов’язком є останній етап, на якому

відбувається документування інциденту, бо ведення звітності є необхідною умовою для подальшого аналізу та розроблення заходів з покращення захисту інформації. Необхідно також розглядати можливість швидкого відновлення даних шляхом створення гарячих резервних копій, які можна миттєво активувати у разі збою, також потрібно використовувати відмовостійкі сервери із можливістю автоматичного перемикання на резервні ресурси та регулярне тестування DRP, з метою перевірки ефективності процесів відновлення після можливих атак чи технічних збоїв. Ідеальний варіант, коли стартапи мають команду реагування на інциденти, яка відповідатиме за швидке усунення загроз та комунікацію з клієнтами у разі кібератаки.

Таблиця 3

Компоненти моніторингу інформаційної безпеки

(узагальнено авторами)

Назва компоненти	Сутність
1) SIEM-системи (Security Information and Event Management)	аналіз журналів подій (логів), виявлення аномалій та автоматичне реагування на підозрілі активності;
2) SOC (Security Operations Center)	якщо стартап швидко розвивається, доцільно залучати спеціалізованих фахівців або віддавати на аутсорс послуги кібербезпеки;
3) контроль доступу	використання механізмів мультифакторної аунтефікації (MFA) та регулярний аудит прав доступу для запобігання внутрішнім загрозам;
4) моніторинг користувацької активності	аналіз поведінки користувачів для виявлення нетипових дій;
5) тестування на вразливості	регулярне сканування системи на наявність незакритих вразливостей

На етапі імплементації стартап-проєктів зростає потреба в комплексних заходах щодо забезпечення інформаційної безпеки. Захист IT-інфраструктури, постійний моніторинг загроз та готовність до кіберінцидентів є ключовими факторами успішного розвитку стартапу. Впровадження цих заходів допоможе

не лише захистити дані, але й забезпечити стабільність бізнес-процесів, що критично важливо для залучення інвесторів та довіри клієнтів.

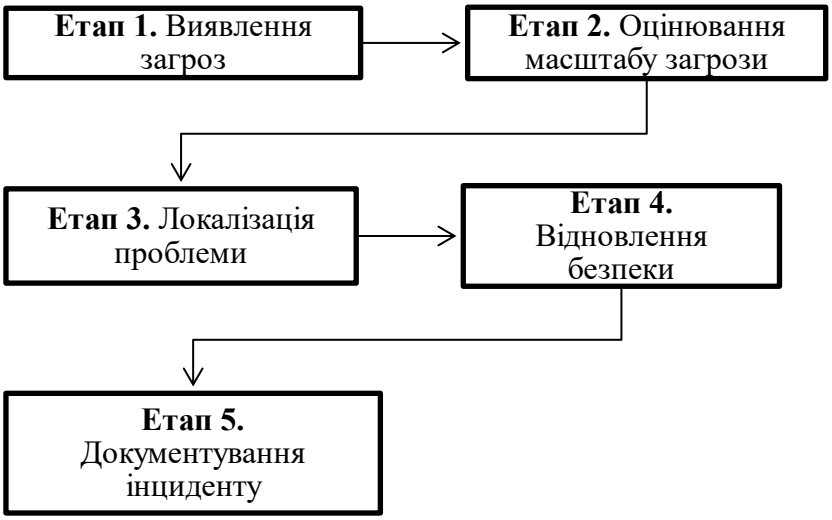

Рис. 1. Послідовність реагування на інциденти в стартап-проєктах

Джерело: власна розробка авторів

Отже, в умовах цифровізації бізнесу стартапи стикаються з низкою унікальних викликів у сфері інформаційної безпеки, серед яких основними є: висока невизначеність та обмежені ресурси, які не дозволяють впроваджувати складні та дорогі системи кіберзахисту; використання відкритого коду та сторонніх сервісів, що підвищує ризики вразливостей. Основними загрозами для стартап-проєктів є кіберзлочинність, витоки даних, фішингові атаки, соціальна інженерія та атаки на цифрову репутацію. Крім того, захист інтелектуальної власності потребує використання шифрування, юридичних механізмів (NDA, патентування) та безпечного зберігання інформації. На етапі масштабування стартапу зростають ризики атак, тому необхідно впроваджувати системи моніторингу, аудитів безпеки та планів аварійного відновлення. Таким чином, для ефективного управління кіберризиками стартап-проєкти повинні застосовувати комплексний підхід, що включає технологічні, організаційні та юридичні заходи.

Для підвищення рівня інформаційної безпеки стартапам рекомендується дотримуватися наступних принципів:

- розробити політику інформаційної безпеки через визначення рівня доступу для співробітників (принцип мінімальних привілеїв); регламентування використання паролів, двофакторної автентифікації (2FA) та менеджерів паролів;

- впровадити сучасні технологічні рішення шляхом шифрування даних, використання VPN для захисту віддаленого доступу, регулярного оновлення ПЗ для усунення вразливостей;

- захистити інтелектуальну власність та конфіденційну інформацію шляхом використання NDA (Non-Disclosure Agreement) для співробітників і партнерів, обмеження доступу до критично важливих даних, патентування унікальних технологічних рішень;

- забезпечити безпеку при масштабуванні, а саме впроваджувати SIEM-системи для моніторингу загроз, використовувати віртуальні приватні хмари для захисту веб-додатків, регулярно проводити аудит безпеки;

- підготуватися до можливих інцидентів шляхом розроблення плану реагування на кібератаки та аварійне відновлення, проведення навчання персоналу з основ кібергігієни, ведення журналу інцидентів та аналізувати їх для вдосконалення систем безпеки.

Стартапи, які впроваджують ці заходи, зменшують ризики кібератак, захищають свою репутацію та підвищують довіру клієнтів та інвесторів.

В майбутньому розвиток інформаційних систем зможе забезпечити подальший розвиток таких автоматизованих систем кібербезпеки:

- використання штучного інтелекту та машинного навчання для виявлення загроз у реальному часі;
- адаптація Zero Trust моделі для стартапів;
- захист даних у Web3 та блокчейн-проєктах.

Щодо ролі регулювання та стандартів у кібербезпеці стартапів, то може стати можливим дослідження впливу європейських стандартів (GDPR, NIS2) та американських норм (CISA, SOC 2) на безпеку технологічних стартапів, також розроблення рекомендацій щодо адаптації регуляторних вимог для невеликих бізнесів. В аспекті соціальної інженерії та методів протидії, можна виокремити: вивчення нових тактик фішингових атак й методів їх виявлення та аналіз ефективності навчальних програм для учасників стартапів.

Отже, можна зазначити, що інформаційна безпека є важливою умовою сталого розвитку стартап-проєктів. Незахищеність від кіберзагроз може призвести до значних репутаційних та фінансових втрат, тому компаніям варто впроваджувати комплексні підходи щодо захисту даних, починаючи з ранніх етапів діяльності. Використання сучасних технологій, обґрунтована політика управління ризиками та навчання персоналу допоможуть мінімізувати загрози та забезпечити стабільне зростання стартапу в умовах цифрової економіки.

Література

Бачинський, Т. (2025). *Що таке GDPR та чи варто його виконувати поза межами ЄС*. URL: https://legalaid.ua/ua/shho-take-gdpr/
(дата звернення 15. 03. 2025).

Гуменюк, В. (2025). *CPRA для бізнесу: чому CCPA недостатньо?* URL: https://legalitgroup.com/cpra-dlya-biznesu-chomu-ccpa-nedostatno/ (дата звернення 15. 03. 2025).

Кицюк, В. М., Пупинін, О. С. (2024). Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації,* 2 (58), 103-108. https://doi.org/10.31673/2409-7292.2024.020012.

Легенчук, С. Ф., Назаренко, Т. П., & Царук, І. М. (2021). Принципи захисту даних у системі обліку: управлінські аспекти. *Економіка, управління та адміністрування*. (2 (96)), 61-69.

Прохорова, В. В., Чобіток, В. І. (2023). Стратегічний розвиток стартапів в інноваційному середовищі. *БізнесІнформ*. (9), 325-330. https://doi.org/10.32983/2222-4459-2023-9-325-330.

Скорик, Г. І., & Недошитко, А. А. (2021). Розвиток стартапів в Україні: проблеми та перспективи. *Вісник Хмельницького національного університету*. (6, Том 1), 65-69. https://doi.org/10.31891/2307-5740-2021-300-6-11.

Якименко, Ю. М., Савченко, В. А., & Легомінова, С. В. (2022). *Системний аналіз інформаційної безпеки: сучасні методи управління: підручник*. Державний університет телекомунікацій.

Ясинська, А. (2023). Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство* (56). https://doi.org/10.32782/2524-0072/2023-56-118.

ISO/IEC 27001:2022 (2022). Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001 (дата звернення 15. 03. 2025).