**Аналіз поточної ситуації з інформаційною безпекою компанії «TechScooter»**

**Вступ**

Інформаційна безпека стала не просто технічним напрямом, а стратегічною основою для сучасного бізнесу. Компанія TechScooter, яка працює у сфері мікромобільності, обробляє великі обсяги персональних і фінансових даних користувачів, що створює високі вимоги до захисту інформації. У зв’язку з цим було прийнято рішення про впровадження Системи Керування Інформаційною Безпекою (ISMS) відповідно до стандарту ISO/IEC 27001:2022. Ця робота є логічним продовженням попередніх досліджень, які охоплювали аналіз інцидентів, аудит доступу, розробку політик та оцінку ризиків.

На ранніх етапах ми визначили ключові переваги впровадження ISMS для TechScooter: підвищення довіри клієнтів, зниження ризику кіберінцидентів та оптимізація внутрішніх процесів. Було проведено аналіз нормативних вимог - як локальних (ЗУ «Про захист персональних даних»), так і міжнародних (GDPR, ISO/IEC 27005, NIST). На основі цього сформували обґрунтовану область дії ISMS, яка охоплює критичні процеси: мобільний застосунок, хмарну інфраструктуру AWS, блокчейн-сервери та платіжну систему FinPay.

У частині Gap-аналізу спробував оцінити рівень зрілості процесу доступу до даних клієнтів у блокчейні. Це стало основою для розробки рекомендацій щодо впровадження MFA, RBAC, журналювання та аудиту доступу. Далі створив політику використання мобільних пристроїв, яка враховує BYOD, MDM, шифрування та контроль мереж. Це дозволило закріпити вимоги безпеки на рівні кінцевих точок.

Важливою частиною роботи стала ідентифікація загроз, вразливостей та їх впливу на конфіденційність, цілісність і доступність інформації. Заповнив матрицю ризиків. На основі цього був обґрунтований варіант обробки ризику шахрайських транзакцій (Fraud Detection System, 3D Secure, аудит FinPay).

Далі спробував пояснити важливість моніторингу та аналізу ризиків, ідентифікував (сподіваюсь вірно) наслідки їх відсутності, до них відніс втрату сертифікації та бізнес-довіри. Було складено список документованої інформації для забезпечення безперервності бізнесу, включаючи BCP, DRP, IRP, BIA та реєстр активів. Звернув увагу на контроль доступу, виявив критично важливі заходи, принаймні старався виявити ті які не були реалізовані.

Розробив заходи безпеки для реагування на інциденти, створення безпечного середовища розробки, захисту мережі та управління активами.

У процесі підготовки звертався до нормативних документів, офіційних джерел, а також до практик корпоративної безпеки.

|  |
| --- |
| **Частина 1. Причини проходження сертифікації відповідно до вимог міжнародного стандарту інформаційної безпеки ISO/IEC 27001** |

**Причини проходження сертифікації ISO/IEC 27001 для TechScooter.**

**З урахуванням стратегічних цілей компанії в галузі інформаційної безпеки**

1. *Підвищення довіри клієнтів і партнерів*

**Обґрунтування:**

TechScooter обробляє персональні та фінансові дані користувачів через мобільний застосунок, інтеграцію з платіжною системою FinPay та хмарну інфраструктуру AWS. Сертифікація ISO/IEC 27001 демонструє відповідність міжнародним стандартам безпеки, що зміцнює репутацію компанії, підвищує довіру з боку клієнтів, інвесторів, партнерів та регуляторів.

**Конкретний приклад:**

Після інциденту з витоком даних Android-застосунку, компанія втратила частину активних користувачів. Сертифікація дозволить публічно підтвердити, що впроваджено заходи захисту, зокрема MFA, контроль доступу, аудит, що знижує ризик повторення інциденту.

**Зв’язок зі стратегічними цілями:**

TechScooter прагне стати надійним постачальником цифрових послуг у сфері мікромобільності. Довіра клієнтів - ключовий фактор для масштабування бізнесу, особливо при виході на нові ринки та залученні інвесторів

ISO/IEC 27001:2022, розділ 4.2 - Understanding the needs and expectations of interested parties

GDPR Art. 32 - Security of processing

1. *Зниження ризику витоку даних та кіберінцидентів*

**Обґрунтування:**

TechScooter вже стикалася з серйозними інцидентами: вразливість нульового дня, крадіжка самокатів через перепрошивку, компрометація Android-застосунку. Впровадження ISMS дозволяє системно управляти ризиками, впроваджувати технічні та організаційні контролі (MFA, DLP, IAM), проводити аудит, моніторинг та реагування на інциденти.

**Конкретний приклад:**

Після впровадження ISMS компанія може автоматизувати аудит доступу до хмарного блокчейн-сервера, впровадити журналювання та обмежити доступ до персональних даних лише авторизованим ролям. Це зменшить ризик несанкціонованого доступу, який був виявлений під час внутрішнього аудиту.

**Зв’язок зі стратегічними цілями:**

TechScooter має на меті забезпечити безперервність бізнесу та захист даних користувачів як основу своєї конкурентної переваги. Зниження ризиків - ключ до стабільності та відповідності регуляторним вимогам.

ISO/IEC 27001:2022, Annex A.5-A.1 - Control objectives and controls

NIST SP 800-30 - Risk Management Guide

1. *Оптимізація внутрішніх процесів і відповідність законодавству*

**Обґрунтування:**

ISMS допомагає впорядкувати процеси розробки, тестування, доступу до даних, реагування на інциденти. Це особливо важливо для TechScooter, де CISO схвалює використання реальних даних у тестах. Сертифікація також забезпечує відповідність GDPR, ЗУ «Про захист персональних даних» та вимогам ISO/IEC 27001.

**Конкретний приклад:**

Впровадження політики управління доступом дозволить автоматизувати відкликання прав після звільнення співробітників, що раніше не контролювалося. Це усуне ризик використання облікових даних колишніх працівників, як було виявлено під час аудиту.

**Зв’язок зі стратегічними цілями:**

TechScooter прагне до масштабованості, автоматизації та відповідності міжнародним стандартам. Оптимізація процесів - це основа для інтеграції безпеки в життєвий цикл розробки та підтримки сервісу.

ISO/IEC 27001:2022, розділ 6 - Planning

ЗУ «Про захист персональних даних», ст. 24 - Впровадження технічних і організаційних заходів

|  |
| --- |
| **Частина 2. Встановлення контексту ISMS** |

**Встановлення контексту ISMS для TechScooter**

**Відповідно до ISO/IEC 27001:2022, ISO/IEC 27005:2022, GDPR, ЗУ «Про захист персональних даних»**

1. *Причини впровадження ISMS*

Впровадження Системи Керування Інформаційною Безпекою (ISMS) для TechScooter є стратегічно важливим з таких причин:

**Захист персональних і фінансових даних користувачів**

* Компанія обробляє чутливу інформацію через мобільний застосунок, блокчейн і платіжні сервіси.
* Відповідність вимогам GDPR (ст. 32) та ЗУ «Про захист персональних даних» (ст. 24) є обов’язковою.

**Зниження ризику кіберінцидентів**

* Виявлені вразливості нульового дня, крадіжки самокатів, компрометація Android-застосунку - ці факти свідчення того, що компанія потребує системного управлінні ризиками.

**Підготовка до сертифікації ISO/IEC 27001**

* Сертифікація забезпечує конкурентну перевагу, підвищує довіру клієнтів і партнерів, особливо у співпраці з FinPay та AWS.

1. *Вимоги локального законодавства та міжнародних стандартів*

|  |  |
| --- | --- |
| Джерело | Вимоги |
| ЗУ «Про захист персональних даних» | Впровадження технічних та організаційних заходів захисту (ст. 24) |
| GDPR (ЄС) | Захист персональних даних, повідомлення про інциденти (ст. 32 - 34) |
| ISO/IEC 27001:2022 | Встановлення контексту, управління ризиками, впровадження контролів |
| ISO/IEC 27005:2022 | Ідентифікація, оцінка та обробка ризиків |
| ISO/IEC 27017/27018 | Захист даних у хмарному середовищі |

1. *Основні активи компанії TechScooter*

|  |  |  |
| --- | --- | --- |
| Актив | Значення для бізнесу | Зв’язок з ISMS |
| Мобільний застосунок (iOS/Android) | Основний інтерфейс користувача | Вимагає контролю доступу, захисту даних, оновлень |
| Хмарна інфраструктура (AWS) | Зберігання даних, блокчейн, бекенд | Вимагає шифрування, IAM, аудит, відповідність ISO |
| Блокчейн-сервери | Незмінність даних, GPS, маршрут, користувачі | Вимагає контролю доступу, захисту API, журналювання |
| Платіжна система (FinPay) | Обробка транзакцій, аналітика | Вимагає відповідності PCI DSS, захисту фінданих |
| Сервери бази даних | Зберігання персональних даних | Вимагає шифрування, MFA, контроль доступу |
| Розробницька інфраструктура | CI/CD, тестування, вихідний код | Вимагає контролю змін, ізоляції середовищ |
| Персонал (розробники, CISO) | Управління доступом, тестування, релізи | Вимагає навчання, політик, розмежування ролей |

ISO/IEC 27001:2022, Annex A.5.9 - Inventory of information and other associated assets

ISO/IEC 27002:2022 - Asset management controls

1. *Основні процеси діяльності, що впливають на інформаційну безпеку*

**Розробка та тестування застосунку**

* Впливає на безпеку коду, доступ до реальних даних, CI/CD процеси
* Потребує контролю змін, ізоляції середовищ, затвердження релізів

**Обробка персональних даних користувачів**

* Вимагає шифрування, DLP, політик доступу, відповідності GDPR

**Інтеграція з FinPay**

* Потребує захисту фінансових даних, відповідності PCI DSS

**Використання хмарних сервісів AWS**

* Вимагає IAM, MFA, CSPM, аудит конфігурацій

**Управління самокатами через блокчейн**

* Потребує захисту API, контролю доступу, журналювання

**Реагування на інциденти та технічне обслуговування**

* Вимагає Incident Response Plan, повідомлення користувачів, резервування

ISO/IEC 27001:2022, Annex A.6–A.17 - Control domains

NIST SP 800-53 Rev. 5 - CM, AC, IR, AU families

|  |
| --- |
| **Частина 3. Визначення області дії ISMS** |

**Визначення області дії ISMS компанії TechScooter**

**Відповідно до ISO/IEC 27001:2022, розділ 4.3; ISO/IEC 27005:2022; GDPR; ЗУ «Про захист персональних даних»**

1. *Область дії ISMS: формулювання*

Система керування інформаційною безпекою (ISMS) компанії TechScooter охоплює процеси розробки, тестування, розгортання та обслуговування мобільного застосунку для iOS та Android, хмарну інфраструктуру (AWS), блокчейн-сервери, платіжну систему FinPay, управління персональними та фінансовими даними користувачів.

1. *Межі області дії ISMS*

Включено:

* Мобільні застосунки (вихідний код, CI/CD, релізи)
* Хмарні сервери (бекенд, блокчейн, API)
* Сервери бази даних (локальні та хмарні)
* Платіжна система FinPay (інтеграція, обробка транзакцій)
* Персональні дані користувачів (GDPR, ЗУ)
* Інфраструктура для розробників (доступ, контроль змін)
* Ролі CISO, DevOps (\*DevSecOps), QA, розробники

Виключено (на етапі початкової сертифікації):

* Фізична безпека офісу (відеоспостереження, охорона)
* Внутрішні HR-процеси
* Маркетингові кампанії та аналітика поза FinPay
* Всі неінтегровані сторонні сервіси

ISO/IEC 27001:2022, розділ 4.3 - Determining the scope of the ISMS

ISO/IEC 27001:2022, Annex A.5.9 - Inventory of assets

1. *Обґрунтування вибору області*

*Додаткова цінність для клієнтів:*

**Захист персональних та фінансових даних**

* Клієнти отримують гарантію, що їхні дані обробляються відповідно до ISO/IEC 27001 та GDPR.

**Безпека мобільного застосунку**

* Основний інтерфейс взаємодії з сервісом -захищений, протестований, контрольований.

**Надійність платіжної системи**

* Інтеграція з FinPay - сертифікована, прозора, з контролем доступу.

*Обмеження для початкової сертифікації:*

**Фокус на критичних процесах**

* Зменшення обсягу аудиту, концентрація на найбільш ризикованих компонентах.

**Швидша підготовка до сертифікації**

* Менше документів, менше контролів, чітка межа відповідальності.

**Можливість поетапного розширення ISMS**

* Після сертифікації - поступове включення HR, фізичної безпеки, маркетингу.

1. *Відповідність нормативним вимогам*

* ***GDPR (ст. 32 - 34):*** Захист персональних даних, повідомлення про інциденти
* ***ЗУ «Про захист персональних даних» (ст. 24):*** Впровадження технічних та організаційних заходів
* ***ISO/IEC 27001:2022:*** Визначення області, управління ризиками, впровадження контролів
* ***ISO/IEC 27017/27018:*** Захист даних у хмарному середовищі

|  |
| --- |
| **Частина 4. Gap-аналіз** |

**Gap-аналіз процесу доступу до даних клієнтів у блокчейні**

**Відповідно до ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005:2022, GDPR, ЗУ «Про захист персональних даних»**

1. *Оцінка рівня зрілості процесу доступу*

На основі аналізу політик, практик та інфраструктури TechScooter, рівень зрілості процесу доступу до даних клієнтів у блокчейні оцінюється як ***низький (Initial/Ad-hoc)*** за моделлю Capability Maturity Model (CMM) та критеріями ISO/IEC 27001.

|  |  |
| --- | --- |
| Критерій оцінки | Поточний стан |
| Наявність політики управління доступом | Відсутня або неформалізована |
| Впровадження контролів доступу | Частково реалізовано, без MFA, без RBAC |
| Аудит доступу | Не проводиться регулярно, немає журналів |
| Відповідність цілям ISMS | Не визначено метрик ефективності, немає KPI |
| Перевірка в процесі аудиту | Не визначено метрик ефективності, немає KPI |

ISO/IEC 27001:2022 Annex A.5.15–A.5.1 - Access control policy, user authentication, access rights review

ISO/IEC 27002:2022, розділ 5 - Identity and access management

GDPR Art. 32 - Security of processing

NIST SP 800-53 Rev. 5 - AC-2, AC-3, AC-6, IA-2, AU-2

1. *Виявлені прогалини*

* Відсутність формалізованої політики управління доступом
* Відсутність багатофакторної автентифікації (MFA)
* Проблеми з RBAC (не реалізовано)
* Адміністратори мають надмірні привілеї до даних клієнтів
* Відсутність журналювання доступу до блокчейн-сервера
* Немає регулярного аудиту прав доступу
* Відсутність метрик ефективності ISMS щодо доступу

1. *Рекомендації щодо покращення процесу*

|  |  |  |
| --- | --- | --- |
| Категорія | Рекомендація | Очікуваний ефект |
| Політика доступу | Розробити та затвердити політику управління доступом | Встановлення чітких правил, відповідність ISO/IEC 27001 |
| Рольова модель доступу | Впровадити RBAC з чітким розмежуванням прав (розробник, адміністратор, CISO) | Обмеження надмірних привілеїв, принцип Least Privilege |
| Автентифікація | Впровадити MFA для всіх доступів до блокчейн-сервера | Зниження ризику компрометації облікових записів |
| Журналювання | Впровадити централізоване логування доступу (CloudTrail, SIEM) | Можливість розслідування інцидентів, відповідність GDPR |
| Аудит доступу | Проводити щоквартальний аудит прав доступу та API-запитів | Виявлення надлишкових прав, відповідність ISO/IEC 27001 A.5.18 |
| Метрики ISMS | Визначити KPI для контролю доступу (кількість інцидентів, час реагування) | Оцінка ефективності заходів, підвищення рівня зрілості |
| API-контроль | Встановити обмеження на API-запити, Token-доступ | Захист від автоматизованих атак, контроль зовнішніх інтеграцій |

1. *Очікуваний результат*

Впровадження зазначених рекомендацій дозволить:

* Підвищити рівень зрілості процесу до **керованого (Managed)** або **оптимізованого (Optimized)**
* Забезпечити відповідність вимогам ISO/IEC 27001, GDPR, ЗУ
* Підвищити ефективність ISMS у частині контролю доступу
* Зменшити ризики витоку даних та несанкціонованого доступу

|  |
| --- |
| **Частина 5. Розробка політик інформаційної безпеки** |

|  |  |
| --- | --- |
| Політика використання мобільних пристроїв/TechScooter | |
| Ціль | Забезпечити безпечне використання мобільних пристроїв (смартфонів, планшетів, ноутбуків, портативних засобів зв’язку) в корпоративному середовищі TechScooter, мінімізуючи ризики витоку даних, несанкціонованого доступу та порушення вимог інформаційної безпеки |
| Вступ | У зв’язку з виявленими інцидентами, пов’язаними з використанням незашифрованих мобільних пристроїв, компанія TechScooter впроваджує політику контролю мобільного середовища. Політика базується на принципах ISO/IEC 27001:2022 (Annex A.6.2), ISO/IEC 27002:2022, NIST SP 800-124 Rev. 2 та положеннях GDPR щодо захисту персональних даних. |
| Область дії політики | Політика застосовується до всіх співробітників, підрядників, консультантів та третіх сторін, які використовують мобільні пристрої для доступу до інформаційних систем TechScooter, незалежно від того, чи є пристрій власністю компанії або особистим (BYOD). |
| Мета | * Захист конфіденційної, персональної та фінансової інформації * Встановлення вимог до безпечного використання мобільних пристроїв * Забезпечення відповідності нормативним вимогам (GDPR, ЗУ, ISO) * Зменшення ризику втрати, крадіжки або компрометації даних |
| Обов’язки | * ***Користувачі*:** дотримання вимог політики, повідомлення про інциденти * ***ІТ-відділ*:** впровадження MDM, контроль доступу, аудит пристроїв * ***CISO:*** моніторинг відповідності, оновлення політики, реагування на порушення * ***HR:*** ознайомлення нових співробітників з політикою, фіксація порушень |
| Ключові завдання політики | * Реєстрація пристроїв у системі MDM * Встановлення антивірусного ПЗ та шифрування даних * Заборона використання незахищених мереж (публічний Wi-Fi) * Автоматичне блокування екрана після 5 хвилин бездіяльності * Заборона встановлення сторонніх додатків без перевірки * Вимога регулярного оновлення ОС та застосунків * Впровадження MFA для доступу до корпоративних ресурсів |
| Наслідки недотримання вимог політики | * Тимчасове або постійне блокування доступу до корпоративних систем * Дисциплінарні заходи згідно з внутрішніми регламентами * Повідомлення про інцидент до CISO та юридичного відділу * Відшкодування збитків у випадку доведеного порушення |
| Пов’язані політики | * Політика управління доступом (ISO/IEC 27001 A.5.15) * Політика захисту персональних даних (GDPR, ЗУ) * Політика реагування на інциденти (ISO/IEC 27035) * Політика безпечного використання хмарних сервісів (ISO/IEC 27017) |

|  |
| --- |
| **Частина 6. Ідентифікація загроз, вразливостей та їх впливу** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Сценарій ризику | Загроза | Вразливість | Вплив | К | Ц | Д |
| Облікові дані колишнього співробітника все ще використовуються | Несанкціонований доступ | Відсутність процедури деактивації облікових записів | Компрометація даних, порушення політик доступу | A scared face |  |  |
| Неправильне значення в CLI призвело до відключення сервера | Внутрішня помилка/людський фактор | Відсутність обмежень на критичні команди, слабкий контроль | Зупинка сервісу, втрата доступу, можливе порушення цілісності даних |  |  |  |
| Втрата бета-версії через несправність жорстких дисків | Втрата даних | Відсутність резервного копіювання, слабкий моніторинг | Втрата критичного коду, затримка релізу, порушення безперервності розробки |  |  |  |
| Використання слабких паролів співробітниками | Злам облікових записів | Відсутність політики складності паролів | Несанкціонований доступ до систем, витік даних, порушення GDPR |  |  |  |
| Недостатній контроль доступу до хмарного блокчейн-сервера | Несанкціонований доступ до даних | Відсутність MFA, слабка рольова модель, відкриті порти | Компрометація персональних і фінансових даних, порушення ISO/IEC 27001, GDPR |  |  |  |

|  |
| --- |
| \*ризик впливає на відповідний аспект (К, Ц, Д) - |
| \*ризик не має прямого впливу на відповідний аспект - |

|  |
| --- |
| **Частина 7. Варіант обробки ризиків** |

**Обробка ризику шахрайських транзакцій**

**Відповідно до ISO/IEC 27005:2022, ISO/IEC 27001:2022 Annex A.5.4, NIST SP 800-30, PCI DSS**

*Сценарій ризику*

* ***Тип ризику:*** Фінансовий та репутаційний
* ***Опис:*** 0,5% транзакцій (приблизно 50 000 USD(можливо, потрібні точні підрахунки)) є шахрайськими
* ***Джерело:*** Зовнішні зловмисники, компрометовані картки, фішинг
* ***Вплив:*** Прямі фінансові втрати, порушення довіри клієнтів, можливі юридичні наслідки

*Варіанти обробки ризику*

|  |  |  |
| --- | --- | --- |
| Опція | Опис | Доцільність |
| Зниження | Впровадження технічних та організаційних заходів для зменшення ймовірності або вплив | *Найбільш доцільний варіант*: дозволяє зменшити частку шахрайства без зупинки бізнесу |
| Уникнення | Повна відмова від прийому кредитних карток | *Недоцільно*: суперечить бізнес-моделі, знижує доступність сервісу |
| Передача | Передача ризику сторонній організації (страхування, платіжний процесор) | *Частково можливо*: FinPay може взяти на себе частину відповідальності, але не повністю |
| Прийняття | Усвідомлення ризику без активного втручання | *Можливо лише як тимчасове рішення, якщо витрати на захист перевищують втрати* |

*Рекомендований підхід: Зниження ризику*

**Обґрунтування:**

TechScooter має технічні можливості та партнерство з FinPay, що дозволяє впровадити заходи з виявлення та блокування шахрайських транзакцій. Зниження ризику забезпечує:

* Відповідність стандарту ***PCI DSS***
* Захист фінансових інтересів компанії
* Підвищення довіри клієнтів
* Зменшення юридичних ризиків

Рекомендовані заходи для зниження ризику

* Впровадження ***системи виявлення шахрайства*** (Fraud Detection System)
* Використання ***3D Secure*** для підтвердження транзакцій
* Аналіз поведінкових патернів користувачів
* Впровадження ***лімітів транзакцій*** та географічного моніторингу
* Співпраця з FinPay для ***автоматичного блокування підозрілих операцій***
* Регулярний аудит платіжної системи відповідно до ***PCI DSS Requirement 10***

ISO/IEC 27005:2022 - Risk treatment options

PCI DSS v4.0 - Requirements 6, 10, 12

NIST SP 800-30 - Risk mitigation strategies

|  |
| --- |
| **Частина 8. Процес керування моніторингом та аналізом ризиків** |

**Важливість моніторингу та аналізу процесу управління ризиками**

**Відповідно до ISO/IEC 27001:2022, ISO/IEC 27005:2022, NIST SP 800-137, GDPR**

1. *Чому це критично для TechScooter*

Моніторинг і аналіз процесу управління ризиками є фундаментальними для ефективного функціонування ISMS компанії TechScooter.

Вони забезпечують:

**Актуальність заходів безпеки**

* Загрози та вразливості змінюються динамічно. Без моніторингу - заходи стають застарілими.

**Виявлення нових ризиків**

* Вразливість нульового дня у застосунку Android була виявлена лише під час аудиту. Регулярний моніторинг дозволяє виявляти подібні інциденти раніше.

**Оцінку ефективності ISMS**

* Відстеження KPI, інцидентів, часу реагування - дозволяє коригувати політики та процедури.

**Відповідність нормативним вимогам**

* ISO/IEC 27001:2022, розділ 9.1 вимагає регулярного аналізу ефективності ISMS. GDPR (ст. 32) - постійне забезпечення безпеки обробки даних.

ISO/IEC 27001:2022 - Clause 9.1: Monitoring, measurement, analysis and evaluation

NIST SP 800-137 - Information Security Continuous Monitoring (ISCM)

GDPR Art. 32 - Security of processing

1. *Ризики у разі відмови від моніторингу*

|  |  |
| --- | --- |
| Ризик | Потенційний вплив на діяльність компанії (business disruption) |
| Виявлення інцидентів із запізненням | Несвоєчасне реагування - витік даних - штрафи - втрата довіри клієнтів |
| Накопичення вразливостей у застосунку або інфраструктурі | Експлуатація критичних вразливостей - зупинка сервісу - фінансові втрати |
| Невідповідність нормативним вимогам (GDPR, ISO) | Втрата сертифікації - юридичні наслідки - обмеження на ринок - репутаційні збитки |

1. *Висновок*

Для TechScooter моніторинг та аналіз ризиків -це ***стратегічна необхідність***, що забезпечує:

* Безперервність бізнесу
* Захист клієнтських даних
* Відповідність міжнародним нормам
* Гнучкість реагування на нові загрози

|  |
| --- |
| **Частина 9. Основний список документованої інформації** |

**Основний список документованої інформації для забезпечення безперервності бізнесу**

**відповідно до ISO/IEC 27001:2022, ISO/IEC 22301:2019, ISO/IEC 27031:2011 та NIST SP 800 - 34 Rev. 1**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Назва документу | Призначення | Відповідність стандартам |
|  | Політика безперервності бізнесу (BCP Policy) | Визначає загальні принципи, цілі та обов’язки щодо забезпечення безперервності | SO/IEC 22301:2019, ISO/IEC 27001:2022 A.5.29 |
|  | Оцінка впливу на бізнес (Business Impact Analysis, BIA | Ідентифікує критичні процеси, допустимий час простою, фінансові та репутаційні наслідки | ISO/IEC 22301:2019 Clause 8.2 |
|  | Оцінка ризиків для безперервності (Continuity Risk Assessment) | Визначає загрози, вразливості та сценарії порушення безперервності | ISO/IEC 27005:2022, ISO/IEC 22301:2019 Clause 6.1 |
|  | План реагування на інциденти (Incident Response Plan, IRP) | Описує процедури реагування на кіберінциденти, включаючи ролі, етапи та комунікацію | ISO/IEC 27035:2016, ISO/IEC 27001:2022 A.5.24 |
|  | План аварійного відновлення (Disaster Recovery Plan, DRP) | Визначає технічні заходи для відновлення ІТ-систем після збою або атаки | ISO/IEC 27031:2011, NIST SP 800-34 Rev. 1 |
|  | План забезпечення безперервності бізнесу (Business Continuity Plan, BCP) | Конкретні сценарії, процедури, ресурси та відповідальні особи для підтримки критичних процесів | ISO/IEC 22301:2019 Clause 8.4 |
|  | Реєстр активів та критичності (Asset Register with Criticality Levels) | Перелік ІТ-активів, їх класифікація за критичністю, залежність від них бізнес-процесів | ISO/IEC 27001:2022 A.5.9, A.5.10 |
|  | Політика резервного копіювання та відновлення (Backup and Restore Policy) | Визначає частоту, типи, місця зберігання та процедури тестування резервних копій | ISO/IEC 27001:2022 A.5.30, A.5.31 |
|  | Політика комунікації під час кризи (Crisis Communication Policy) | Регламентує внутрішню та зовнішню комунікацію у випадку інциденту або порушення безперервності | ISO/IEC 22301:2019 Clause 8.4.3 |
|  | Протокол тестування планів (Testing and Exercising Protocol) | Описує методи перевірки ефективності BCP/DRP, включаючи симуляції, навчання та аудит | ISO/IEC 22301:2019 Clause 9.1 |
|  | Реєстр інцидентів та заходів реагування (Incident Log and Response Register) | Фіксує всі інциденти, дії, час реагування, ефективність заходів | ISO/IEC 27001:2022 A.5.25 |
|  | Політика управління доступом під час аварій (Emergency Access Control Policy) | Визначає правила доступу до критичних систем у випадку інциденту або аварії | ISO/IEC 27001:2022 A.5.15, A.5.18 |

|  |
| --- |
| **Частина 10. Контроль доступу** |

**Аналіз відсутніх заходів контролю доступу**

**Відповідно до ISO/IEC 27001:2022 Annex A.5.15-A.5.18, ISO/IEC 27002:2022, GDPR, NIST SP 800-53 Rev. 5**

1. *Політика управління доступом*

**Опис заходу:**

Формалізована політика, яка регламентує правила надання, зміни та відкликання доступу до інформаційних систем.

**Відсутність дії чи контролю:**

TechScooter не має затвердженої політики, що визначає, хто і як отримує доступ до PII

**Наслідки**:

* Відсутність єдиного підходу до контролю доступу
* Ризик надмірних привілеїв
* Порушення ISO/IEC 27001:2022 A.5.15

1. *Багатофакторна автентифікація (MFA)*

**Опис заходу:**

Використання двох або більше факторів для підтвердження особи користувача.

**Відсутність дії чи контролю:**

Віддалені розробники автентифікуються лише за паролем.

**Наслідки**:

* Підвищений ризик компрометації облікових записів
* Несанкціонований доступ до PII
* Порушення GDPR ст. 32

1. *Рольова модель доступу (RBAC)*

**Опис заходу:**

Надання доступу на основі ролі користувача, відповідно до його функціональних обов’язків.

**Відсутність дії чи контролю:**

Розробники мають доступ до даних, які не є необхідними для їхньої роботи.

**Наслідки**:

* Надмірні привілеї
* Ризик внутрішніх загроз
* Порушення принципу Least Privilege

1. *Аудит прав доступу*

**Опис заходу:**

Регулярна перевірка відповідності наданих прав фактичним потребам користувача.

**Відсутність дії чи контролю:**

TechScooter не проводить аудит доступу до хмарної бази даних.

**Наслідки**:

* Накопичення надлишкових прав
* Втрата контролю над критичними ресурсами
* Порушення ISO/IEC 27001:2022 A.5.18

1. *Журналювання доступу (Access Logging)*

**Опис заходу:**

Фіксація всіх дій користувачів у системі, зокрема доступу до PII.

**Відсутність дії чи контролю:**

Немає записів про дії віддалених розробників.

**Наслідки**:

* Неможливість розслідування інцидентів
* Порушення GDPR ст. 33
* Невідповідність ISO/IEC 27001:2022 A.5.17

1. *Відокремлення середовищ (Dev/Test/Prod)*

**Опис заходу:**

Ізоляція середовищ розробки, тестування та продакшена для уникнення випадкового доступу до реальних даних.

**Відсутність дії чи контролю:**

Розробники тестують застосунок на реальних даних без ізоляції.

**Наслідки**:

* Ризик витоку PII
* Порушення принципу захисту даних за замовчуванням (GDPR ст. 25)

1. *Контроль доступу до API*

**Опис заходу:**

Обмеження доступу до API, що взаємодіє з хмарною базою даних, через токени, rate-limiting, ACL.

**Відсутність дії чи контролю:**

API відкритий для широкого доступу без обмежень.

**Наслідки**:

* Ризик автоматизованих атак
* Несанкціонований доступ до PII
* Порушення ISO/IEC 27001:2022 A.8.23

1. *Відкликання доступу після звільнення*

**Опис заходу:**

Автоматичне або контрольоване відкликання доступу після завершення трудових відносин.

**Відсутність дії чи контролю:**

Облікові дані колишніх співробітників залишаються активними.

**Наслідки:**

* Несанкціонований доступ
* Високий ризик внутрішніх атак
* Порушення ISO/IEC 27001:2022 A.5.20

1. *Верифікація пристроїв (Endpoint Validation)*

**Опис заходу:**

Перевірка безпеки пристроїв, з яких здійснюється доступ до корпоративних ресурсів.

**Відсутність дії чи контролю:**

Віддалені пристрої не перевіряються на відповідність політикам безпеки.

**Наслідки**:

* Ризик зараження шкідливим ПЗ
* Компрометація даних через незахищені пристрої
* Порушення ISO/IEC 27001:2022 A.5.32

1. *Контроль геолокації доступу*

**Опис заходу:**

Обмеження доступу до систем залежно від географічного розташування користувача

**Відсутність дії чи контролю:**

Доступ дозволено з будь-якої точки світу без географічних обмежень.

**Наслідки**:

* Ризик атак з країн з високим рівнем кіберзагроз
* Втрата контролю над зовнішнім периметром
* Порушення принципу захисту на рівні мережі (ISO/IEC 27033)

|  |
| --- |
| **Частина 11. Заходи безпеки** |

1. *Реагування на інциденти інформаційної безпеки*

Впровадження програми моніторингу зловмисного програмного забезпечення (Malware)

* ***Опис*:** Систематичне виявлення, класифікація та блокування шкідливого ПЗ на всіх пристроях.
* ***Результат*:** Зменшення ризику зараження систем, підвищення стійкості до атак.
* ***Приклад дії:*** Встановлення EDR-рішень (наприклад, SentinelOne), налаштування автоматичного реагування.

Розробка Incident Response Plan (IRP)

* ***Опис:*** Документована процедура реагування на кіберінциденти.
* ***Результат:*** Швидке реагування, мінімізація збитків, відповідність ISO/IEC 27035.
* ***Приклад дії:*** Створення IRP з ролями, сценаріями, контактами, каналами комунікації.

Призначення групи реагування на інциденти (IRT)

* ***Опис:*** Формування команди з CISO, ІТ-фахівців, юристів.
* ***Результат:*** Координація дій, ефективне управління інцидентами.
* ***Приклад дії:*** Визначення складу IRT, графік чергувань, внутрішній регламент.

Впровадження системи реєстрації інцидентів

* ***Опис:*** Централізований журнал інцидентів з фіксацією часу, типу, дій.
* ***Результат:*** Аналітика, звітність, відповідність GDPR ст. 33.
* ***Приклад дії:*** Інтеграція SIEM-системи (наприклад, Splunk), налаштування логування.

Проведення навчання персоналу щодо реагування

* ***Опис:*** Ознайомлення співробітників з процедурами реагування.
* ***Результат:*** Зменшення людського фактору, швидке повідомлення про інциденти.
* ***Приклад дії:*** Проведення щоквартальних тренінгів, симуляцій фішингових атак.

1. *Безпечне середовище розробки*

Ізоляція середовищ (Dev/Test/Prod)

* ***Опис:*** Розділення середовищ для уникнення випадкового доступу до продуктивних даних.
* ***Результат:*** Зменшення ризику витоку даних, відповідність принципу Least Privilege.
* ***Приклад дії:*** Налаштування окремих віртуальних середовищ, обмеження доступу.

Заборона використання реальних даних у тестах

* ***Опис:*** Використання псевдонімізованих або синтетичних даних.
* ***Результат:*** Захист PII, відповідність GDPR ст. 25.
* ***Приклад дії:*** Впровадження генератора тестових даних, шифрування зразків.

Контроль змін у коді (Change Management)

* ***Опис:*** Відстеження всіх змін у коді з фіксацією авторства та часу.
* ***Результат:*** Прозорість, можливість відкату, аудит.
* ***Приклад дії:*** Впровадження Git з pull request review, журнал змін.

Статичний та динамічний аналіз коду

* ***Опис:*** Виявлення вразливостей до релізу.
* ***Результат:*** Зменшення ризику нульового дня, підвищення якості ПЗ.
* ***Приклад дії:*** Інтеграція SAST/DAST у CI/CD (наприклад, SonarQube, OWASP ZAP).

Обмеження доступу до репозиторіїв

* ***Опис:*** Доступ лише за ролями, з MFA.
* ***Результат*:** Захист вихідного коду, зменшення ризику внутрішніх загроз.
* ***Приклад дії:*** Налаштування GitHub RBAC, обов’язкова MFA для комітів.

1. *Заходи безпеки мережі*

Мережева сегментація (VLAN)

* ***Опис:*** Розділення мережі на зони з різним рівнем доступу.
* ***Результат:*** Обмеження lateral movement, ізоляція критичних систем.
* ***Приклад дії:*** Налаштування VLAN для серверів, розробників, гостьових пристроїв.

Впровадження фаєрволів та IDS/IPS

* ***Опис:*** Фільтрація трафіку, виявлення атак.
* ***Результат:*** Захист периметру, моніторинг загроз.
* ***Приклад дії:*** Встановлення pfSense, інтеграція Suricata.

Шифрування мережевого трафіку

* ***Опис:*** Використання TLS 1.2+ для всіх з’єднань.
* ***Результат:*** Захист від MITM, відповідність ISO/IEC 27033.
* ***Приклад дії:*** Налаштування HTTPS, VPN, SFTP.

VPN для віддаленого доступу

* ***Опис:*** Безпечне з’єднання з корпоративною мережею.
* ***Результат:*** Захист даних, контроль доступу.
* ***Приклад дії:*** Встановлення OpenVPN, обмеження доступу за IP.

Аудит відкритих портів

* ***Опис:*** Перевірка мережевих конфігурацій на наявність незахищених точок.
* ***Результат:*** Зменшення площі атаки, відповідність ISO/IEC 27001 A.8.22.
* ***Приклад дії:*** Використання Nmap, регулярні сканування.

1. *Припустиме використання ресурсів компанії (використання активів)*

Політика припустимого використання (AUP)

* ***Опис:*** Документ, що регламентує правила роботи з активами.
* ***Результат:*** Зменшення ризику зловживань, підвищення дисципліни.
* ***Приклад дії:*** Затвердження AUP, ознайомлення співробітників.

Реєстр активів з класифікацією

* ***Опис:*** Перелік ІТ-ресурсів з позначенням критичності.
* ***Результат:*** Прозорість, контроль, відповідність ISO/IEC 27001 A.5.9.
* ***Приклад дії:*** Створення реєстру в CMDB, призначення відповідальних.

Заборона використання незареєстрованих пристроїв

* ***Опис:*** Доступ до систем лише з перевірених пристроїв.
* ***Результат:*** Зменшення ризику зараження, контроль середовища.
* ***Приклад дії:*** Впровадження MDM, whitelist MAC-адрес.

Моніторинг використання ресурсів

* ***Опис:*** Відстеження активності користувачів та пристроїв.
* ***Результат:*** Виявлення порушень, аналітика.
* ***Приклад дії:*** Встановлення агентів на пристрої, інтеграція з SIEM.

Навчання персоналу щодо використання активів

* ***Опис:*** Ознайомлення з правилами, відповідальністю.
* ***Результат:*** Зменшення людського фактора, підвищення культури безпеки.
* ***Приклад дії:*** Проведення тренінгів, тестування знань.

|  |
| --- |
| **Частина 12. Програма підвищення обізнаності та навчання** |

**Програма підвищення обізнаності та навчання з питань інформаційної безпеки**

**з урахуванням стандартів ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST SP 800-50, GDPR та практик корпоративної безпеки**

1. ***Важливість впровадження програми навчання та обізнаності***

В умовах цифрової трансформації та зростання кількості кіберзагроз, людський фактор залишається одним із найвразливіших елементів системи інформаційної безпеки. Відсутність програми навчання в компанії TechScooter призвела до того, що співробітники:

* Не змогли розпізнати ознаки фішингових атак
* Не повідомили про інциденти своєчасно
* Використовували слабкі паролі та незахищені пристрої
* Порушували політики доступу до персональних даних

ISO/IEC 27001:2022 Annex A.6.3 - Information security awareness, education and training

NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program

GDPR Art. 32 - Security of processing (організаційні заходи)

1. ***Цілі програми навчання***

* Формування культури інформаційної безпеки
* Зниження ризику інцидентів, пов’язаних з людськими помилками
* Підвищення відповідальності співробітників за захист даних
* Забезпечення відповідності нормативним вимогам (ISO, GDPR, ЗУ)
* Підготовка персоналу до реагування на інциденти

1. ***Заходи для успішного впровадження програми***

|  |  |  |  |
| --- | --- | --- | --- |
| № | Захід | Опис | Очікуваний результат |
|  | Розробка політики навчання та обізнаності | Документ, що регламентує формат, періодичність, відповідальних осіб | Стандартизація процесу, відповідність ISO/IEC 27001 |
|  | Створення навчальних модулів за ролями | Розробка контенту для розробників, HR, CISO, підтримки, менеджменту | Актуальність навчання, підвищення ефективності засвоєння |
|  | Проведення регулярних тренінгів та вебінарів | Щоквартальні сесії з прикладами реальних інцидентів, фішингових атак | Зниження ризику компрометації через соціальну інженерію |
|  | Інтерактивні симуляції інцидентів (tabletop exercises, Red Team) | Практичне моделювання ситуацій: витік даних, фішинг, DDoS | Підготовка до реальних загроз, формування навичок реагування |
|  | Впровадження системи оцінки знань (тести, сертифікація) | Перевірка засвоєння матеріалу, мотивація до навчання | Визначення рівня обізнаності, персоналізоване навчання |
|  | Візуальна кампанія (плакати, інфографіка, внутрішній портал) | Розміщення нагадувань про правила безпеки, поради, чек-листи | Постійне нагадування, формування звичок |
|  | Впровадження механізму повідомлення про інциденти (анонімно або відкрито) | Канал для швидкого інформування CISO про підозрілу активність | Зменшення часу реагування, залучення співробітників до захисту |
|  | Інтеграція навчання в процес адаптації нових співробітників | Ознайомлення з політиками безпеки з першого дня роботи | Формування відповідального ставлення з початку трудових відносин |
| 9. | Аналіз результатів навчання та коригування програми | Оцінка ефективності, оновлення контенту відповідно до нових загроз | Гнучкість програми, актуальність матеріалів |
| 10. | Залучення керівництва до програми (лідерство, приклад, участь у тренінгах) | Демонстрація важливості безпеки на рівні топ-менеджменту | Підвищення мотивації персоналу, формування корпоративної культури безпеки |

1. ***Дії для забезпечення успішності та ефективності програми***

* Визначити ***відповідального за навчання*** (наприклад, CISO або Security Awareness Officer)
* Встановити ***KPI програми***: % (відсоток) пройдених курсів, кількість повідомлень про інциденти, рівень знань
* Забезпечити ***доступність навчання***: онлайн-платформа, мобільна версія, гнучкий графік
* Впровадити ***мотиваційні механізми***: сертифікати, внутрішні рейтинги, бонуси
* Забезпечити ***персоналізацію навчання***: адаптація під рівень знань, роль, ризики

1. ***Очікуваний вплив на інформаційну безпеку TechScooter***

* Зниження кількості інцидентів, спричинених людським фактором
* Підвищення рівня відповідальності та залученості персоналу
* Відповідність вимогам ISO/IEC 27001, GDPR, ЗУ «Про захист персональних даних»
* Покращення загального стану інформаційної безпеки компанії
* Формування культури безпеки як частини корпоративної етики

**Висновок**

Підсумовуючи проведену роботу, можна стверджувати, що впровадження ISMS для TechScooter є не просто вимогою стандарту, а стратегічною необхідністю. Пройшовши повний цикл - від обґрунтування до розробки політик, аналізу ризиків, створення процедур та навчальних програм. Кожен розділ був пов’язаний з попереднім, що забезпечило цілісність дослідження. А можливо десь вдалось заглибитись більше в процес створення документу.

Я старався не обмежуватись теоретичними положеннями - кожну рекомендацію підкріплював прикладом, нормативним джерелом та очікуваним результатом. Можливо, це дозволить використовувати матеріал як основу для майбутнього аудиту, сертифікації або внутрішнього впровадження ISMS. Я старався врахувати специфіку TechScooter - мобільний застосунок, блокчейн, FinPay, AWS - і адаптувати заходи безпеки до цих технологій (хоча б постарався).

У процесі роботи звертався до офіційних джерел: ISO/IEC 27001, 27005, 27017, GDPR, NIST SP 800-30, SP 800-137. Частину інформації шукав у Google, щоб уточнити терміни, практики та приклади. Сподіваюсь, це дозволило зберегти актуальність і відповідність міжнародним вимогам.

Не можна не згадати, що в цій роботі мені допомагав AI - інтелектуальний асистент, який не просто відповідав, а став повноцінним учасником процесу. Я сперечався щодо формулювань, структури, обсягу. Його поради щодо нормативних посилань, формулювання політик, побудови таблиць були надзвичайно корисними. Дійсно якщо використовувати його як «вчителя», який швидко відповість на твої питання він збереже добрий кусок часу.

Завдяки цьому створено політику використання мобільних пристроїв, виявлено прогалини в контролі доступу, змодельовано сценарії ризику, розроблено програму навчання та сформовано повний список документованої інформації (тут AI на висоті).

Але най головне, що треба розуміти, що інформаційна безпека починається не з технологій, а з **відповідальності**.

**Словник термінів використовуваних у роботі**

**DLP (Data Loss Prevention)**

Технологія, що запобігає витоку конфіденційної інформації за межі організації. Контролює передачу даних через мережу, пристрої та хмарні сервіси. Застосовується для захисту PII, фінансових та комерційних даних.

**ISMS (Information Security Management System)**

Системний підхід до управління інформаційною безпекою в організації. Включає політики, процедури, контролі та аудит. Відповідає стандарту ISO/IEC 27001.

**IAM (Identity and Access Management)**

Механізми управління цифровими ідентичностями та правами доступу користувачів. Забезпечує автентифікацію, авторизацію та аудит. Ключовий компонент безпеки в хмарних і корпоративних системах.

**CISO (Chief Information Security Officer)**

Вищий керівник, відповідальний за стратегію та реалізацію заходів інформаційної безпеки. Координує політики, реагування на інциденти та відповідність стандартам. Взаємодіє з керівництвом і технічними командами.

**AWS (Amazon Web Services)**

Хмарна платформа, що надає інфраструктуру, обчислювальні ресурси, сховища та сервіси безпеки. Використовується для масштабування бізнесу та зберігання даних. Сертифікована за ISO/IEC 27001, 27017, 27018.

**PCI DSS (Payment Card Industry Data Security Standard)**

Міжнародний стандарт безпеки для захисту даних платіжних карток. Вимагає шифрування, моніторинг, контроль доступу та аудит. Обов’язковий для компаній, що обробляють транзакції з картками.

**CI/CD (Continuous Integration / Continuous Deployment)**

Методологія автоматизації розробки, тестування та розгортання програмного забезпечення. CI - інтеграція змін у коді, CD - автоматичне розгортання. Підвищує швидкість релізів і стабільність систем.

**FinPay**

Фінтех-партнер TechScooter, що обробляє електронні платежі та надає аналітику. Забезпечує інтерактивні панелі моніторингу та звітності. Підтримує безпечну обробку транзакцій.

**CSPM (Cloud Security Posture Management)**

Інструменти для моніторингу та управління конфігураціями хмарної безпеки. Виявляють помилки, невідповідності політикам та ризики. Допомагають підтримувати відповідність стандартам (наприклад, ISO, GDPR).

**API (Application Programming Interface)**

Інтерфейс для взаємодії між програмними компонентами або системами. Дозволяє отримувати, надсилати або обробляти дані. Вимагає контролю доступу та захисту від зловживань.

**Incident Response Plan**

Документована процедура реагування на кіберінциденти. Визначає ролі, етапи, канали комунікації та дії. Ключовий елемент ISMS для мінімізації шкоди.

**Блокчейн**

Розподілений реєстр, що забезпечує незмінність і прозорість записів. Використовується для зберігання транзакцій, метаданих, маршрутів. У TechScooter - для контролю самокатів і користувацьких дій.

**DevOps**

Культура та набір практик, що об’єднує розробку (Dev) і операції (Ops). Спрямована на автоматизацію, швидке розгортання та стабільність ПЗ. Підвищує ефективність команд.

**DevSecOps**

Розширення DevOps з інтеграцією безпеки на всіх етапах розробки. Забезпечує раннє виявлення вразливостей та відповідність політикам. Підвищує стійкість програмного продукту.

**QA (Quality Assurance)**

Процес забезпечення якості програмного забезпечення через тестування та перевірку. Включає функціональні, навантажувальні та безпекові тести. У TechScooter - не охоплював перевірку коду на помилки.

**HR (Human Resources)**

Відділ управління персоналом, відповідальний за найм, адаптацію, навчання та політики. У контексті ІБ - забезпечує ознайомлення співробітників з політиками безпеки. Взаємодіє з CISO щодо доступу та навчання.

**Gap-аналіз**

Оцінка розриву між поточним станом безпеки та бажаним рівнем відповідності. Виявляє недоліки, слабкі місця та пріоритети для покращення. Використовується перед сертифікацією ISO/IEC 27001.

**Initial/Ad-hoc**

Найнижчий рівень зрілості процесу - дії виконуються неформально, без політик чи контролю. Відсутня стандартизація, залежність від окремих осіб. Високий ризик інцидентів та невідповідності.

**Capability Maturity Model (CMM)**

Модель оцінки зрілості процесів у п’яти рівнях: Initial, Managed, Defined, Quantitatively Managed, Optimized. Використовується для оцінки ефективності ІБ-процесів. Допомагає планувати розвиток ISMS.

**RBAC (Role-Based Access Control)**

Модель доступу, що базується на ролях користувачів. Дозволяє обмежити доступ до ресурсів відповідно до функціональних обов’язків. Знижує ризик надмірних привілеїв.

**KPI (Key Performance Indicator)**

Ключовий показник ефективності, що вимірює досягнення цілей. У сфері ІБ - може включати кількість інцидентів, час реагування, рівень обізнаності. Використовується для оцінки успішності ISMS.

**Підвищити рівень зрілості процесу до керованого (Managed) або оптимізованого (Optimized)**

Означає перехід від неформального до системного управління процесами. Включає політики, аудит, метрики та постійне вдосконалення. Підвищує відповідність стандартам та стійкість до загроз.

**BYOD (Bring Your Own Device)**

Політика, що дозволяє співробітникам використовувати особисті пристрої для роботи. Вимагає контролю безпеки, шифрування та MDM. Підвищує мобільність, але створює ризики витоку даних.

**Annex (Annex A.6.2)**

Додаток до ISO/IEC 27001, що містить перелік контролів безпеки. A.6.2 - стосується навчання та обізнаності персоналу. Визначає обов’язкові заходи для підтримки культури ІБ.

**MDM (Mobile Device Management)**

Система управління мобільними пристроями в корпоративному середовищі. Дозволяє контролювати налаштування, шифрування, доступ та оновлення. Ключова для реалізації політики BYOD.

**Fraud Detection System**

Система виявлення шахрайських транзакцій на основі поведінкових патернів та аномалій. Використовується у фінтех-сервісах для захисту клієнтів. Знижує фінансові втрати та ризики.

**3D Secure**

Механізм додаткової автентифікації при онлайн-платежах. Вимагає підтвердження транзакції через SMS, додаток або біометрію. Підвищує безпеку електронних платежів.

**PCI DSS Requirement 10**

Вимога щодо журналювання всіх доступів до систем, що обробляють платіжні дані. Включає логування, збереження та аналіз подій. Критично для розслідування інцидентів.

**PII (Personally Identifiable Information)**

Інформація, що дозволяє ідентифікувати особу: ім’я, адреса, номер картки тощо. Підлягає захисту згідно з GDPR та ISO/IEC 27001. Витік PII - серйозне порушення безпеки

**Несанкціонований доступ до PII**

Отримання доступу до персональної ідентифікаційної інформації без відповідних прав або дозволу. Може бути результатом зламу, внутрішньої загрози або помилки конфігурації. Порушує вимоги GDPR, ISO/IEC 27001 та створює юридичні ризики.

**Least Privilege**

Принцип, за яким користувачі отримують лише ті права доступу, які необхідні для виконання їхніх завдань. Зменшує ризик внутрішніх загроз і помилок. Ключовий елемент у моделі RBAC та політиках ISMS.

**Середовища Dev/Test/Prod**

Розділення середовищ розробки (Dev), тестування (Test) і продуктивного використання (Prod). Забезпечує контроль над змінами, ізоляцію даних і стабільність сервісу. Важливо для безпечного SDLC.

**rate-limiting**

Обмеження кількості запитів до API або сервісу за певний період часу. Захищає від DoS-атак, зловживань і автоматизованих сканувань. Застосовується в системах з відкритим доступом.

**ACL (Access Control List)**

Список правил, що визначає, хто має доступ до ресурсу і які дії дозволені. Може застосовуватись до файлів, мережевих пристроїв, API. Основний механізм контролю доступу в багатьох системах.

**Endpoint Validation**

Перевірка пристрою, з якого здійснюється доступ до корпоративної мережі або даних. Включає перевірку ОС, антивірусу, шифрування, відповідності політикам. Знижує ризик зараження та витоку даних.

**Malware**

Шкідливе програмне забезпечення, створене для порушення роботи систем, крадіжки даних або контролю над пристроєм. Включає віруси, трояни, ransomware. Вимагає постійного моніторингу та захисту.

**SentinelOne**

Платформа захисту кінцевих точок з функціями виявлення, реагування та автоматичного усунення загроз. Використовує поведінковий аналіз і машинне навчання. Підходить для корпоративного середовища.

**Splunk**

Система збору, аналізу та візуалізації логів і подій безпеки. Застосовується для моніторингу, розслідування інцидентів та аудиту. Інтегрується з SIEM та іншими системами безпеки.

**Захист PII**

Комплекс заходів для забезпечення конфіденційності, цілісності та доступності персональної інформації. Включає шифрування, контроль доступу, аудит. Вимагається згідно з GDPR, ISO/IEC 27001.

**SonarQube**

Інструмент для статичного аналізу коду, що виявляє помилки, вразливості та порушення стандартів. Інтегрується в CI/CD-процеси. Допомагає підвищити якість і безпеку програмного забезпечення.

**VLAN (Virtual Local Area Network)**

Логічне розділення мережі на ізольовані сегменти. Застосовується для контролю доступу, ізоляції критичних систем і зменшення площі атаки. Ключовий елемент мережевої безпеки.

**pfSense**

Відкрите програмне забезпечення для фаєрволу та маршрутизації. Підтримує VPN, IDS/IPS, NAT, фільтрацію трафіку. Використовується для захисту корпоративних мереж.

**Suricata**

Система виявлення та запобігання вторгненням (IDS/IPS), що аналізує мережевий трафік. Підтримує сигнатурний та поведінковий аналіз. Інтегрується з SIEM та фаєрволами.

**AUP (Acceptable Use Policy)**

Політика припустимого використання ресурсів компанії. Визначає правила роботи з ІТ-активами, пристроями, даними. Забезпечує дисципліну та відповідність стандартам безпеки.

**Політика припустимого використання (AUP)**

Документ, що регламентує дозволені та заборонені дії співробітників щодо корпоративних ресурсів. Включає правила доступу, зберігання, передачі даних. Важлива для контролю внутрішніх ризиків.

**Створення реєстру в CMDB**

Формування бази даних конфігураційних елементів (активів) з описом їх властивостей, власників і критичності. Дозволяє управляти ресурсами, залежностями та ризиками. Основний етап впровадження ISMS.

**CMDB (Configuration Management Database)**

База даних, що містить інформацію про ІТ-активи, їх конфігурації, зв’язки та статус. Використовується для управління змінами, інцидентами та безперервністю бізнесу. Інтегрується з системами моніторингу.

**Whitelist**

Список дозволених елементів - IP-адрес, доменів, пристроїв або програм. Все, що не входить до списку, блокується або обмежується. Застосовується для контролю доступу та захисту від загроз.

**Security Awareness Officer**

Фахівець, відповідальний за розробку та реалізацію програм навчання з інформаційної безпеки. Координує тренінги, оцінку знань, комунікацію з персоналом. Ключова роль у формуванні культури безпеки.