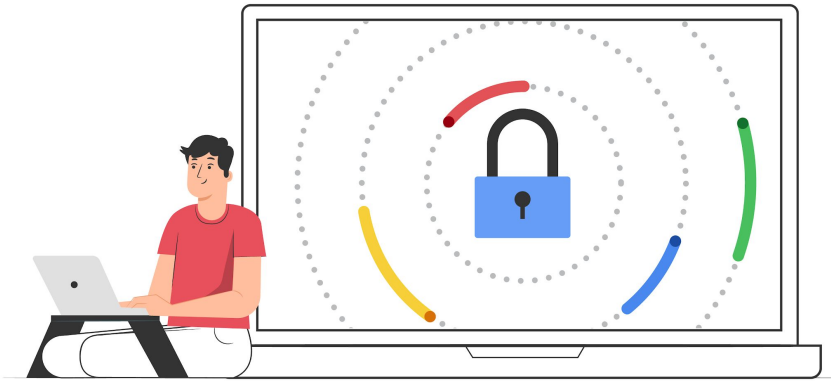
Безпечніше з Google

Google | ISSP

Онлайн-курс

Основи кібербезпеки для бізнесу

Стратегії й тактики підвищення безпеки бізнесу



Артем Михайлов

Директор з корпоративних рішень, партнер, ISSP

Досвід:

- 15+ років досвіду в галузі кібербезпеки
- 350+ складних проєктів з кібербезпеки
- 20+ країн, де ведеться бізнес
- 3+ роки розробки рішень з кібербезпеки для малого та середнього бізнесу, vCISO

Спеціалізація:

- Проєктування архітектури кібербезпеки для великих та малих підприємств
- Керування ризиками й управління комплексними аудитами з кібербезпеки

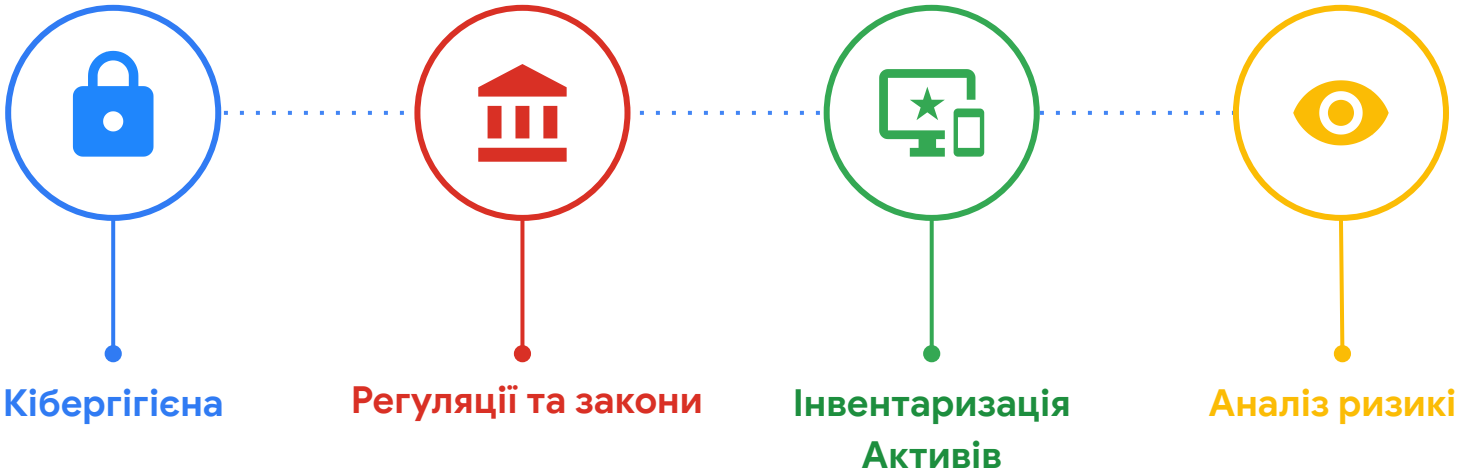
Email: amykhailov@issp.com
Київ

Програма

1. Обов’язкові принципи кібербезпеки
2. Методології з кібербезпеки
3. Розбудова стратегії з кібербезпеки
4. Розбудова тактики з кібербезпеки
5. Висновки та поради

1 Обов’язкові принципи кібербезпеки

Практичні принципи кібербезпеки



Кібергігієна: Проблематика

Виклики кібергігієни

Співробітникам

Відсутність мотивації

- знання з кібергігієни не приносять видимої доданої вартості на ринку праці

Розуміння важливості

- відсутність знань з кібербезпеки ускладнює розуміння наслідків неправильної поведінки в кіберпросторі

CISO*

Складність вимірювання

- відсутність інструментів оцінки готовності співробітників визначати та зменшувати рівень ризику загрози

“Людський фаєрвол”

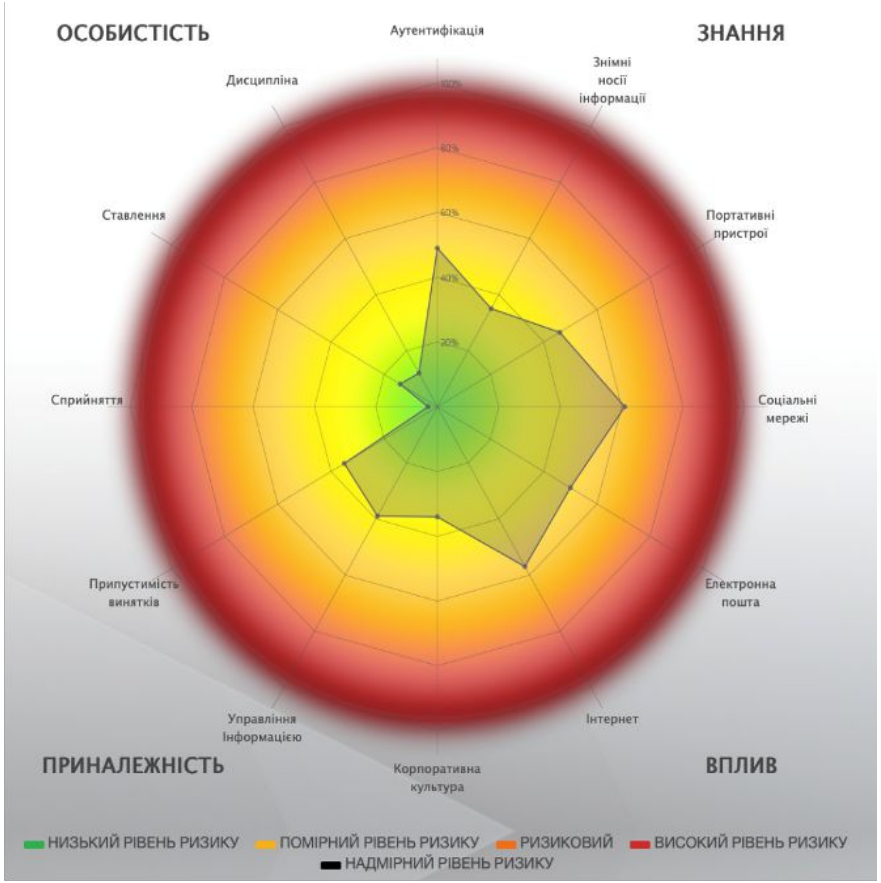
- інструменти кібербезпеки не можуть захистити від усіх випадкових натискань та фішингових кампаній

*CISO (англ. Chief Information Security Officer) – Директор з Інформаційної безпеки

Залишковий ризик після навчання

Кібергігієна охоплює такі навички:

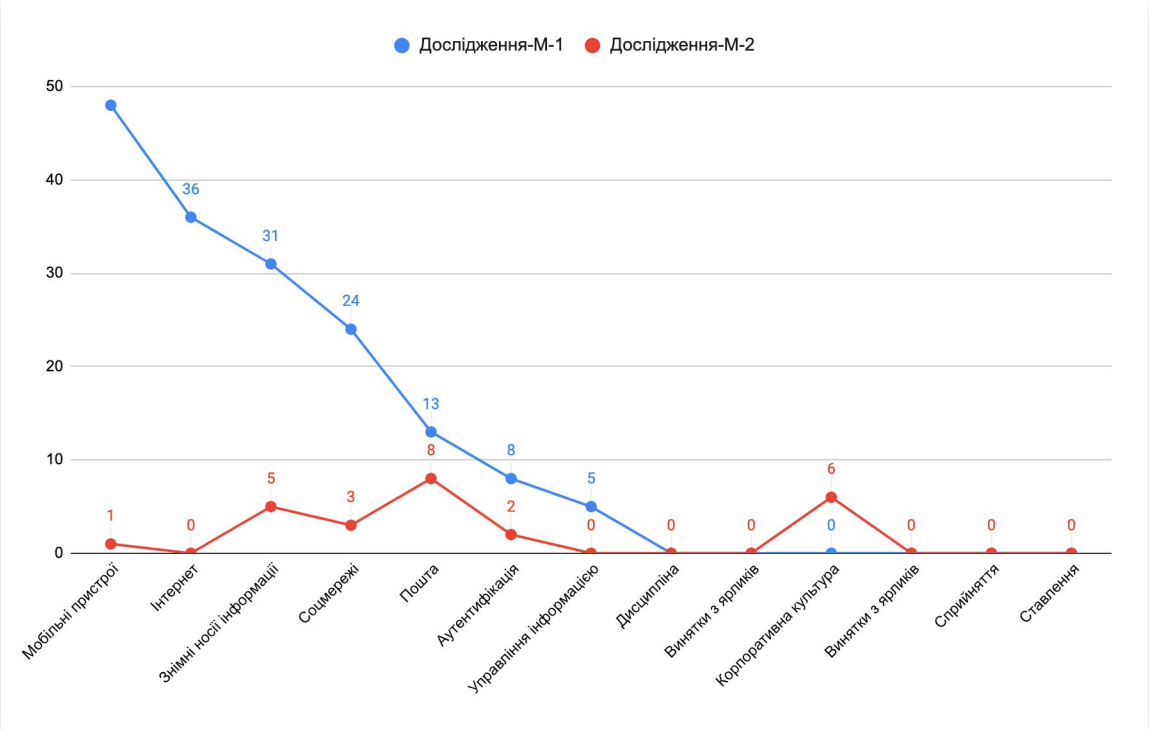
1. **Людський фактор** (Особистість) = хто ми є як особистості
2. **Технічні знання** = наскільки добре ми розуміємо технологію та безпеку
3. **Приналежність** = ступінь ризику, на який ми піддаємось в організації
4. **Зовнішні фактори** (Вплив) = ризики, яким ми піддаємось у кіберпросторі



Секрет успіху – регулярність тренінгових ініціатив

Динаміка якості навичок з кібергігієни

- Перші тренінги з кібербезпеки приносять найбільше користі
- Системні повторювання – запорука залишатись пильним



Джерело: ISSP

Рекомендовані теми для підвищення обізнаності

- Секція 1. Ви є ціллю
- Секція 2. Соціальна інженерія
- Секція 3. Фішинг
- **Секція 4. Захищений браузінг**
- **Секція 5. Соціальні мережі**
- **Секція 6. Безпека смартфонів**
- **Секція 7. Паролі**
- **Секція 8. Шифрування**
- **Секція 9. Безпека даних**
- **Секція 10. Знищення даних**
- Секція 11. Безпека WiFi
- Секція 12. Віддалена робота
- Секція 13. Інсайдерська загроза
- **Секція 14. Служба підтримки**

*за рекомендаціями SANS Institute – приватної комерційної компанії США, яка спеціалізується на інформаційній безпеці та навчанні з кібербезпеки.

Рекомендовані теми для підвищення обізнаності

- **Секція 15. IT персонал**
- **Секція 16. Фізична Безпека**
- **Секція 17. Захист ПК**
- **Секція 18. Захист домашньої мережі**
- **Секція 19. Захист дітей онлайн**
- **Секція 20. Мене зламали, що робити?**
- Секція 21. Лідерство і вищий менеджмент
- Секція 22. APT*
- Секція 23. Хмари
- **Секції 24 – 30. Законодавство**
- **Секція 31. Необхідні кроки, щоб залишатися в безпеці**

***APT** (англ. Advanced Persistent Threat) – складна кібератака

Практичні поради

1. **Впровадити** кібергігієну, як перший ефективний та доступний крок
2. **Ознайомитись** з комерційними платформами для опанування кібергігієни
3. **Провести** тренінг для своїх співробітників у вигляді воркшопу від запрошеного тренера з кібербезпеки
4. **Перевірити** знання і навички співробітників провівши фішингову компанію

*__фішинг__ – вид атаки, під час якої зловмисник намагається ввести в оману користувача з метою видобування конфіденційної інформації або інфікування користувацької системи

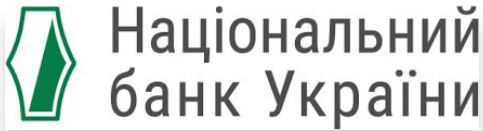
Регуляції в кібербезпеці

Кібербезпека – зарегульована у світі галузь.
Закони та нормативи у сфері кібербезпеки часто базуються на стандартах, визнаних галузевою спільнотою

Визначення чинних стандартів для Вашої галузі може бути важким та часто вимагає консультації з експертом з кібербезпеки

Закони й регуляції України

- Указ «Про Стратегію кібербезпеки України», п.4.4 4.4. Розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки
- Постанова КМУ №518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури»
- Закон про Критичну Інфраструктуру та її захист
- Постанови Національного Банку України (№95, 58, ...)
- Статті ККУ 163, 360-363



Проблематика

1
Взаємодія різних бізнесів

Більші гравці не завжди хочуть вести бізнес із меншими вразливими партнерами, через яких на них можуть організувати кібератаки

2
Регулювання

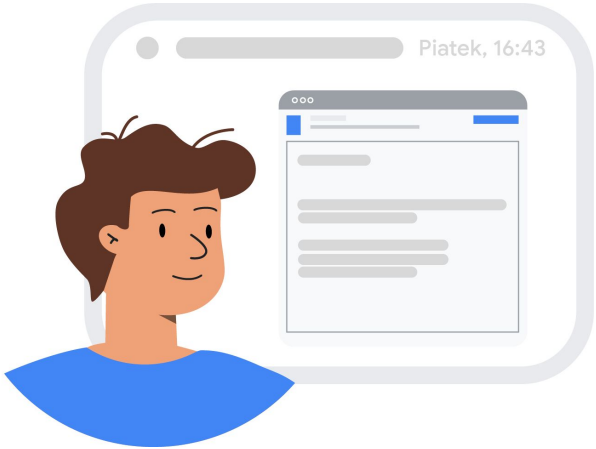
Наявність обов'язкових несинхронізованих регуляцій робить їх важкими для дотримання

3
Фокус зусиль

Синхронізація дотримання норм з практиками кібербезпеки є важким або неефективним процесом

Загальні рекомендації

- Перегляньте основи про:
  - Захист конфіденційних даних
  - Українське законодавство та національну стратегію у сфері кібербезпеки
  - Законодавство ЄС (GDPR*)
  - Галузеві стандарти/рамки (ISO, NIST, CIS, SOC2)
- Визначте вимоги до дотримання вашого бізнесу, віднайдіть схожі та визначте план відповідності



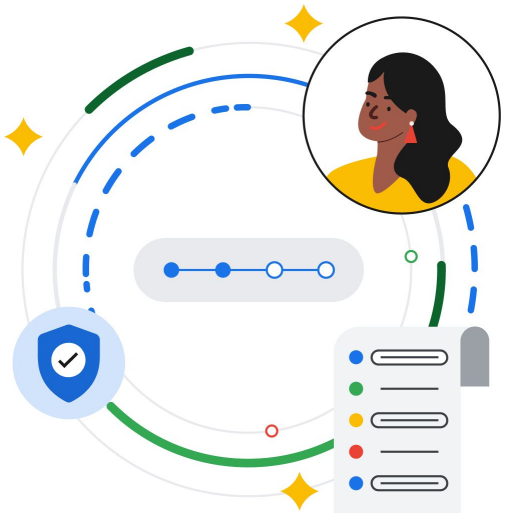
*GDPR (англ. General Data Protection Regulation) – Загальний регламент про захист даних, це закон Європейського Союзу, який регулює захист персональних даних фізичних осіб на території ЄС

Практичні поради: визначте Вашого регулятора та закони

- **Визначте** та зверніться до Вашого(-их) регулятора(-ів), щоб встановити всі дійсні закони та правила, які включають питання IT та безпеки
- **Перевірте** наявність бізнес-активності або часткової активності в інших країнах
- **Дізнайтеся**, де знаходиться Ваш клієнт. Може застосовуватися іноземне законодавство

Практичні поради: визначте релевантні вимоги законів та регуляцій

- **Перегляньте** вимоги від Ваших партнерів, клієнтів та інших зацікавлених сторін
- **Визначте** перелік вимог, які вам потрібно дотримуватися, і окресліть можливі "конфліктні вимоги"
- **Проводьте** облік усіх вимог
- **Призначте** відповідальну особу для моніторингу змін у законах та правилах, а також команду за реагуванням та підтримкою відповідності всім вимогам
- **Розгляньте** можливість консультації з експертом



Активи

Обладнання та пристрої

- комп'ютери та ноутбуки
- мобільні пристрої
- мережеве обладнання
- сервери

Програмне забезпечення

- операційні системи
- офісні програми
- спеціалізоване програмне забезпечення

Дані та інформація

- клієнтська база даних
- фінансові звіти
- документація проєктів

Людські ресурси

- співробітники IT-відділу
- керівництво
- штат спеціалістів з безпеки інформації

Активи

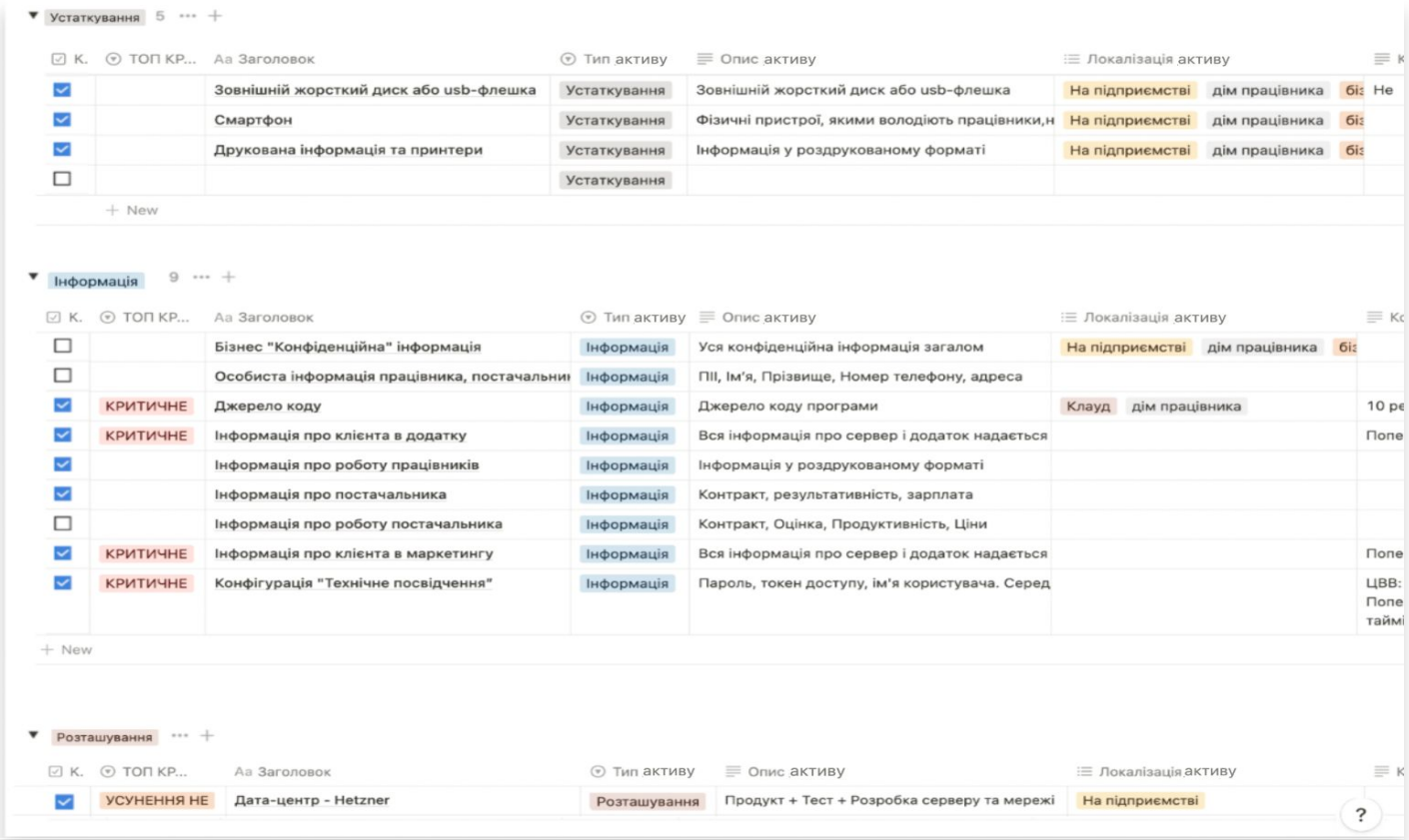
Інтелектуальна власність	Фізичні активи	Послуги та договори
• патенти • товарні знаки • авторські права	• офісні приміщення • дата-центри • обладнання для фізичної безпеки (камери, сигналізації тощо)	• постачальники обслуговування • договори на обслуговування • ліцензії та сертифікати

25 тис

нових загальних IT-вразливостей та ризиків було виявлено у 2022 році

Джерело: Statista

Інвентаризація активів



Устаткування 5

К.	ТОП КР...	Аа Заголовок	Тип активу	Опис активу	Локалізація активу	К
☑		Зовнішній жорсткий диск або usb-флешка	Устаткування	Зовнішній жорсткий диск або usb-флешка	На підприємстві дім працівника біз	Не
☑		Смартфон	Устаткування	Фізичні пристрої, якими володіють працівники,н	На підприємстві дім працівника біз	
☑		Друкована інформація та принтери	Устаткування	Інформація у роздрукованому форматі	На підприємстві дім працівника біз	
☐			Устаткування			

+ New

Інформація 9

К.	ТОП КР...	Аа Заголовок	Тип активу	Опис активу	Локалізація активу	Ко
☐		Бізнес "Конфіденційна" інформація	Інформація	Уся конфіденційна інформація загалом	На підприємстві дім працівника біз	
☐		Особиста інформація працівника, постачальни	Інформація	ПІІ, Ім'я, Прізвище, Номер телефону, адреса		
☑	КРИТИЧНЕ	Джерело коду	Інформація	Джерело коду програми	Клауд дім працівника	10 ре
☑	КРИТИЧНЕ	Інформація про клієнта в додатку	Інформація	Вся інформація про сервер і додаток надається		Попе
☑		Інформація про роботу працівників	Інформація	Інформація у роздрукованому форматі		
☑		Інформація про постачальника	Інформація	Контракт, результативність, зарплата		
☐		Інформація про роботу постачальника	Інформація	Контракт, Оцінка, Продуктивність, Ціни		
☑	КРИТИЧНЕ	Інформація про клієнта в маркетингу	Інформація	Вся інформація про сервер і додаток надається		Попе
☑	КРИТИЧНЕ	Конфігурація "Технічне посвідчення"	Інформація	Пароль, токен доступу, ім'я користувача. Серед		ЦВВ: Попе тайм

+ New

Розташування

К.	ТОП КР...	Аа Заголовок	Тип активу	Опис активу	Локалізація активу	К
☑	УСУНЕННЯ НЕ	Дата-центр - Hetzner	Розташування	Продукт + Тест + Розробка серверу та мережі	На підприємстві	

?

на малюнку зображений приклад інвентаризації активів

Практичні поради

- **Не лякайтеся** “забути” важливий актив. У вас завжди буде змога додати його пізніше
- **Створіть** “живий” список. Що повнішим він буде, тим легше на наступних стадіях
- **Розбудуйте** ефективну систему кібербезпеки за наявності вичерпного списку того, що потребує захисту

- **Розпочинайте** з простого списку і згодом додавайте параметри (тип активу, пов’язаність з іншими, локація, відповідальний за актив і т. д.)
- **Оновлюйте** список щойно є зміни в організації (новий актив додався, змінився або ви його позбулися)
- **Аналізуйте** поділ відповідальності з третіми сторонами (хмарний провайдер, постачальники - в чиїй зоні відповідальності даний актив)

Практична вправа

Складіть список ТОП-5 важливих для Вашої організації категорій активів

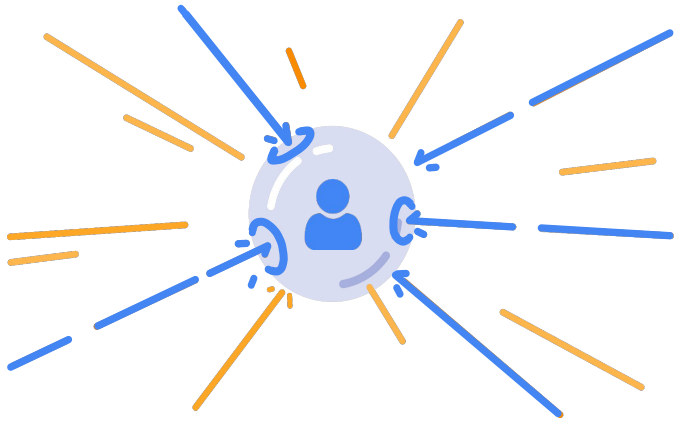
Складіть список ТОП-3 конкретних активів з кожної категорії, які є критичними для діяльності бізнесу

3:00

Ризики кібербезпеки

Ризики кібербезпеки – вплив **невизначеності** на інформацію та технології:

- стосуються втрати **конфіденційності**, **цілісності** чи **доступності** інформації, даних або систем
- **відображають потенційні негативні наслідки місії**, **функцій**, **іміджу / репутації** та активів, особистостей, інших організацій та нації



Визначення базується на ISO Guide 73 [6] та NIST SP 800-60 Vol. 1 Rev. 1 [7]

Кількісний та якісний аналіз ризиків

Кількісний аналіз

Кількісний аналіз оцінює:

- ймовірність успіху у досягненні цілей проєкту
- резерв непередбаченості

Мета:

- надати числову оцінку загального впливу ризику на бізнес

Якісний аналіз

Якісний аналіз визначає:

- пріоритетність обробки ризиків у проєкті
- ризикову експозицію шляхом множення значень ймовірності та впливу

Мета:

- проаналізувати та оцінити характеристики індивідуально визначених ризиків

Проведення оцінки ризиків

1. **Проведіть дослідження щодо оцінки ризиків:**
    - Випишіть очевидні кіберризики
    - Опитайте свою команду, які ризики вони можуть додати до Вашого списку
    - Подивіться на загальні ризики та ризики вашої галузі, доступні в Інтернеті

Проведення оцінки ризиків

2. **Зіставте виявлені ризики зі списком Ваших активів**, які були визначені раніше - для кожного активу (із Вашого списку активів) запишіть всі виявлені ризики та наслідки для Вашої організації, наприклад:

Актив: Сервери для резервного копіювання	**Ризик**: Пожежа в дата-центрі **Причина**: Сервери для резервного копіювання знаходяться в тому ж фізичному місці, що й основний сервер	**Наслідок**: Компанія втратить всі дані без можливості відновлення

Проведення оцінки ризиків

3. **Оцініть наслідки ризику:**
   - Оцініть критичність наслідків цього ризику, використовуйте шкалу **високий**, **помірний**, **низький**
   - Оцініть, ймовірність виникнення ризику, використовуючи ту ж шкалу
   - Присвойте бали всім ризикам, а потім визначте найважливіші ризики (**Ймовірність × Вплив**)

Актив: Сервери для резервного копіювання	**Ризик**: Пожежа в дата-центрі **Причина**: Сервери для резервного копіювання знаходяться разом з основним сервером	**Наслідок**: Компанія втратить всі дані без можливості відновлення	**Поточна безпека**: Є ручний вогнегасник та детектор пожежі	**Ймовірність**: *3 – Висока* (Є багато електронних пристроїв, які можуть загорітися, персоналу потрібно 1 година, щоб дістатися до офісу вночі)	**Вплив:** *3 – Високий* (Знадобиться багато років, щоб знову зібрати дані)	**Загальний ризик:** 9 – Дуже високий

Проведення оцінки ризиків

4. **Визначте наскільки цей ризик прийнятний та розробіть план управління ризиками:**
    - Для кожного ризику вирішіть, який захід зменшення буде застосовуватися
    - Вирішіть, які пари Ризик-Актив повинні бути зменшені, передані, прийняті або уникнуті
    - Призначте персонал та порядок дій, відповідальні за зменшення, передачу, уникнення або прийняття ризиків

Поточна безпека:	**Ймовірність**:	**Вплив:**	**Загальний ризик:**	**Рішення:**	**Відповідальний/Дія:**
Є ручний вогнегасник та детектор пожежі	*3 – Висока* (Є багато електронних пристроїв, які можуть загорітися, персоналу потрібно 1 година, щоб дістатися до офісу вночі)	*3 – Високий* (Знадобиться багато років, щоб знову зібрати дані)	9 – Дуже високий	Зменшення ризику	IT має перенести резервне копіювання в хмару. Бюджет має бути підтверджений

Приклад завершеної оцінки ризиків

GRS* = значення CIA
Активу × Ймовірність

Бачення ризиків | Обслуговування | Звіт +

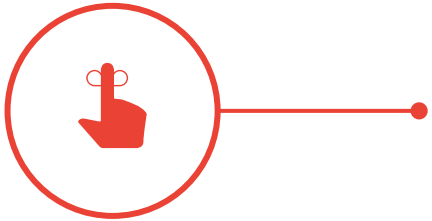
Filter Sort New

заголовок	Актив	Тип_активу	Σ C I A	Ризик	Σ ЗРР
Конфігурація "Технічне посвідчення" + Користувачі не встановлюють достатньо надійні паролі	Конфігурація "Технічне посвідчення"	Інформація	АКТИВ: 3|3|3| РИЗИК: 1|1|1| ЙМОВІРНІСТЬ: 3	Користувачі не встановлюють достатньо надійні паролі	27
Конфігурація "Технічне посвідчення" + Інсайдер з доступом адміністратора переглядає конфіденційні дані	Конфігурація "Технічне посвідчення"	Інформація	АКТИВ: 3|3|3| РИЗИК: 1|1|1| ЙМОВІРНІСТЬ: 3	Інсайдер з доступом адміністратора переглядає конфіденційні дані	27
Джерело коду + Вихідний код програми може бути знищений або підроблений на користь зловмисника	Джерело коду	Інформація	АКТИВ: 3|3|2| РИЗИК: 1|1|1| ЙМОВІРНІСТЬ: 3	Вихідний код програми може бути знищений або підроблений на користь зловмисника	24
Гнучкі звіти та пристрої + Програмне забезпечення написано з неприпустимим рівнем вразливостей	Гнучкі звіти та пристрої	Програмне забезпечен...	АКТИВ: 1|3|3| РИЗИК: 1|1|1| ЙМОВІРНІСТЬ: 3	Програмне забезпечення написано з неприпустимим рівнем вразливостей	21
Гнучні звіти та пристрої + Критично важливі для бізнесу додатки зазнають негативного впливу при зміні базової операційної платформи	Гнучкі звіти та пристрої	Програмне забезпечен...	АКТИВ: 1|3|3| РИЗИК: 1|1|1| ЙМОВІРНІСТЬ: 3	Критично важливі для бізнесу додатки зазнають негативного впливу при зміні базової операційної платформи	21
Конфігурація "Технічне посвідчення" + Перехоплення та модифікація інформації, пов'язаної зі службами додатків, з метою вчинення шахрайства	Конфігурація "Технічне посвідчення"	Інформація	АКТИВ: 3|3|3| РИЗИК: 1|1|0| ЙМОВІРНІСТЬ: 3	Перехоплення та модифікація інформації, пов'язаної зі службами додатків, з метою вчинення шахрайства	18

***GRS** (англ. Gross Risk Score) – загальний рівень ризику
****CIA** (англ. Confidentiality, Integrity, and Availability) – конфіденційність, цілісність та доступність

2 Методології з кібербезпеки

Проблематика



Великий вибір інструментів

різноманіття можливих інструментів та технік робить важким визначення наступних кроків на шляху з покращення кібербезпеки

Складність сфери

наявність методології допомагає зорієнтуватись у сфері кібербезпеки та скласти повноцінну картину

Наявність стандартів

зацікавлені сторони можуть просити показати, що Ви турбуєтесь про кібербезпеку, і Вам потрібно буде спиратися на визнані стандарти.

Рішення

- Оберіть свій єдиний фреймворк
- Оберіть один із найпростіших стандартів і почніть з малого (наприклад, SOC2), якщо Ваші регуляції не вимагають від Вас впровадження конкретного стандарту

Практичні поради: визначте Вашого регулятора та закони

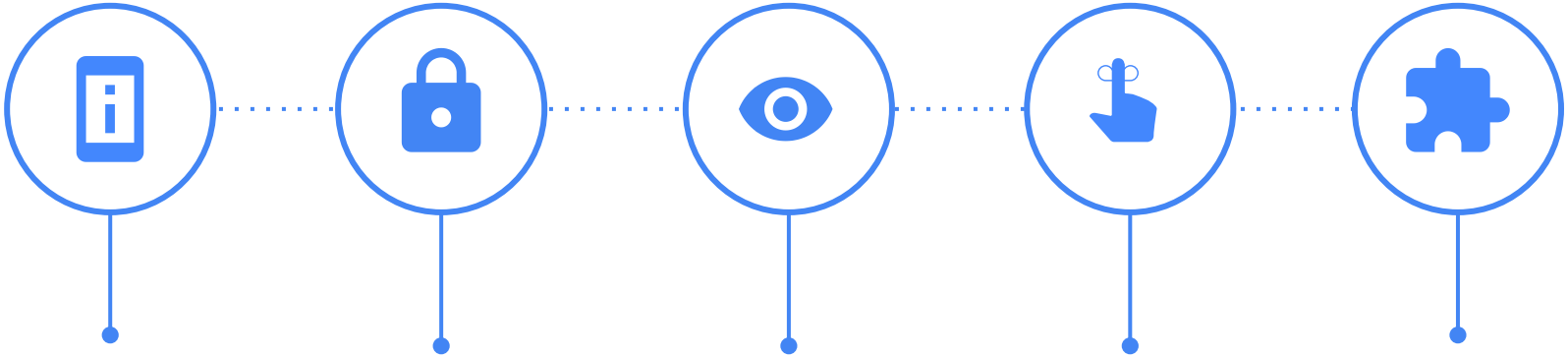
- Визначте регуляції, яким вам потрібно слідувати
- Визначте, на яких стандартах базуються регуляції:
  - ISO27k (~100+ контролей + оцінка ризиків) – найімовірніше, це той, який вам потрібен
  - NIST (Ідентифікація - Захист - Виявлення - Реагування - Відновлення)
  - SOC2 (спрощений ISO)
  - CIS Controls (153 контролей)
  - Належать до галузі (PCI DSS, SWIFT Security, HIPAA тощо)

Практичні поради: визначте Вашого регулятора та закони

- Виберіть той стандарт, який найбільше підходить, та розпочніть розробку Вашої системи управління інформаційною безпекою (ISMS)

3 Розбудова стратегії з кібербезпеки

Контролі кібербезпеки



Ідентифікація

Які процеси та активи потребують захисту?

Захист

Застосування відповідних мір для захисту активів і процесів

Виявлення

Впровадження відповідних контролів

Реагування

Відпрацювання технік для стримування загрози

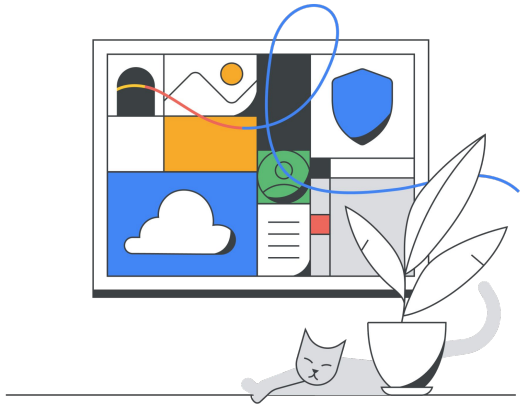
Відновлення

Впровадження процесів для відновлення спроможностей та сервісів, пошкоджених у випадку кіберзагрози

Стратегія з кібербезпеки

Стратегія з кібербезпеки – зменшити ризики, які впливають на наші активи.

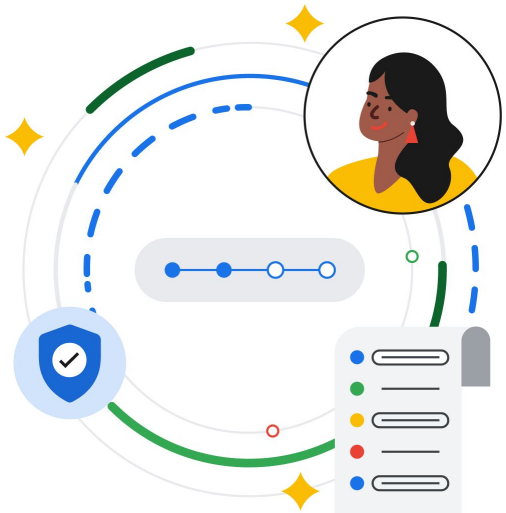
- Для цього ми впроваджуємо контролі кібербезпеки:
  - класу управління доступом
  - резервного копіювання
  - захисту ПК та серверів
  - захисту хмар
  - керування вразливостями
  - управління мобільними пристроями
  - моніторингу і ситуативного аналізу



Контролі класу управління доступом

Основні принципи управління доступом:

- Ідентифікація за допомогою унікального імені користувача
- Обліковий запис користувача має бути захищеним секретним фактором – паролем
- Надійний пароль
- Двофакторна аутентифікація
- Обмежений до мінімально необхідного рівня доступ користувача



Контролі класу управління доступом

Основні принципи управління доступом:

- Щорічний перегляд доступу кожного користувача (розгляньте можливість перегляду 2 або 3 рази для адміністраторів)
- Впровадження центрального довідника користувачів для можливості централізовано керувати користувачами (модифікувати права доступу, анулювати доступ користувачів тощо)
- Використання інтеграції для надання користувачам прав, щоб зберігати облікові записи користувачів централізовано в різних системах

Контролі резервного копіювання

Повне резервне копіювання

Створення копій всіх даних у своєму цифровому оточенні або його частині

- \+ найшвидше відновлення
- – найдорожчі
- – займають найбільше місця

Диференційне резервне копіювання

Створення копії всіх файлів, створених або змінених з моменту останнього повного резервного копіювання резервними копіями

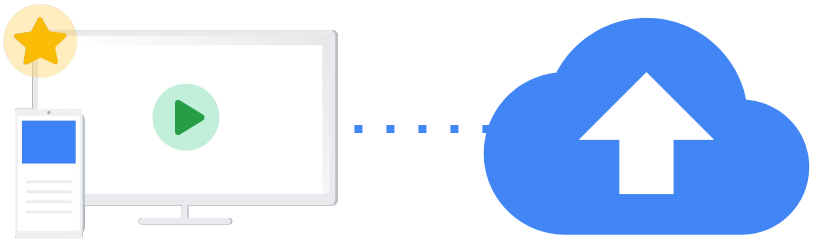
- \+ недорогі
- – довге відновлення

Інкрементальне резервне копіювання

Зберігання лише даних, змінених після останнього резервного копіювання будь-якого типу

Помилки, яких варто уникати під час резервного копіювання

- **Не робити резервні копії взагалі**
- **Зберігання** резервних копій на тому ж обладнанні
- **Не** робити тестування резервної копії
- **Не** робити резервні копії достатньо часто
- **Маркування** Ваших резервних копій



Контролі захисту ПК та серверів

Проблематика

- Кінцева точка є найоперативнішим елементом IT-середовища в будь-якому бізнесі чи галузі та має найбільше асоційованих загроз, через її динамічне використання
- Більшість даних, які важливі у короткостроковій перспективі, зазвичай зберігаються на кінцевій точці, що робить її захист ще більш важливим

Рішення

- Посилення захисту кінцевої точки
- Використання традиційного програмного забезпечення безпеки (наприклад антивірус / брандмауер*)
- Шифрування Диску
- Моніторинг аномальної поведінки в реальному часі на кінцевій точці

***Брандмауер** – програма чи пристрій, що здійснює захист комп'ютерних мереж

Контролі захисту ПК та серверів

- **Придбання** пристроїв у авторизованого дилера.
- **Використання** ліцензійних операційних систем, придбаних у авторизованих дилерів
- Регулярне **оновлення** операційної системи
- **Відсутність** всіх непотрібних функції та служб

- **Наявність** антивірусного програмного забезпечення та брандмауера
- **Використання** сучасного програмного забезпечення для виявлення та реагування на інциденти на кінцевій точці
- **Зберігайте** обережність – не відкривайте підозрілі електронні листи та посилання

Пам'ятайте: взяття під контроль кінцевої точки є ключовою метою для зловмисника. Мати контроль над будь-якою кінцевою точкою у вашій мережі відкриває майже необмежені можливості для хакерів поступово захопити всю інфраструктуру.

Контролі захисту хмар: Проблематика

Сервери

- Сервери важко обслуговувати та належним чином захищати
- Сервери менш надійні, ніж хмари, з точки зору доступності

Хмари

- **Хмари** – сучасна альтернатива серверам
- Хмара гарантує певний, але не повний рівень захисту

Контролі захисту хмар

Існують **три** основні концепції хмари, які мають різний баланс підходу до спільної відповідальності:

- **Інфраструктура як сервіс (IaaS)**
- **Платформа як сервіс (PaaS)**
- **Програмне забезпечення як сервіс (SaaS)**

Контролі захисту хмар: Рішення

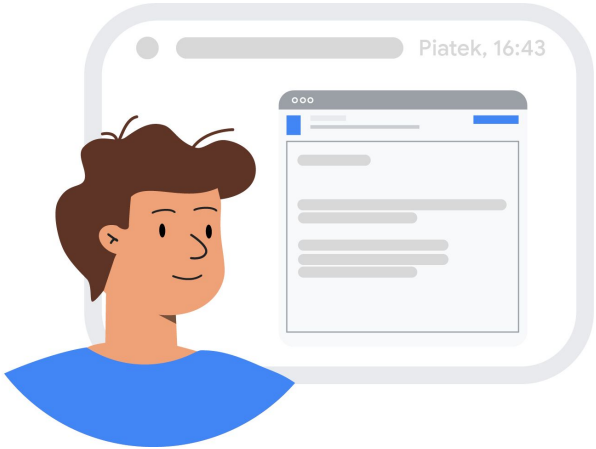
1. Зрозумійте концепцію **спільної відповідальності** для забезпечення безпеки Вашої хмари
    - Провайдер хмари відповідає тільки за обслуговування та доступність апаратного забезпечення через Інтернет

Контролі захисту хмар: Рішення

2. Розгляньте **стратегію безпеки хмари**, щоб захистити свої конфіденційні дані та забезпечити відповідність нормативам
    - Об'єкти провайдера хмари можуть бути розташовані за кордоном, і з’являється ризик виникнення проблеми з дотриманням вимог законодавства
3. Дізнайтеся, яка різниця між **інфраструктурою**, **платформою** та **програмним забезпеченням як сервісами**

Контролі захисту хмар: Процес

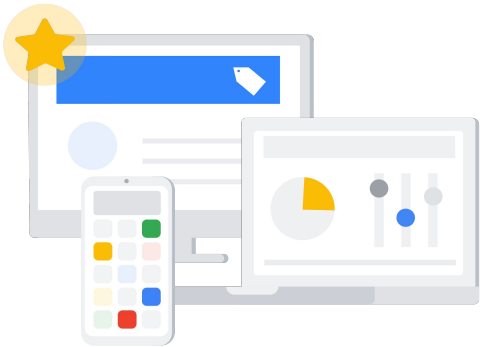
1. Складіть список **високорівневих вимог** до **IT-інфраструктури** (наприклад, електронна пошта з власним доменним ім'ям, система CRM*, база даних з інформацією про клієнтів тощо)
2. Визначте, які з цих пунктів доступні з **IaaS, PaaS, SaaS**, та витрати, котрі з ними пов'язані



***CRM-система** (англ. Customer Relationship Management) – система управління взаємовідносинами з клієнтами, це програмне забезпечення, яке допомагає компаніям автоматизувати та покращувати свої процеси взаємодії з клієнтами

Контролі захисту хмар: Процес

3. Спробуйте перейти від **IaaS** (менше навантаження з безпеки) до **PaaS і SaaS** відповідно
4. Намагайтеся мінімізувати **кількість провайдерів хмари**, яких Ви збираєтеся використовувати. Це допоможе зменшити зусилля для підтримки інфраструктури хмари в довгостроковій перспективі



Контролі захисту хмар: Процес

5. Розгляньте **опціональні** та **включені послуги** з безпеки у Вашій або загальних умовах:
    - **Посилений контроль доступу:** двофакторна аутентифікація
    - **Доступність** та **можливість масштабування** відповідно до потреб Вашого бізнесу (наприклад, цілодобово)

Контролі захисту хмар: Процес

5. Розгляньте **опціональні** та **включені послуги** з безпеки у Вашій або загальних умовах:
    - **Підтримка** та **моніторинг інцидентів** з безпеки (повинно бути цілодобово)
    - Надані **опції резервного копіювання**: висока доступність, автоматичні резервні копії, відмовостійкий сайт
    - **Провайдер хмари** дбає про свою **безпеку**: контроль доступу, установка патчів, пентести*, управління вразливостями

*** пентест** (англ. penetration test) або Тестування на проникнення – це активне випробування системи на наявність вразливостей та спробу проникнення зловмисників.

Контролі захисту хмар: Процес

6. Після налаштування хмарної системи проведіть **високорівневий аудит кібербезпеки** архітектури хмари та оцініть пов'язані ризики

У провайдера хмари має бути необхідна для Вашої діяльності **сертифікація з безпеки**

Контролі керування вразливостями

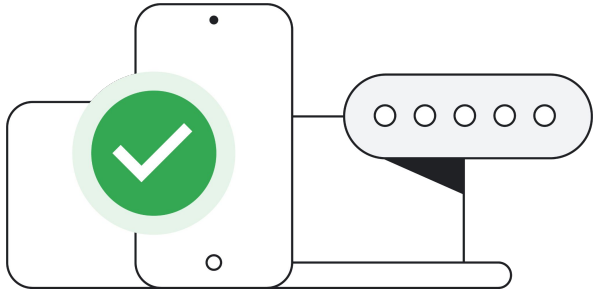
Проблематика	Рішення	План дій
• Щодня виявляються нові вразливості • IT-активи неминуче стають вразливими	• Провести сканування на вразливості усієї інфраструктури. • Обробити результати, встановивши патч або іншим чином нейтралізувавши вразливість	Співпраця з експертами у кібербезпеці може покращити ефективність системи захисту. **Приклад**: Консультант може запропонувати рекомендації для вдосконалення моніторингу безпеки.

автоматизувати та проводити регулярно

Контролі управління мобільними пристроями

Проблематика: Особисті мобільні пристрої, які використовуються для бізнес-цілей або BYOD* – значуща загроза з точки зору інформаційної безпеки

Рішення: Регулярно робіть резервні копії своїх важливих даних, таких як фотографії, документи й контакти



***BYOD** (англ. Bring Your Own Device) – це політика, яка дозволяє працівникам організації використовувати свої особисті пристрої для виконання робочих завдань

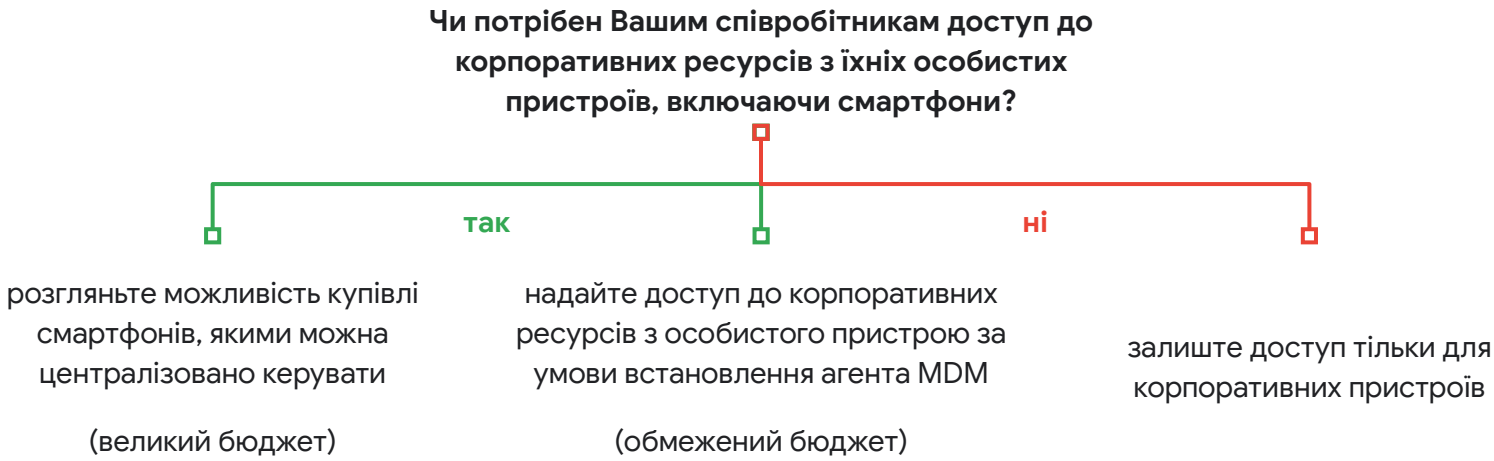
Контролі управління мобільними пристроями

1. Визначте список служб, які повинні бути доступні з пристроїв BYOD*
2. Визначте список співробітників, яким потрібен доступ відповідно до бізнес-процесу
3. Запропонуйте встановити агент MDM* на пристроях BYOD, якщо це прийнятно для Ваших співробітників

*__BYOD__ (англ. Bring Your Own Device) – це політика, яка дозволяє працівникам організації використовувати свої особисті пристрої для виконання робочих завдань

*__MDM__ (англ. Mobile Device Management) – управління мобільними пристроями

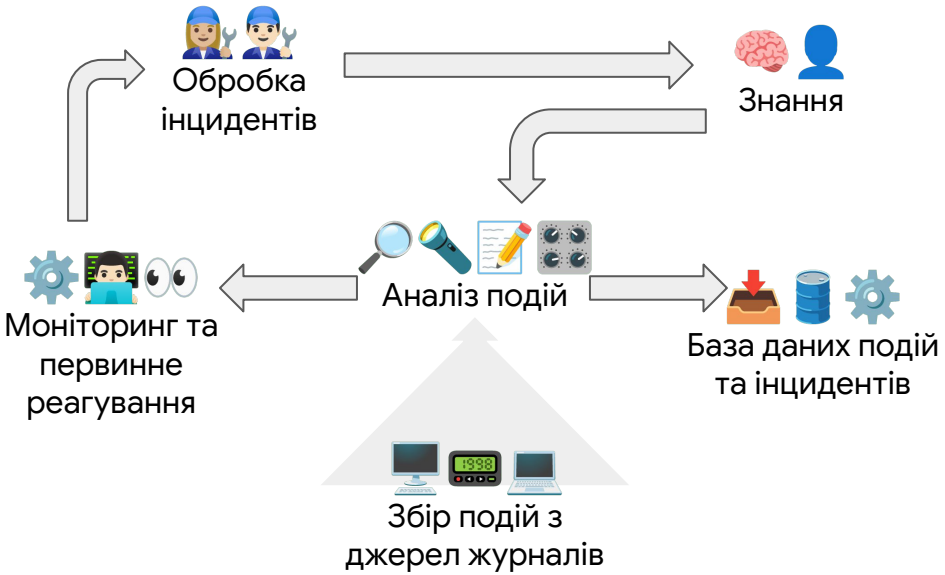
Контролі управління мобільними пристроями: Процес



Контролі з моніторингу і ситуативного аналізу

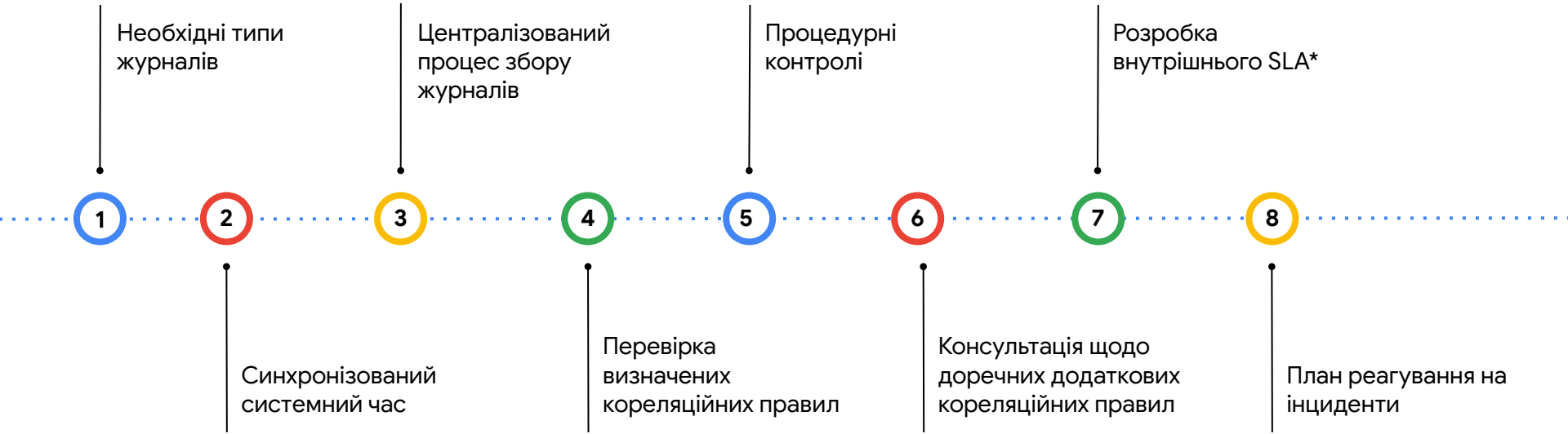
Кібербезпека вимагає спостереження за сповіщеннями систем

Рішення – інструмент управління безпекою та подіями в IT (SIEM*)



*SIEM (англ. security information and event management) – програмними продуктами, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management).

Контролі з моніторингу та ситуативного аналізу



***SLA** (англ. Service-level agreement) – угода між постачальником послуг і користувачем про рівень послуг.

Практична вправа

Робота з контролями кібербезпеки

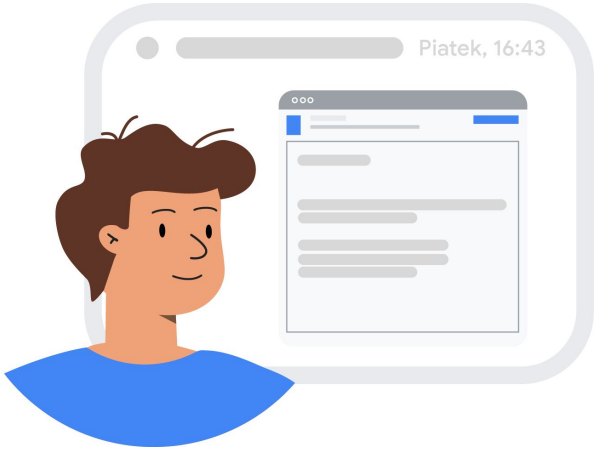
10:00

CIS Controls

4 Розбудова тактики з кібербезпеки

Тактика з кібербезпеки

Тактика кібербезпеки – засновується на **стратегії з кібербезпеки** і **визначає пріоритети** щодо саме які заходи маємо впроваджувати в короткостроковій перспективі.



- Впровадження систем і засобів з кібербезпеки - для зниження ризиків
- SOC сервіси - для виявлення аномалій
- Аудити кібербезпеки - для перевірки себе

SOC Сервіси*

Типові SOC Сервіси від постачальників керованих послуг з кібербезпеки:

Кероване виявлення та реагування

- Виявлення загроз
- Полювання на загрози
- Розширене реагування на інциденти

***SOC Сервіси** (англ. Security Operations Center) – послуги з виявлення, реагування та реагування на інциденти безпеки

SOC Сервіси

Типові SOC Сервіси від постачальників керованих послуг з кібербезпеки:

Керовані послуги безпеки

- Керування ідентифікацією та доступом
- Керування журналами
- Управління пристроями та платформами безпеки
- Сендбокс* як послуга

***сендбокс** або пісочниця (англ. sandbox) — механізм для безпечного виконання програм. Пісочниці часто використовують для запуску непротестованого коду, неперевіреного коду з ненадійних джерел, а також для запуску та виявлення вірусів

SOC Сервіси

Типові SOC Сервіси від постачальників керованих послуг з кібербезпеки:

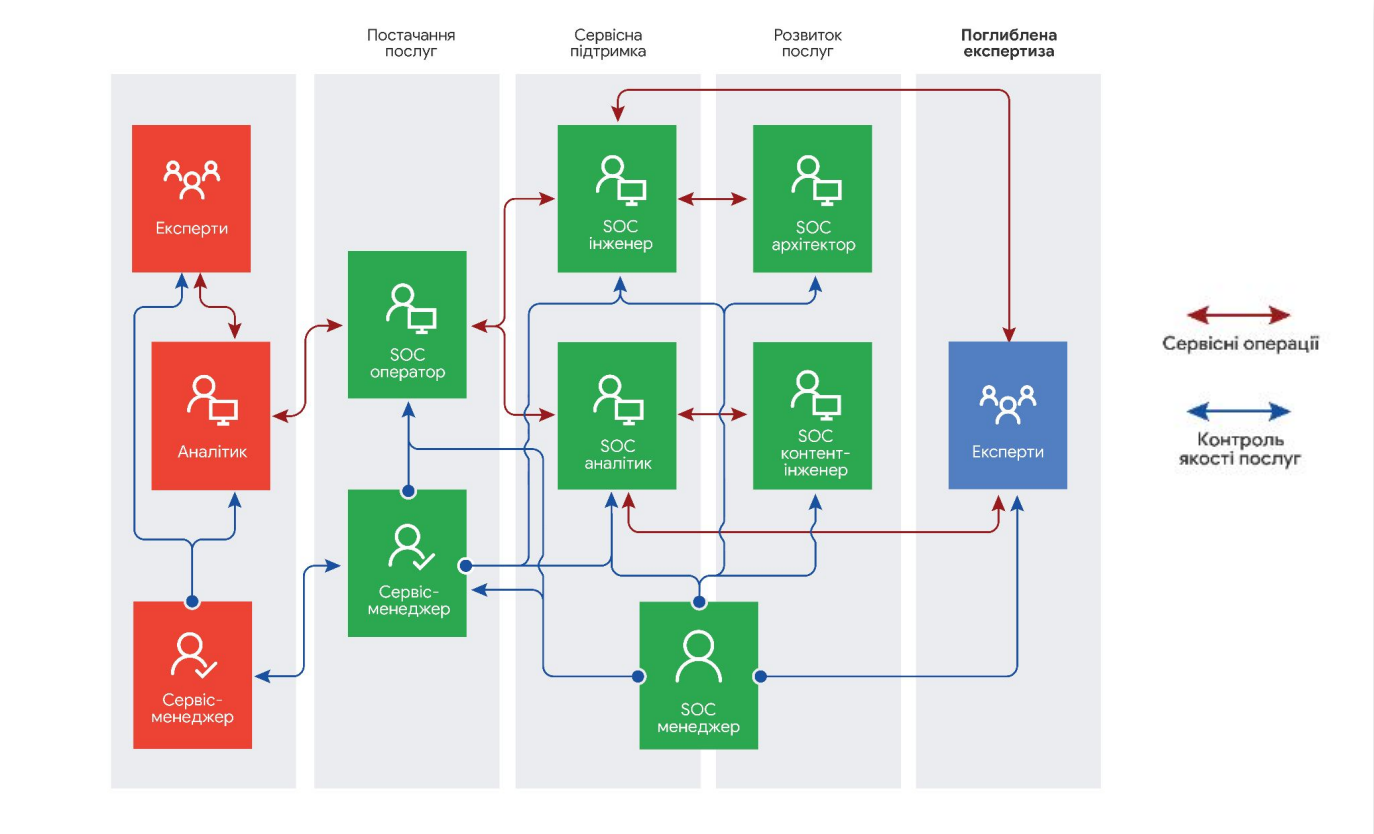
Управління вразливостями

- Тестування безпеки додатків, DAST*
- Аналіз вихідного коду, SAST**
- Сканування вразливостей
- Оцінка вразливостей

***DAST** (англ. Dynamic Application Security Testing) – динамічне тестування безпеки додатків – процес аналізу веб-додатку через фронт-енд для пошуку вразливостей шляхом імітації атак
****SAST** (англ. Static Application Security Testing) – статичне тестування безпеки додатків – методологія тестування, яка аналізує вихідний код для виявлення вразливостей безпеки, які роблять програми організації сприйнятливими до атак

Хороші безпекові операції –
багатошарові немов цибуля

SOC структура в ISSP



Аудити кібербезпеки

Проблематика

- Зловмисники завжди можуть знайти нові способи проникнення у Ваші мережі
- Хакери мають необмежений час, щоб знайти спосіб зламати Вас
- 100% впевненості, що Ваша інфраструктура зараз не скомпрометована не існує

Рішення

- Проводити тест на проникнення (пентест)
  - якщо Ваша компанія розробляє програмний код, необхідно шукати вразливості безпосередньо в коді
- Проводити оцінку компрометації

5 Висновки та поради

Наступні кроки

1 Для бізнесу 👨‍💼👩‍💼🏢

Стратегічні кібероперації:

- розбудова спроможностей і планування
- розумні інвестиції

2 Для IT 👩‍💻👨‍💻

Технічні кібероперації:

- посилення технічної кібербезпеки
- виявлення та реагування
- впевненість, що інвестиції в кібербезпеку дають ефективний результат

3 Для відповідності вимогам 🏛️☑️👀

Нетехнічні кібероперації:

- демонстрація прогресу
- розбудова бізнес-процесів з урахуванням вимог кібербезпеки

Дякую за увагу!