

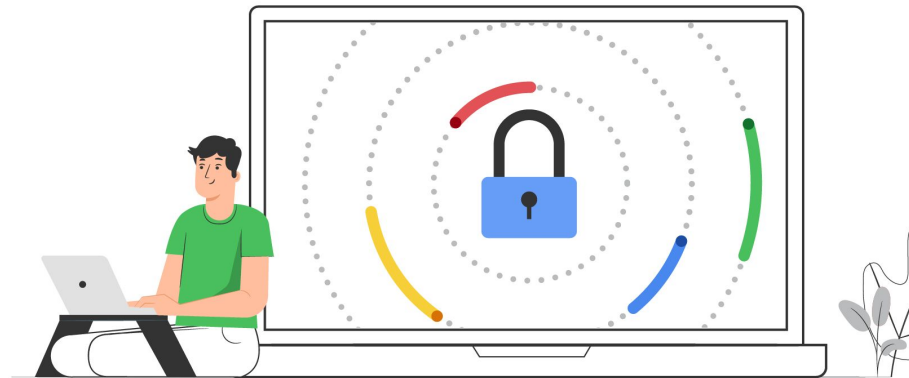
 Безпечніше з Google

Google | **ISSP** | **ROOSH**

Онлайн-програма

Основи кібербезпеки для бізнесу

Кейс-стаді: кібербезпека очима
підприємця



Анастасія Тітова

Керівниця операційного відділу, Roosh

Досвід:

- 9 років в операційній діяльності (operations)
- 2 роки в продажах і маркетингу

Спеціалізація:

- запуск та побудова адміністративних функцій в компанії
- створення та масштабування корпоративних процесів
- робота з ризиками



😊 LinkedIn: Anastasiia Titova

📍 Лісабон

Roosh

Roosh — інвестиційна група, яка масштабує видатні tech-компанії по всьому світу. Група інвестує у компанії з фокусом на капіталізацію ([Roosh Ventures](#)) та прибутковість (Roosh X).

Roosh має команду інвесторів, підприємців та партнерів з понад 10-річним досвідом, які не тільки фінансують бізнеси, а й допомагають їм зростати глобально.

У портфоліо Roosh також входять R&D-компанія [Neurons Lab](#), компанії [Reface](#) та [Zibra AI](#), найбільше в Україні AI-ком'юніті [AI HOUSE](#), європейське ком'юніті [Roosh Circle](#) та інші.

😊 Вебсайт: [Roosh](#)

📍 Київ



ROOSH

Програма

- 1 Кейс-стаді: досвід Roosh
- 2 Сесія запитань-відповідей з модератором

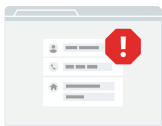
1

Кейс-стаді:
досвід Roosh



Впровадження системи кібербезпеки в Roosh

Причини серйозно займатись кібербезпекою



Настання серйозного інциденту

Настання серйозного інциденту показує вразливість компанії до кібератак і явно вказує на необхідність побудови системи кібербезпеки



Дотримання вимог

Дотримання вимог (Compliance), тобто потреба підігнати певні процеси в компанії до міжнародних стандартів для отримання потрібної сертифікації



Превентивні міри

Зрілість та превентивна робота з ризиками

Roosh розпочала свій шлях
побудови системи кібербезпеки
задля превентивної роботи з
ризиками

Роль CISO* в екосистемі Roosh

*CISO (англ. Chief Information Security Officer) – директор з інформаційної безпеки

Ключові ролі CISO



Стратег

Узгодження стратегії кіберризиків, розумне управління кібер- та інформаційними ризиками



Радник

Роль довіреної контактної особи для керівництва вищого рівня (власників ризиків)



Технолог

Оцінювання та впровадження технології безпеки для розбудови організаційних спроможностей

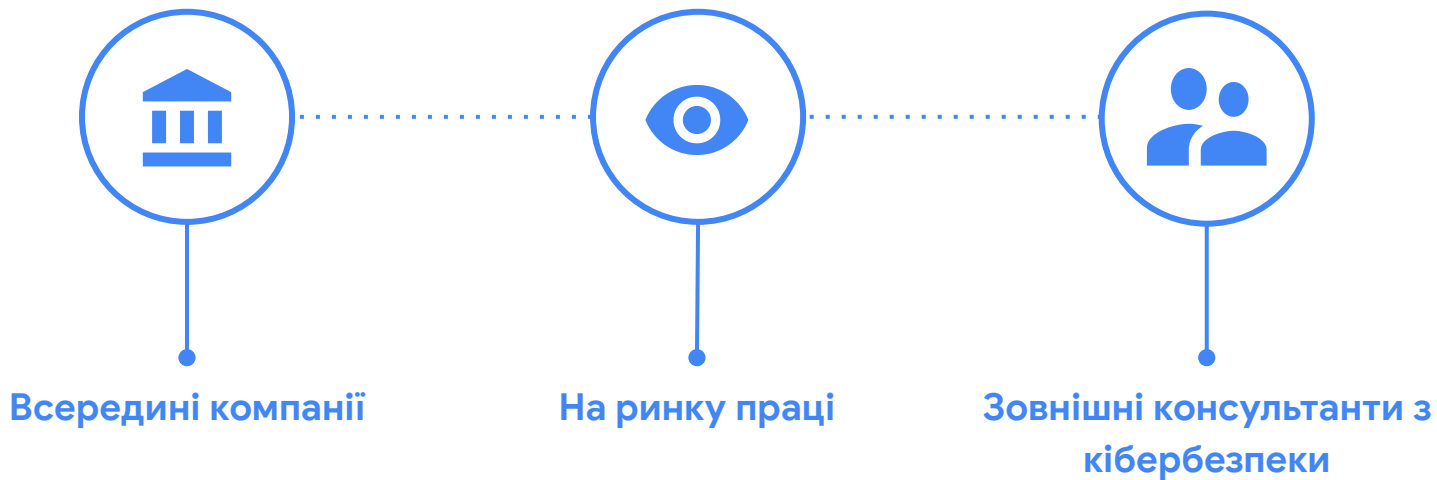


Охоронець

Захист бізнес-активів з розумінням ландшафту загроз та керуванням SOC*

*SOC (англ. Security Operations Center) – операційний центр безпеки, централізований підрозділ захисту та контролю ризиків безпеки установи.

Де шукати CISO?



Основні проблеми при пошуці CISO

1. **Наявність малої кількості фахівців** з релевантним досвідом всередині компанії
2. **Нестача спеціалістів** з кібербезпеки на ринку праці
3. **Непостійне завантаження** для CISO в малих та середніх бізнесах (МСБ)
4. **Висока вартість послуг** спеціалістів з кібербезпеки при відносно невеликому бюджеті МСБ



Який є вихід?



Розпочати побудову
системи кібербезпеки
власноруч



Шукати спеціалістів на
ринку праці з розумінням,
що це може зайняти
велику кількість часу



Звернутись за допомогою
до компаній або
незалежних консультантів
з кібербезпеки

→ Roosh обрав звернутися до консультантів

CISO як сервіс

✓ CISO як сервіс:

- виступає надійним радником з кібербезпеки
- надає уніфіковану платформу для управління ризиками, політиками та завданнями
- визначає найкращий наступний крок на шляху до кібербезпеки
- допомагає визначити технологічний обсяг роботи, необхідний для кібербезпеки
- допомагає в організації операцій з кібербезпеки

! CISO як сервіс:

- не замінює повністю штатного CISO через природу кібербезпеки
- не може взяти на себе відповідальність за ризики
- не може приймати одноосібні рішення щодо бюджетних витрат
- не є кінцевим менеджером з кібербезпеки
- не надає технологічних рішень для зменшення ризиків або автоматизації кібербезпеки



Перші кроки у побудові системи кібербезпеки

Крок 1: Аналіз поточного стану речей

1

Аналіз компонентів бізнес-контексту

- проєкти
- підрозділи
- департаменти та специфіка їх функціонування

2

З'ясування “периметру”

- визначити які підрозділи потрібно чи не потрібно захищати
- визначити які проєкти потребують окремих систем

3

Інвентаризація всіх активів

- техніка
- мережева інфраструктура
- сервіси та ПЗ
- об'єкти інтелектуальної власності тощо

Крок 2: Оцінка ризиків

1. Для кожного з активів робимо оцінку трьох параметрів (CIA) по п'ятибальній шкалі, де :

- **5 - найвищий рівень** критичності параметра для активу
- **1 - найнижчий рівень критичності**



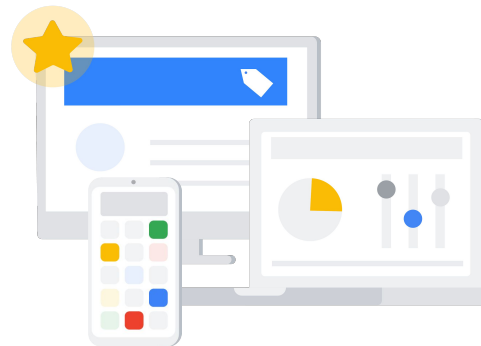
Крок 2: Оцінка ризиків

2. Робимо перелік можливих ризиків (прописуємо ризики власноруч або беремо вже наявні підходи до їх оцінки). Roosh скористався системою CIS контролів* для оцінки ризиків.

3. Оцінюємо рівень критичності наслідків тієї чи іншої загрози для кожного параметру CIA за п'ятибальною шкалою, де:

- **5 - найвищий рівень** критичності наслідків для активу
- **0 - найнижчий**, непритаманний ризик для активу

4. Оцінюємо вірогідність настання ризику кожного з цих параметрів (також за п'ятибальною шкалою).



*CIS (англ. Critical Security Controls) – міжнародно визнаний рекомендований набір найкращих практик кібербезпеки

Крок 2: Оцінка ризиків

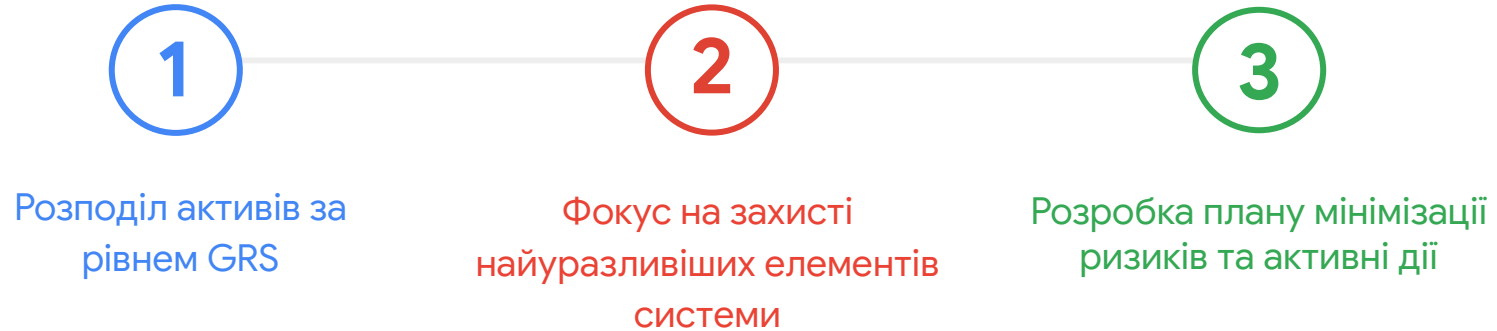
5. Рахуємо GRS* простим додаванням перемножених параметрів на вірогідність

$$\text{GRS} = \text{Asset CIA score} \times \text{Threat CIA} \times \text{Likelihood}$$



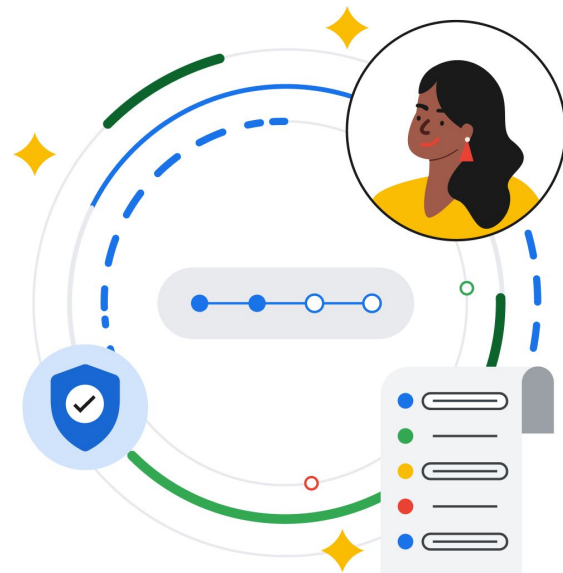
*GRS (англ. Gross Risk Score) – загальний рівень ризику

Крок 3: Пріоритезація




Побудова бази для системи кібербезпеки

- Перша оцінка ризиків Roosh – навесні 2023 року
 - Тривалість два місяці
 - Компанії з однорідною структурою можуть проходити цей етап швидше
- Повторна оцінка – влітку 2024 року

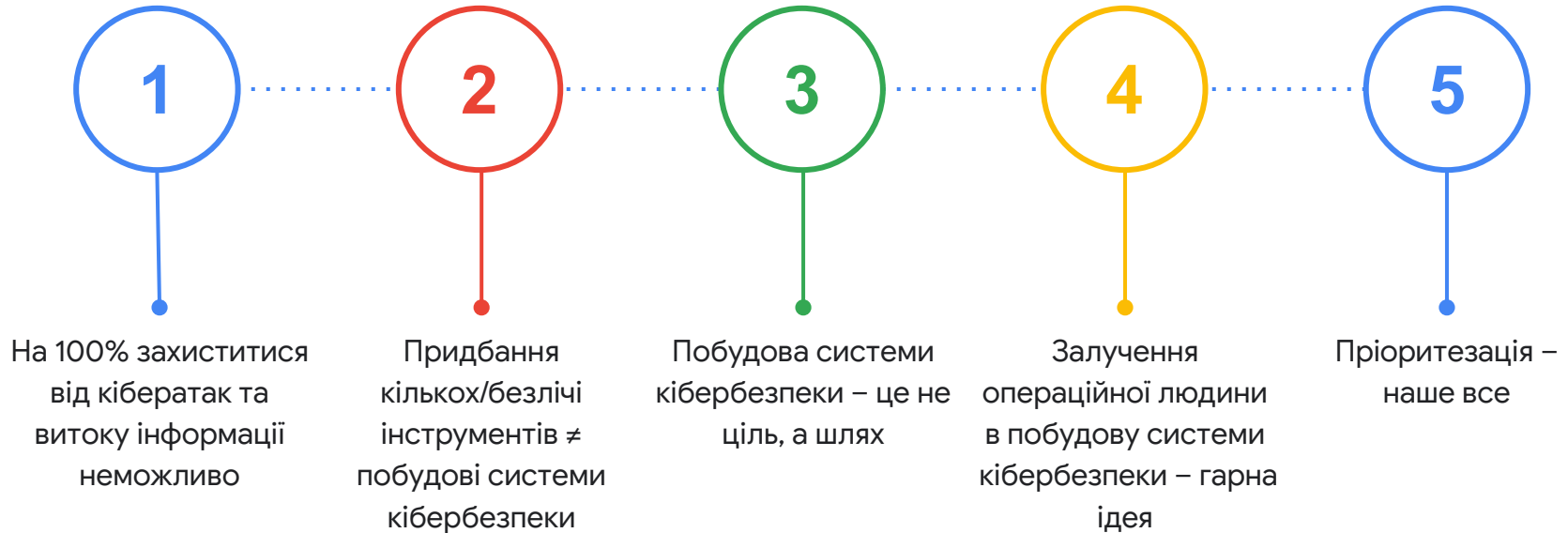


Компаніям, які динамічно
розвиваються, важливо робити
періодичну синхронізацію
бізнес-цілей та цілей в
кібербезпеці



Перша оцінка ризиків сюрпризи та усвідомлення

Сюрпризи та інсайти





Risk assessment 2.0

Нові усвідомлення

Усвідомлення №1 про переоцінку кіберризиків

Переоцінка ризиків важлива і потрібна

За 1,5 року між оцінками кіберризиків в стратегії компанії багато чого змінилося. Переоцінка дозволила:

- Розставити пріоритети згідно з новою стратегією
- Взяти в опрацювання нові портфельні компанії
- Відкласти роботу над тими ризиками, актуальність яких відпала

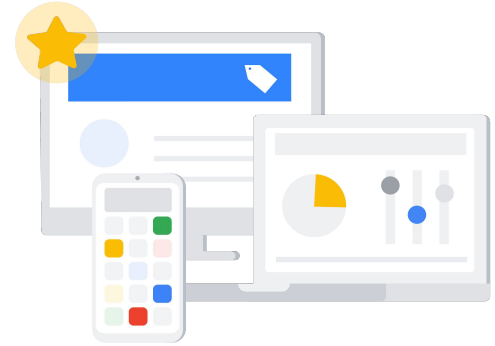


Усвідомлення №2 про переоцінку кіберризиків

Ретельна оцінка загроз (в т.ч. у фінансовому еквіваленті) дає більш чітке розуміння доцільності придбання інструментів з кібербезпеки.

Якщо вартість усунення наслідків настання певного ризику сягає \$100,000, то ґрунтовно можна інвестувати \$10,000+ в інструменти зі зменшення наслідків цього ризику.

І навпаки, якщо “вартість” настання певного ризику є незначною, то немає сенсу купляти дорогі інструменти для роботи з цим ризиком.



Усвідомлення №3 про переоцінку кіберризиків

Після первинної оцінки ризиків важливо розставити додаткові акценти

GRS (загальний рівень ризику) дає верхньорівневе розуміння вразливих місць, проте керівник разом із технічною командою можуть внести свої корективи в пріоритетність зменшення впливу цих ризиків.

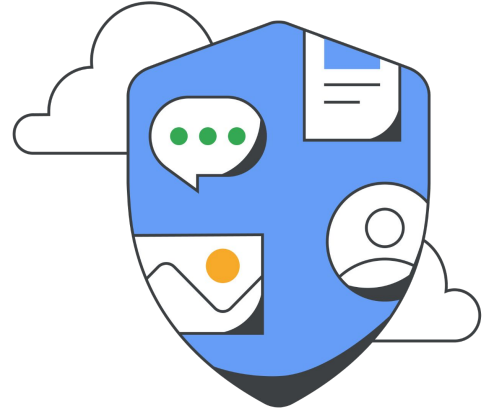
Наприклад, якщо найуразливішим активом вашої компанії є конфіденційна інформація - можна зробити додатковий фокус саме на конфіденційності.



Усвідомлення №4 про переоцінку кіберризиків

Налагоджені базові процеси в системному адмініструванні - надійна основа для кібербезпеки

Якщо базові технічні процеси (напр. онбординг, офбординг, управління ліцензіями, управління рівнями доступу) не налаштовані – кібербезпека буде страждати, навіть за наявності великої кількості дорогих інструментів.



Висновки

Сьогодні ви дізнались, що:

- **Кібербезпека** – це процес достатньо складний і комплексний, з величезною кількістю завдань, які неможливо виконати на всі 100%
- Дуже важливо рухатись системно і згідно з правильними пріоритетами
- Аналіз ризиків допомагає визначити правильні пріоритети, а періодична переоцінка ризиків дає можливість рухатись в унісон з бізнесом
- Якісно налагоджені процеси в компанії - фундамент для успішної реалізації стратегії з кібербезпеки



Дякуємо за увагу!