Асоціація малих міст УКРАЇНИ

СУПЕРМАРКЕТ РІШЕНЬ для громад

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

CyberLab Комп'ютерна криміналістика

# Управління ризиками кібербезпеки

# Короткий відступ про гранти

# План зустрічі

01 Чому це важливо?

02 Ключові етапи управління ризиками

03 Ідентифікація активів та вразливостей

04 Методи оцінки ризиків для державних структур

05 Стратегії реагування на ризик

06 Один інцидент – різні рішення

07 Система внутрішнього контролю та моніторингу

08 Практичні кроки для швидкого впровадження

# Чому це важливо сьогодні?

**Ефективне управління ризиками** це фундамент стабільної роботи організацій будь-якого масштабу.

- **Перехід на випередження.** Недостатньо реагувати на інциденти, необхідно виявляти загрози до їх реалізації.
- **Мінімізація наслідків.** Обмеження фінансових та репутаційних втрат.
- **Безперервність роботи.** Гарантія того, що критичні процеси не зупиняться через кібератаку.
- **Захист даних.** Збереження конфіденційності та цілісності інформації.

# Ключові етапи управління ризиками

**~ІДЕТИФІКАЦІЯ**

Визначення критичних активів, потенційних загроз та наявних вразливостей в інфраструктурі організації.

**~ОЦІНКА:**

Аналіз ймовірності настання інциденту та потенційного масштабу збитків (кількісна та якісна оцінка).

**~РЕАГУВАННЯ:**

Вибір оптимальної стратегії поводження з виявленим ризиком (усунення, пом'якшення, прийняття або передача).

**~МОНІТОРИНГ:**

Безперервний контроль ефективності впроваджених заходів та відстеження нових загроз у реальному часі.

# Ідентифікація активів та вразливостей

## Що ми захищаємо? (Активи)

**Критичні інформаційні активи** це основа функціонування. Щоб щось захистити, треба знати, що у нас є.

- Сервери, бази даних, хмарні сховища.
- Інтелектуальна власність та персональні дані клієнтів.
- Ключовий персонал.
- Репутація компанії та довіра партнерів.

## Де наші слабкі місця? (Вразливості)

**Вразливість** це недолік, який може бути використаний загрозою. Їх потрібно системно виявляти.

- Застаріле програмне забезпечення без патчів.
- Слабкі паролі та відсутність багатофакторної аутентифікації (MFA).
- Недостатня обізнаність персоналу (соціальна інженерія).
- Неправильно налаштовані права доступу.

# Методи оцінки ризиків для державних структур

## Які фреймворки використовувати?

NIST RMF (Risk Management Framework)

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

ISO/IEC 27005

## Специфічні фактори

Нульовий етап інвентаризації

Врахування вразливостей архітектури

Ризик невідповідності вимогам

## Кількісна чи Якісна оцінка?

Кількісна (фінансова) оцінка - оцінка коштів, що будуть втрачені, для держсектору застосовувати важко

Якісна оцінка - найбільш практичний інструмент. Використовується класична формула Ризик = Ймовірність × Наслідки.

# Стратегії реагування на ризик

### Пом'якшення (Mitigate)

Впровадження засобів контролю для зменшення ймовірності або впливу. Наприклад: встановлення антивірусу, налаштування фаєрволу.

### Уникнення (Avoid)

Повна відмова від діяльності, що створює ризик. Наприклад: відключення вразливого старого сервера, заборона використання флешок.

### Передача (Transfer)

Перенесення фінансових або операційних наслідків на третю сторону. Наприклад: кіберстрахування, аутсорсинг хмарному провайдеру.

### Прийняття (Accept)

Свідома згода на ризик, якщо вартість захисту перевищує можливі збитки. Застосовується лише для ризиків низького рівня.

# Один інцидент – різні рішення

**У кібербезпеці немає універсальних відповідей. Стратегія реагування завжди залежить від контексту та критичності активу.**

Розглянемо сценарій: "Втрата службового ноутбука або флешки".

## Контекст А: Відсутність цінної інформації

На флешці були лише публічні презентації з останньої сесії міськради та фотографії з корпоративу. Інформаційна цінність нульова. Рішення: просто списуємо носій і купуємо новий.

Ризик ПРИЙМАЄМО

## Контекст Б: Це ноутбук, з яким часто їздять у відрядження.

Знаючи про ризик втрати, ви заздалегідь налаштували повне шифрування диска (BitLocker), складні паролі та можливість віддаленого стирання через MDM. Рішення: залізо втрачено (фінансовий збиток), але інформація у безпеці.

Ризик ПОМ’ЯКШЕНО.

## Контекст В: Страховка

Організація страхує корпоративну техніку від крадіжки чи втрати. Страхова компанія покриває вартість нового ноутбука.

Ризик ПЕРЕДАЄМО.

## Контекст Г: Робота з надзвичайно чутливими даними.

Робота з надзвичайно чутливими даними (наприклад, реєстр військовозобов'язаних). Рішення: політика "нульової довіри" — відключення USB-портів на всіх ПК, фізична заборона виносити техніку за межі захищеного периметра.

Ризику УНИКАЄМО.

# Один інцидент – різні рішення

Розглянемо разом декілька прикладів:

- Виявлено критичну вразливість (наприклад, у старій Windows 7.
- Потужна DDoS-атака на вебсайт організації.
- Виявлено критичну вразливість (напр., Log4j) у програмному забезпеченні

# Система внутрішнього контролю та моніторингу

**Керування ризиками не закінчується на папері.** Це безперервний процес, що вимагає постійного нагляду та оперативного реагування на інциденти.

- SIEM-системи: Централізований збір та аналіз подій безпеки з усієї інфраструктури.
- План реагування (IRP): Чіткі інструкції для команди: хто що робить у перші хвилини атаки.
- Регулярні аудити: Періодичне сканування на вразливості та пентести.
- Показники ефективності: Відстеження метрик ефективності безпеки (наприклад, середній час виявлення загрози).

# Практичні кроки для швидкого впровадження

**01 Інвентаризація**

Складіть повний реєстр IT-активів, даних та доступу користувачів. Знайдіть найважливіше.

**02 Базова безпека**

Впровадьте базові контролі: MFA, оновлення ПЗ, бекапи (правило 3-2-1), управління паролями.

**03 Навчання**

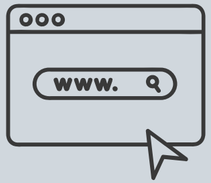
Проведіть тренінги для співробітників щодо фішингу та соціальної інженерії. Створіть культуру безпеки.

**04 Оцінка та адаптація**

Проведіть першу оцінку ризиків, розробіть план обробки та регулярно переглядайте стратегію.

# Як звернутися до служби підтримки кібербезпеки

Служба підтримки - це швидкий доступ до фахової допомоги у сфері кібербезпеки




**Заповнити звернення на сайті Супермаркет рішень для громад**

через кнопку «Звернутися до служби підтримки» на сайті supersolution.net.ua

**Отримати зворотній зв’язок**

АСОЦІАЦІЯ МАЛИХ МІСТ УКРАЇНИ

СУПЕРМАРКЕТ РІШЕНЬ для громад

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

CyberLab Комп'ютерна криміналістика

Служба підтримки

+38 (096) 380 17 39, +38 (093) 477 50 67