Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

«Технології захисту інформації»

Лабораторна робота №3

Управління ризиками та моделювання загроз

Виконав:

Студент 4-го курсу

Групи KN1-B22

Демченко Дмитро

Кам’янець-Подільський – 2025

**Мета:** розробити модель загроз для простої системи, оцінити ризики.

**1. Інвентаризація активів**

1.1 База даних (БД)

* Опис: postgresql/mysql сервер з критичними бізнес-даними
* Розташування: Внутрішня мережа (192.168.1.10)
* Критичність: ВИСОКА
* Дані: Персональні дані користувачів, фінансові записи, облікові дані

1.2 Веб-сервер

* Опис: Apache/Nginx веб-сервер з публічним додатком
* Розташування: DMZ (10.0.1.5), доступний з Інтернету
* Критичність: СЕРЕДНЯ
* Функції: Обробка HTTP/HTTPS запитів, взаємодія з БД

1.3 Робочі станції (10 шт.)

* Опис: Windows 10/11 комп'ютери співробітників
* Розташування: Внутрішня мережа (192.168.1.20-30)
* Критичність: СЕРЕДНЯ
* Використання: Доступ до внутрішніх систем, електронна пошта, документообіг

**2. Ідентифікація загроз за тріадою CIA**

2.1 База даних

Конфіденційність (Confidentiality)

* З-1.1: SQL-ін'єкції через веб-додаток
* З-1.2: Несанкціонований доступ через скомпрометовані облікові дані
* З-1.3: Витік даних через інсайдерів
* З-1.4: Перехоплення трафіку БД (відсутність шифрування)

Цілісність (Integrity)

* З-1.5: Модифікація даних зловмисниками після злому
* З-1.6: Помилки в резервних копіях (corrupted backups)
* З-1.7: Атаки типу "людина посередині" (MITM)

Доступність (Availability)

* З-1.8: ddos атаки на сервер БД
* З-1.9: Ransomware шифрування бази даних
* З-1.10: Відмова обладнання (апаратний збій)

2.2 Веб-сервер

Конфіденційність

* З-2.1: Експлуатація вразливостей веб-додатку (OWASP Top 10)
* З-2.2: Витік конфігураційних файлів з паролями
* З-2.3: Компрометація SSL/TLS сертифікатів

Цілісність

* З-2.4: Дефейс сайту (зміна вмісту)
* З-2.5: Впровадження шкідливого коду (backdoor)
* З-2.6: Підміна контенту через XSS атаки

Доступність

* З-2.7: ddos атаки layer 7 (HTTP flood)
* З-2.8: Вичерпання ресурсів сервера
* З-2.9: Відмова служби через експлойти

2.3 Робочі станції

Конфіденційність

* З-3.1: Фішингові атаки на співробітників
* З-3.2: Крадіжка облікових даних через keylogger
* З-3.3: Фізичний доступ до незаблокованих ПК

Цілісність

* З-3.4: Зараження шкідливим ПЗ (malware)
* З-3.5: Несанкціонована модифікація системних файлів
* З-3.6: Встановлення неліцензійного ПЗ

Доступність

* З-3.7: Ransomware атаки на робочі станції
* З-3.8: Відмова системи через оновлення
* З-3.9: Проблеми з мережевим підключенням

**3. Матриця оцінки ризиків**

3.1 Шкала оцінювання

Ймовірність (Probability):

* 1 = Дуже низька (< 5%)
* 2 = Низька (5-25%)
* 3 = Середня (25-50%)
* 4 = Висока (50-75%)
* 5 = Дуже висока (> 75%)

Вплив (Impact):

* 1 = Незначний (мінімальні втрати)
* 2 = Низький (< 10,000 грн)
* 3 = Середній (10,000-100,000 грн)
* 4 = Високий (100,000-500,000 грн)
* 5 = Критичний (> 500,000 грн)

Рівень ризику = Ймовірність × Вплив

* 1-6: НИЗЬКИЙ (зелений)
* 8-12: СЕРЕДНІЙ (жовтий)
* 15-25: ВИСОКИЙ (червоний)

3.2 Оцінка ризиків для БД

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Загроза | Ймовірність | Вплив | Ризик | Рівень |
| З-1.1 | SQL-ін'єкції | 4 | 5 | 20 | Високий |
| З-1.2 | Несанкціонований доступ | 3 | 5 | 15 | Високий |
| З-1.3 | Витік через інсайдерів | 2 | 5 | 10 | Середній |
| З-1.4 | Перехоплення трафіку | 3 | 4 | 12 | Середній |
| З-1.5 | Модифікація даних | 3 | 5 | 15 | Високий |
| З-1.6 | Пошкоджені резервні копії | 2 | 4 | 8 | Середній |
| З-1.7 | MITM атаки | 2 | 4 | 8 | Середній |
| З-1.8 | Ddos на БД | 2 | 3 | 6 | Низький |
| З-1.9 | Ransomware | 3 | 5 | 15 | Високий |
| З-1.10 | Апаратний збій | 2 | 4 | 8 | Середній |

3.3 Оцінка ризиків для веб-сервера

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Загроза | Ймовірність | Вплив | Ризик | Рівень |
| З-2.1 | Експлуатація вразливостей | 4 | 4 | 16 | Високий |
| З-2.2 | Витік конфігурацій | 3 | 3 | 9 | Середній |
| З-2.3 | Компрометація SSL/TLS | 2 | 3 | 6 | Низький |
| З-2.4 | Дефейс сайту | 3 | 3 | 9 | Середній |
| З-2.5 | Backdoor впровадження | 3 | 5 | 15 | Високий |
| З-2.6 | XSS атаки | 4 | 3 | 12 | Середній |
| З-2.7 | Ddos HTTP flood | 4 | 4 | 16 | Високий |
| З-2.8 | Вичерпання ресурсів | 3 | 3 | 9 | Середній |
| З-2.9 | Відмова через експлойти | 3 | 4 | 12 | Середній |

3.4 Оцінка ризиків для робочих станцій

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Загроза | Ймовірність | Вплив | Ризик | Рівень |
| З-3.1 | Фішингові атаки | 5 | 4 | 20 | Високий |
| З-3.2 | Keylogger крадіжка | 3 | 4 | 12 | Середній |
| З-3.3 | Фізичний доступ | 2 | 3 | 6 | Низький |
| З-3.4 | Malware зараження | 4 | 4 | 16 | Високий |
| З-3.5 | Модифікація системи | 2 | 3 | 6 | Низький |
| З-3.6 | Неліцензійне ПЗ | 3 | 2 | 6 | Низький |
| З-3.7 | Ransomware | 4 | 5 | 20 | Високий |
| З-3.8 | Відмова через оновлення | 2 | 2 | 4 | Низький |
| З-3.9 | Мережеві проблеми | 3 | 2 | 6 | Низький |

**4. Пріоритизація ризиків**

Критичні ризики (20-25 балів)

1. З-1.1 — SQL-ін'єкції (20)
2. З-3.1 — Фішингові атаки (20)
3. З-3.7 — Ransomware на станціях (20)

Високі ризики (15-16 балів)

1. З-1.2 — Несанкціонований доступ до БД (15)
2. З-1.5 — Модифікація даних БД (15)
3. З-1.9 — Ransomware на БД (15)
4. З-2.1 — Експлуатація вразливостей веб (16)
5. З-2.5 — Backdoor на веб-сервері (15)
6. З-2.7 — ddos HTTP flood (16)
7. З-3.4 — Malware на станціях (16)

Середні ризики (8-12 балів)

* 10 ризиків середнього рівня

Низькі ризики (1-6 балів)

* 7 ризиків низького рівня

**5. Контрзаходи та рекомендації**

5.1 Захист бази даних

Проти SQL-ін'єкцій (З-1.1)

Контрзаходи:

* Використання параметризованих запитів (prepared statements)
* Валідація та санітизація всіх вхідних даних
* Застосування WAF (Web Application Firewall)
* Регулярне тестування на проникнення
* Принцип найменших привілеїв для облікових записів БД

Пріоритет: КРИТИЧНИЙ  
Вартість впровадження: Середня  
Термін: 1-2 тижні

Проти несанкціонованого доступу (З-1.2)

Контрзаходи:

* MFA (Multi-Factor Authentication) для адміністраторів БД
* Сильна парольна політика (мінімум 12 символів)
* Whitelist IP-адрес для доступу до БД
* Моніторинг спроб входу та блокування після невдач
* Регулярний аудит облікових записів

Пріоритет: ВИСОКИЙ  
Вартість впровадження: Низька  
Термін: 1 тиждень

Проти Ransomware (З-1.9)

Контрзаходи:

* Резервне копіювання 3-2-1:
  + 3 копії даних
  + 2 різні носії
  + 1 копія офсайт (cloud або віддалена локація)
* Автоматичне створення backup кожні 6 годин
* Тестування відновлення щомісяця
* Ізоляція БД від Інтернету
* Snapshot на рівні storage

Пріоритет: ВИСОКИЙ  
Вартість впровадження: Середня  
Термін: 2-3 тижні

Шифрування трафіку (З-1.4, З-1.7)

Контрзаходи:

* SSL/TLS для всіх з'єднань до БД
* Шифрування даних у спокої (encryption at rest)
* VPN тунель між веб-сервером та БД
* Certificates pinning

Пріоритет: СЕРЕДНІЙ  
Вартість впровадження: Низька  
Термін: 1 тиждень

5.2 Захист веб-сервера

Проти експлуатації вразливостей (З-2.1, З-2.5)

Контрзаходи:

* Регулярне оновлення ПЗ та патчі безпеки
* Сканування вразливостей (Nessus, openvas)
* Впровадження WAF (modsecurity, Cloudflare)
* Відключення непотрібних сервісів
* Security headers (CSP, HSTS, X-Frame-Options)
* Code review та SAST/DAST тестування

Пріоритет: ВИСОКИЙ  
Вартість впровадження: Середня  
Термін: 2-4 тижні

Проти ddos атак (З-2.7)

Контрзаходи:

* Використання CDN з ddos захистом (Cloudflare, Akamai)
* Rate limiting на рівні nginx/Apache
* Fail2ban для блокування зловмисних IP
* Load balancer з розподілом навантаження
* Моніторинг трафіку в реальному часі

Пріоритет: ВИСОКИЙ  
Вартість впровадження: Висока  
Термін: 3-4 тижні

Сегментація мережі

Контрзаходи:

* Розміщення веб-сервера в DMZ
* Firewall правила між DMZ та внутрішньою мережею
* Дозволити тільки необхідні порти (80, 443, 3306 до БД)
* VLAN сегментація
* IDS/IPS системи (Snort, Suricata)

Пріоритет: ВИСОКИЙ  
Вартість впровадження: Середня  
Термін: 2-3 тижні

5.3 Захист робочих станцій

Проти фішингу (З-3.1)

Контрзаходи:

* Тренінги з кібербезпеки для співробітників (щоквартально)
* Симуляція фішингових атак
* Email фільтрація з anti-phishing (Proofpoint, Mimecast)
* MFA для всіх корпоративних додатків
* Блокування підозрілих посилань

Пріоритет: КРИТИЧНИЙ  
Вартість впровадження: Середня  
Термін: Постійно (тренінги)

Проти Ransomware та Malware (З-3.7, З-3.4)

Контрзаходи:

* Антивірус корпоративного класу (Kaspersky, ESET, Symantec)
* EDR рішення (Endpoint Detection and Response)
* Application whitelisting
* Відключення макросів у Office за замовчуванням
* Автоматичне резервне копіювання робочих станцій
* Блокування виконання файлів з тимчасових папок
* Patch management система

Пріоритет: КРИТИЧНИЙ  
Вартість впровадження: Висока  
Термін: 3-4 тижні

Контроль доступу (З-3.2, З-3.3)

Контрзаходи:

* Автоматичне блокування ПК після 5 хв. Неактивності
* Шифрування дисків (bitlocker, veracrypt)
* Відеоспостереження в робочих зонах
* MFA для входу в Windows
* USB контроль (блокування невідомих пристроїв)
* Least privilege principle для користувачів

Пріоритет: СЕРЕДНІЙ  
Вартість впровадження: Низька  
Термін: 1-2 тижні

**6. План впровадження (roadmap)**

Фаза 1: Критичні заходи (0-1 місяць)

Тиждень 1-2:

* Впровадження MFA для БД та корпоративних систем
* Налаштування параметризованих запитів (проти SQL-ін'єкцій)
* Початок тренінгів з фішингу для співробітників

Тиждень 3-4:

* Налаштування резервного копіювання БД (3-2-1)
* Встановлення антивірусу та EDR на всі станції
* Базова сегментація мережі (DMZ для веб-сервера)

Фаза 2: Високі ризики (1-2 місяць)

Тиждень 5-8:

* Впровадження WAF для веб-сервера
* Налаштування ddos захисту через CDN
* Шифрування трафіку БД (SSL/TLS)
* Регулярне сканування вразливостей

Фаза 3: Середні ризики (2-3 місяць)

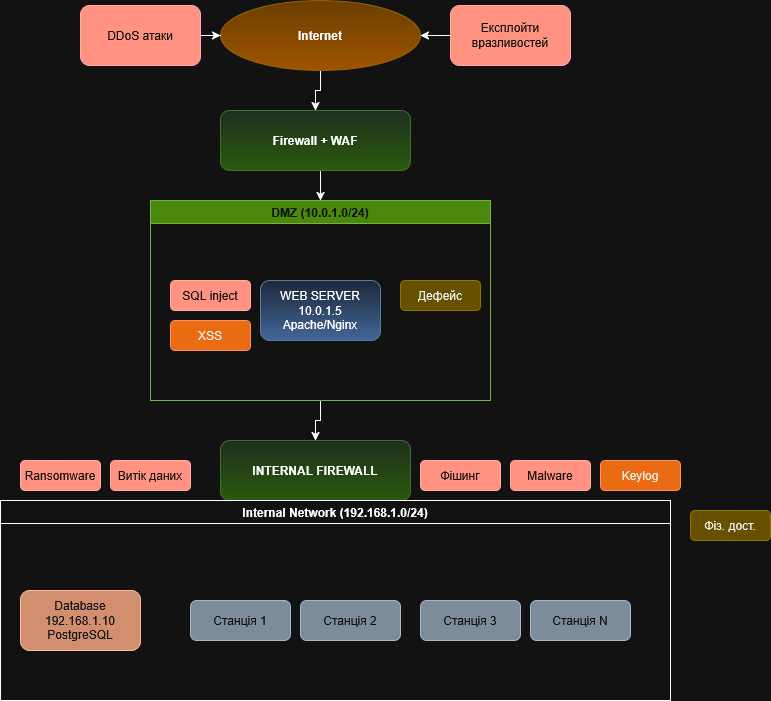
Тиждень 9-12:

* IDS/IPS системи
* Поглиблена сегментація мережі (VLAN)
* USB контроль та шифрування дисків
* Автоматизація patch management

Фаза 4: Постійна підтримка

* Щомісячні тренінги безпеки
* Щоквартальні пентести
* Регулярний аудит безпеки
* Моніторинг та інцидент-менеджмент

**Архітектура системи**



**ВИСНОВКИ**

Ключові знахідки:

1. Виявлено 28 загроз різного рівня критичності
2. 10 ризиків високого рівня потребують негайного втручання
3. Людський фактор — найбільша проблема (фішинг, ransomware)
4. Відсутність сегментації мережі дозволяє lateral movement

Найкритичніші вразливості:

* SQL-ін'єкції у веб-додатку
* Відсутність MFA для адміністративних облікових записів
* Слабка підготовка співробітників до соціальної інженерії
* Недостатнє резервне копіювання