Міністерство освіти і науки України
НТУУ «КПІ ім. Ігоря Сікорського»
Навчально-науковий інститут атомної та теплової енергетики
Кафедра цифрових технологій в енергетиці

Лабораторна робота №3

з дисципліни

«Інформаційне забезпечення комп’ютерних систем»

Тема «Аналіз ризиків та основні принципи забезпечення безпеки»

Варіант №18

Студента 4-го курсу НН ІАТЕ гр. ТР-12
Ковальова Олександра
Перевірив: доцент, Онисько А. І.

КИЇВ 2024

Мета роботи. Ознайомлення та дослідження алгоритму оцінки ризиків інформаційної безпеки організації, набуття практичних навичок щодо застосування методики матричного аналізу ризиків інформаційної безпеки та надання основних рекомендацій з забезпечення безпеки.

Індивідуальне завдання:

Варіант – 18. Організація – приватна поліклініка. Кількість активів – 5.

Хід роботи

Для виконання цієї лабораторної роботи створимо матриці та проведемо аналіз ризиків для приватної поліклініки.

Опис організації та її інформаційних активів:

Приватна поліклініка надає медичні послуги та обробляє чутливу медичну інформацію. Основні інформаційні активи включають:

- Медичні записи пацієнтів
- Інформаційні системи (для управління та реєстрації пацієнтів)
- Системи комунікації з пацієнтами (телефонія, електронна пошта)
- Обладнання для зберігання даних (сервери та комп’ютери)
- Персональні дані співробітників та пацієнтів

Можливі уразливості:

- Відсутність шифрування даних.
- Низький рівень захисту від зовнішніх атак.
- Ненадійні паролі персоналу.
- Відсутність резервного копіювання.
- Ненадійне фізичне розміщення апаратури.

Загрози:

- Кібератаки (включаючи зломи, фішинг).
- Несанкціонований доступ до медичних записів.
- Фізичне пошкодження обладнання.
- Втрата фінансової інформації.
- Витік конфіденційної інформації.

Заходи контролю:

- Шифрування даних.
- Навчання персоналу з інформаційної безпеки.
- Використання двофакторної аутентифікації.
- Системи резервного копіювання.
- Фізичний захист обладнання.

Матриця уразливостей (активи-уразливості):

Вартість активів:				
Медичні записи пацієнтів	*Інформаційні системи*	*Системи комунікації з пацієнтами*	*Обладнання для зберігання даних*	*Персональні дані співробітників та пацієнтів*
4	4	3	4	4

Активи / Уразливості	**Медичні записи пацієнтів**	**Інформаційні системи**	**Системи комунікації з пацієнтами**	**Обладнання для зберігання даних**	**Персональні дані співробітників та пацієнтів**	***Всього: (Σ)***	***Ранжування:***
Шифрування	5	5	3	1	5	73	1
Захист від атак	3	5	3	3	3	65	2
Паролі	3	3	3	1	5	57	3
Резервування	5	3	1	1	3	51	4
Фізичне розміщення	1	1	1	5	1	35	5

Де ранги пріоритетів:

- 1 – незначний;
- 2 – невеликий;
- 3 – середній;
- 4 – серйозний;
- 5 – критичний;

Матриця загроз (уразливості-загрози):

Загрози / Уразливості	**Шифрування**	**Захист від атак**	**Паролі**	**Резервування**	**Фізичне розміщення**	***Всього: (Σ)***	***Ранжування:***
Кібератаки (включаючи зломи, фішинг).	5	5	5	3	1	19	1
Несанкціонований доступ до медичних записів	3	3	5	3	1	15	4
Фізичне пошкодження обладнання	1	1	1	1	5	9	5
Втрата фінансової інформації	5	3	3	5	1	17	2
Витік конфіденційної інформації	5	3	5	3	1	17	2

Матриця засобів контролю (засоби контролю-загрози):

Засоби контролю / загрози	**Кібератаки (включаючи зломи, фішинг).**	**Несанкціонований доступ до медичних записів**	**Фізичне пошкодження обладнання**	**Втрата фінансової інформації**	**Витік конфіденційної інформації**	***Всього: (Σ)***	***Ранжування:***
Шифрування даних	5	5	1	5	5	21	1
Навчання персоналу з інформаційної безпеки	3	5	3	3	5	19	2
Використання двофакторної аутентифікації	5	5	1	3	3	17	3
Системи резервного копіювання	3	3	1	5	3	15	4
Фізичний захист обладнання	1	1	5	1	1	9	5

Рекомендації для забезпечення безпеки:

- *Шифрування даних:* Забезпечити, щоб усі медичні записи та фінансова інформація були зашифровані, що значно знизить ризик витоку даних.
- *Навчання персоналу:* Провести тренінги з інформаційної безпеки, включаючи виявлення фішингових атак, що знизить ймовірність кібератак та несанкціонованого доступу.
- *Двофакторна аутентифікація:* Встановити двофакторну аутентифікацію для всіх систем доступу до чутливих даних, що зменшить ризики вказані в останній матриці.
- *Резервне копіювання:* Налаштувати системи резервного копіювання для забезпечення доступності фінансової інформації у випадку її втрати.
- *Фізичний захист обладнання:* Підсилити фізичну охорону медичної апаратури та серверів, що зменшить ризик фізичного пошкодження.

Висновок.

У ході виконання лабораторної роботи було проведено аналіз ризиків інформаційної безпеки для приватної поліклініки за допомогою матричного підходу. Виявлено критичні активи, основні уразливості, можливі загрози, а також відповідні заходи контролю для зниження ризиків. Проведений аналіз показав, що медичні записи, інформаційні системи та персональні дані є найбільш цінними активами, які потребують особливого захисту, а основні загрози включають кібератаки, витік інформації та фізичне пошкодження обладнання. В результаті були запропоновані конкретні заходи захисту, такі як шифрування, навчання персоналу, двофакторна аутентифікація, резервне копіювання та фізична охорона, що сприятиме підвищенню загальної безпеки поліклініки.

Відповіді на контрольні питання:

1. ***Як класифікуються загрози за результатами їх впливу на інформацію?***
   Загрози класифікуються за їх впливом на три основні властивості інформації: конфіденційність, цілісність та доступність. Порушення конфіденційності загрожує розголошенням інформації, порушення цілісності – її зміною або знищенням, а порушення доступності – недоступністю інформації у потрібний момент.
2. ***Що таке НСД і які існують способи його реалізації?***
   Несанкціонований доступ (НСД) – це доступ до інформаційних ресурсів або систем без дозволу. Способи його реалізації включають підбір паролів, фішингові атаки, використання вразливостей у програмному забезпеченні та фізичний доступ до обладнання.
3. ***Які повинна вирішувати завдання система забезпечення безпеки комп'ютерної системи?***
   Система безпеки комп'ютерної системи повинна забезпечувати розмежування доступу, захист даних, реєстрацію подій, моніторинг роботи користувачів, а також підтримувати цілісність і доступність інформаційних ресурсів.
4. ***Які існують поширені прийоми НСД?***

Поширені прийоми НСД включають соціальну інженерію, підробку ідентифікаційних даних, використання троянських програм і фішингових повідомлень, які спрямовані на отримання особистих даних користувача.

5. ***Які існують основні категорії мережевих атак?***
   Основні категорії мережевих атак включають атаки на доступність, такі як DoS-атаки; атаки на конфіденційність, наприклад, перехоплення трафіку; атаки на цілісність, як-от маніпулювання даними; і атаки на автентифікацію, наприклад, викрадення облікових даних.
6. ***У чому полягають принципи управління доступом?***
   Управління доступом базується на принципах розмежування доступу, обмеження прав користувачів до необхідного мінімуму, а також моніторингу та контролю доступу до ресурсів. Це дозволяє захистити інформаційні ресурси від несанкціонованого використання.
7. ***У чому сенс концепції матриці доступу?***
   Концепція матриці доступу передбачає організацію доступу до ресурсів на основі правил, що визначають, хто має право на виконання певних дій з конкретними ресурсами. Це дозволяє чітко визначити права доступу та обмеження для кожного користувача.
8. ***Що є функціями і механізмами захисту?***
   Функції захисту включають автентифікацію, контроль доступу, моніторинг та реєстрацію подій, шифрування даних, а також резервне копіювання. Механізми захисту можуть включати брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та засоби фізичного захисту.