НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО”
КАФЕДРА АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ

Комп’ютерний практикум № 7
з дисципліни
“Основи захисту інформації”
Варіант 11

Виконав:
студент групи ІС-72
Кривохижа Р.А.

Перевірив:
асистент
Ільїн К.І.

Київ-2020

Тема: Побудова моделі порушника в АС класу 3

Мета: Навчитись аналізувати середовища функціонування інформаційної системи, будувати модель загроз та модель порушника.

Хід роботи:

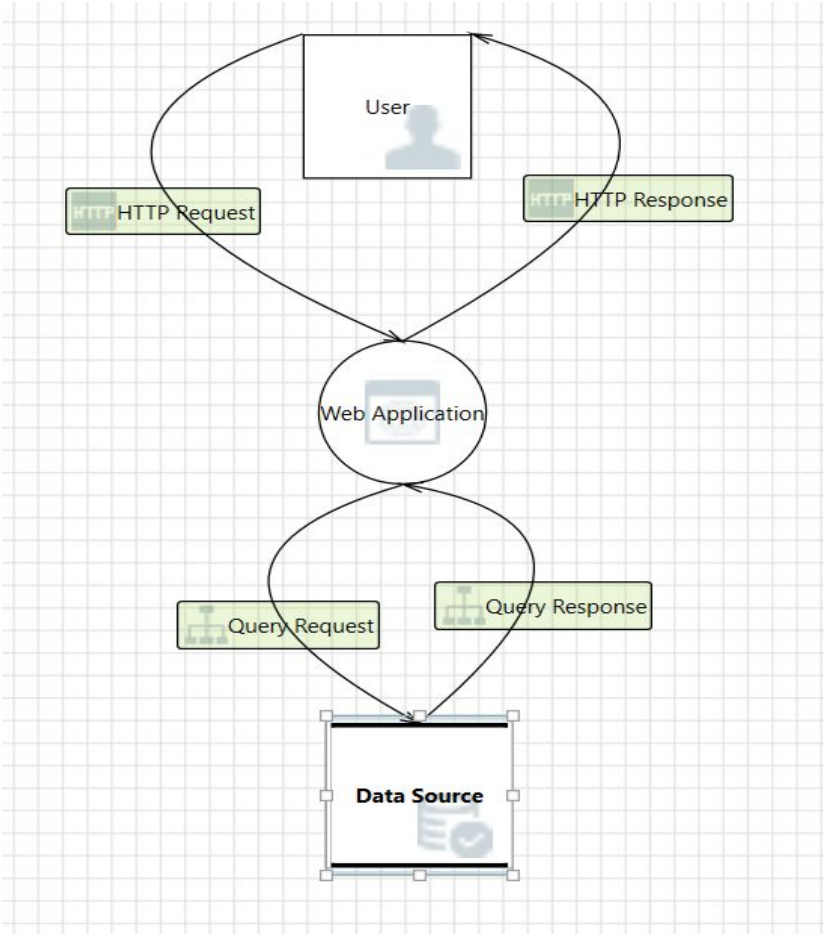

Рис. 1 – Діаграма інформаційних потоків у мережі факультету (система https://do.ipo.kpi.ua/)

Threat List

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
1	HTTP Response		Generated	Not Started	Cross Site Scri...	Tampering	The web server...		HTTP Request	High
2	HTTP Response		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	Web Applicati...		HTTP Request	High
3	HTTP Response		Generated	Not Started	Spoofing of D...	Spoofing	Data Source m...		Query Request	High
4	HTTP Response		Generated	Not Started	Potential SQL I...	Tampering	SQL injection i...		Query Request	High
5	HTTP Response		Generated	Not Started	Potential Exces...	Denial Of Servi...	Does Web Ap...		Query Request	High
6	HTTP Response		Generated	Not Started	Spoofing of S...	Spoofing	Data Source m...		Query Response	High
7	HTTP Response		Generated	Not Started	Cross Site Scri...	Tampering	The web server...		Query Response	High
8	HTTP Response		Generated	Not Started	Persistent Cros...	Tampering	The web server...		Query Response	High
9	HTTP Response		Generated	Not Started	Weak Access C...	Information Di...	Improper data...		Query Response	High
10	HTTP Response		Generated	Not Started	Spoofing the...	Spoofing	User may be s...		HTTP Request	High

Рис. 2 – Загрози, притаманні системі та їх класифікація

Модель порушника

Категорія Порушника	**Кваліфікація**	**Права в системі**	**Засоби, якими володіє порушник**
Адміністратор БД	Висока	Доступ до БД, управління БД, редагування, запис, видалення.	СКБД
Адміністратор криптографічної підсистеми	Середня	Доступ до системи шифратора, встановлення, зміна, видалення алгоритму шифрування.	Апаратні та програмні інструменти криптографічних систем
Оператор	Середня	Обробка інформації, яка міститься в базі даних ІС.	СКБД
Адміністратор ОС	Середня	Установка і оновлення ПЗ, підключення і настройка апаратних пристроїв, настройка мережних протоколів і політики безпеки.	Системний засіб управління аудиту
Розробник	Висока	Модифікація вихідного коду, проведення тестування ПЗ.	Програмні засоби розробки початкового коду
Технічний персонал	Низька	Доступ до приміщень з апаратним і програмним забезпеченням. Обслуговування приміщення.	Ручний інструмент
Зовнішній користувач	Низька	Користування ресурсами системи: читання, запис, редагування(поштова скринька), читання(FTP-сервер)	Спеціалізований набір програмних засобів проникнення в систему, через доступні ресурси.

Модель загроз

1.На атакуючому

Загроза	**Джерело загрози**	**Імовірність + Наслідки**	**Мета (ресурс + порушення К, Ц, Д чи С Конфіденційність/ Цілісність/Доступність/ Спостережність (чи їх комбінацію))**	**Порушник**
Порушення фізичної цілісності АС (її окремих компонентів), пристроїв, обладнання, носіїв інформації	Сервери, БД	Висока + Катастрофічні	Веб-сервер, сервер застосунків, БД к, ц, д, с	Технічний персонал, зовнішній користувач
Модифікація інформаційних ресурсів, в тому числі програмного забезпечення	Сервери	Низька + Катастрофічні	Веб-сервер, сервер застосунків ц, д, с	Оператор, адміністратор ОС, розробник
Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, заземлення, охоронної чи пожежної сигналізації, вентиляції та ін.)	Внутрішня мережа	Висока + Катастрофічні	Фізичні компоненти ц, д, с	Технічний персонал
Отримання несанкціонованого доступу до вузлів	Внутрішня мережа	Висока + катастрофічні	Сервери, робочі комп'ютери +ДКЦС	Адміністратор мережі
Підміна алгоритму шифрування	Шифратор	Середня + катастрофічна	БД+ЦДК	Адміністратор криптографіч

для викрадення інформації				ної підсистеми
Модифікація даних	БД	Висока + катастрофічна	БД+СКЦ	Адміністратор БД
Приховування дій	Система аудиту	Середня + прийнятна	Журнал аудиту + С	Системний адміністратор
Отримання несанкціонованого доступу до внутрішньої мережі	Внутрішня мережа	Середня + катастрофічна	Доступ до БД + СКЦД	Зовнішні користувачі
Викрадення зовнішніх носіїв	Сервери, робочі станції	Висока + катастрофічна	Носії інформації, фізичні компоненти + ЦДК	Технічний персонал
Внесення шкідливого коду	Програмний код	Висока + прийнятна	Програмна закладка + ЦКДС	Розробник

2. На ПЗ

	Загроза	**Джерело загрози**	**Імовірність+наслідки**	**Мета (ресурс + порушення С, К, Ц, Д)**	**Порушник**
https://www.cvedetails.com/cve/CVE-2017-11771/	Windows Search Remote Code Execution Vulnerability	MS Windows Server 2016	Висока + катастрофічна	Сервер + КЦД	Адміністратор мережі
http://www.cvedetails.com/cve/CVE-2015-6111/	Windows IPSec Denial of Service Vulnerability	Windows 8	Висока + прийнятна	Сервер + Д	Користувач

http://www.cvedetails.com/cve/CVE-2011-5279/	CRLF injection vulnerability	IIS	Середня + прийнятна	Сервер + ЦД	Користувач
http://www.cvedetails.com/cve/CVE-2002-1138/	Flaw in Output File Handling for Scheduled Jobs	MS SQL	Висока + прийнятна	БД + КЦД	Персонал, адміністратор БД
https://www.cvedetails.com/cve/CVE-2009-2853/	Gain privileges	Word Press 2.7	Висока + катастрофічна	Веб-сервер + КЦД	Користувач

3.На ресурси БД:

Загроза	**Джерело загрози**	**Імовірність+наслідки**	**Мета (ресурс + порушення С, К, Ц, Д)**	**Порушник**
SQL ін’єкція	БД	Висока + катастрофічна	Конф. Інформація + КЦ	Адміністратори, користувачі
Використання команд UPDATE, INSERT, DELETE	БД	Висока + катастрофічна	Конф. Інф. + КЦ	Адміністратори, користувачі
DoS-атака	БД	Середня + прийнятна	ЦДС	Адміністратори, користувачі

Висновок:

У ході виконання лабораторної роботи було проаналізовано середовища функціонування інформаційної системи, побудовано моделі загроз та порушника.

Додаткові запитання

1. Чи слід включати до моделі загроз загрози типу стихійних та

технологічних лих.

Так, загрози стихійних та технологічних лих слід включати до моделі загроз. Природні та технологічні загрози можуть суттєво пошкодити інформаційну систему, а саме вивести з ладу системи життєзабезпечення АС (електроживлення, заземлення та інші).

2. Стосовно якої інформації, яка обробляється в ІС, повинна будуватись

модель загроз: стосовно лише конфіденційної, чи стосовно відкритої

та конфіденційної?

На мою думку, модель загроз повинна будуватись стосовно конфіденційної та відкритої інформації, адже втрата обох типів інформації під час техногенної або природної загрози може завдати значної школи ІС.

3. Перелічіть основні класи загроз згідно моделі STRIDE.

Класи:

- *Spoofing*
- *Tampering*
- *Repudiation*
- *Information disclosure*
- *Denial of service*
- *Elevation of privilege*

4. Наведіть приклади мережних атак класу Spoofing та DenialOfService.

Приклади мережних атак класу Spoofing:

- *Ip-spoofing - вид хакерської атаки, що полягає у використанні чужого IP-адреси джерела з метою обману системи безпеки.*
- *Arp-spoofing - Вид хакерської атаки, що полягає у використанні чужого IP-адреси джерела з метою обману системи безпеки.*

Приклади мережних атак класу DenialOfService;

- *SYN-флуд - заснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через посилку SYN-пакету з неіснуючою зворотною адресою.*
- *UDP-флуд - заснований на нескінченній посилці UDP-пакетів на порти різних udp-сервісів.*
- *HTTP-флуд - заснований на нескінченному посиланні HTTP-повідомлень GET на 80-й порт із метою завантажити web-сервер настільки, щоб він виявився не в змозі обробляти всю решту запитів.*