НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)

“_____”_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

на тему: Моделювання та оцінка інформаційних ризиків за допомогою методології STRIDE.

Виконав (-ла): студент (-ка) 4-го курсу, групи ФБ-52
(шифр групи)

Юрчук Тарас Юрійович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник д. т. н. проф. каф. ІБ Архипов Олександр Євгенійович ____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.170101 «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

Юрчуку Тарасу Юрійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи:
«Моделювання та оцінка інформаційних ризиків за допомогою методології STRIDE» _____,
науковий керівник роботи:
проф. каф. ІБ д. т. н. Архипов Олександр Євгенійович_____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «27 травня» 2019 р. № 1414-с

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи: Методології моделювання та методи оцінки інформаційних ризиків

4. Зміст роботи: - Визначення поняття інформаційного ризику.

- Аналіз існуючих методів моделювання та оцінки ризиків.

- Створення власної моделі та оцінки ризиків для тестової мережі.

- Порівняння отриманої оцінки з експертною.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

- Презентація_____

6. Дата видачі завдання 17 вересня 2018 р._____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Вивчення літератури	17.09.18 – 12.12.18	
2	Написання літературного огляду	13.12.18 – 29.12.18	
3	Написання загального плану роботи	07.01.19 – 17.01.18	
4	Аналіз існуючих рішень	19.01.19 – 25.01.19	
5	Написання першого розділу диплому	01.02.19 – 01.03.19	
6	Написання другого розділу диплому	03.03.19 – 05.04.19	
7	Проходження переддипломної практики	20.04.19 – 20.05.19	
8	Написання третього розділу диплому	20.04.19 – 20.05.19	
9	Оформлення дипломної роботи	20.05.19 – 30.05.19	
10	Предзахист дипломної роботи	30.05.19	
11	Підготовка графічної частини	01.06.19 – 14.06.19	
12	Захист дипломної роботи	20.06.19	

Студент _____ Юрчук Т. Ю.
(підпис) (ініціали, прізвище)

Науковий керівник роботи _____ Архипов О. Є.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Обсяг роботи 50 сторінки, 9 ілюстрацій, 44 таблиці, немає додатків, 11 джерел літератури.

Об’єктом досліджень є інформаційний ризик.

Суб’єктом досліджень є модель та оцінка інформаційних ризиків.

Моделювання та оцінка інформаційних ризиків за допомогою методології STRIDE.

Ключові слова: Інформаційний ризик, модель інформаційного ризику, оцінка ризику, моделювання інформаційного ризику, ризик-орієнтована модель загроз, методологія STRIDE, єкспертна оцінка ризиків, модель DREAD.

ABSTRACT

The volume of work 50 pages, 9 illustrations, 44 tables, no attachments, 11 sources of literature.

The object of research is the information risk.

The subject of research is the model and assessment of information risks.

Modeling and assessing information risks using the STRIDE methodology.

Key words: information risk, information risk model, risk assessment, information risk modeling, risk-oriented threat model, STRIDE methodology, expert assessment of risks, model DREAD.

ЗМІСТ

Перелік умовних позначень, скорочень і термінів 8

Вступ 9

1 Поняття інформаційного ризику та оцінки ризику 11

1.1 Поняття інформації 11

1.2 Поняття інформаційної загрози 12

1.3 Інформаційна система та захист інформації 13

1.4 Інформаційний ризик 13

Висновки до розділу 1 14

2 Методи моделювання та оцінки інформаційних ризиків 15

2.1 Методології моделювання інформаційних ризиків 15

2.2 Програмне забезпечення для моделювання інформаційних ризиків .. 18

2.3 Методи оцінки інформаційних ризиків 20

2.4 Модель порушника 22

Висновки до розділу 2 23

3 Створення моделі загроз та оцінки ризиків тестової мережі 25

3.1 Модель загроз та оцінка ризиків для першого елемента діаграми 26

3.2 Модель загроз та оцінка ризиків для другого елемента діаграми 28

3.3 Модель загроз та оцінка ризиків для третього елемента діаграми 31

3.4 Модель загроз та оцінка ризиків для четвертого елемента діаграми .. 33

3.5 Модель загроз та оцінка ризиків для п'ятого елемента діаграми 36

3.6 Модель загроз та оцінка ризиків для шостого елемента діаграми 39

3.7 Модель загроз та оцінка ризиків для сьомого елемента діаграми 42

3.8 Модель загроз та оцінка ризиків для восьмого елемента діаграми 44

Висновки до розділу 3 48

Висновки..... 49

Перелік джерел посилань..... 51

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AV – Asset Value – якісна оцінка інформаційного ресурсу.

EF – Exposure factors – якісна оцінка вразливості ресурсу.

ARO – Annual Rate of Occurrence – можливість реалізації загрози.

ALE – Annual Loss Exposure – загальні можливі втрати.

ВСТУП

Актуальність роботи. Інформація в 20 та 21 столітті стала невід'ємною частиною людського життя. Інформація стала ресурсом, який має ціну таку ж як і матеріальні ресурси, наприклад: нафта, вугілля чи електроенергія. Френсіс Бекон ще в 17 столітті казав: «Інформація керує світом. Хто володіє інформацією, той може вирішувати долі народів». Тому на сьогоднішній день володіння інформацією пов'язане з ризиками її втратити. Інформаційні злочини стали дедалі частіше зустрічатись. Викрадення та продаж інформації в наш час є заробітком для великої кількості хакерів та злочинців. Тому появилась необхідність якісно захищати інформацію. Для побудови якісної та ефективної системи захисту інформації використовую різні методи та способи аналізу можливих місць її витоку.

Дану задачу виконують різні експерти, що можуть оцінити систему в якій зберігається інформація, ступінь її вразливості та цінність самої інформації, яка в ній зберігається. Тобто дані експерти оцінюють інформаційні ризики.

Для оцінки інформаційних ризиків також потрібно провести певну роботу. Скласти модель загроз, модель порушника, оцінити інформаційні ресурси та об'єднати всі ці данні для створення єдиної експертної думки щодо вразливості певного елемента системи. Це колосальна робота, адже деколи для оцінки великої системи в якій зберігається та циркулює інформація, наприклад внутрішня мережа великої компанії, може знадобитись не один тиждень роботи. А для підвищення якості такої оцінки потрібно, щоб її проводив не один і навіть не два експерти. Для великих корпоративних мереж може знадобитись ціла група експертів, яка буде складатись з десяти – п'ятнадцяти осіб. Навіть на підготовку такої кількості компетентних експертів потрібно багато ресурсів та часу.

В своїй роботі запропоновано спосіб оцінки ризиків за допомогою якого можна скоротити об'єм роботи виконуваної групою експертів та зменшити кількість експертів до одного. Навіть у великих мережах де об'єм роботи для оцінки може бути великим для однієї людини, кількість експертів сильно не

зросте, достатньо буде максимум три експерти. Якщо використовувати сучасні методології побудови ризик-орієнтованих моделей загроз та моделі оцінки інформації, що базуються на статистичних даних, а не на суб'єктивній думці експертів, можна максимізувати швидкість проведення експертизи з мінімальною затратою часу та людських ресурсів.

Мета досліджень. Показати на прикладі порівняння експертної оцінки та оцінки за допомогою методології STRIDE, що одна людина використовуючи сучасні методи та моделі може дати оцінку інформаційних ризиків, яка буде не гіршою ніж та , що була дана групою експертів.

Завданнями роботи.

1. Побудувати тестову мережу для оцінки ризиків.
2. Побудувати ризик-орієнтовану модель загроз для тестової мережі.
3. За даною моделлю загроз, оцінити ризики використовуючи модель DREAD.
4. Отримати експертну оцінку даних ризиків.
5. Порівняти результати двох оцінок.

Об'єкт досліджень. Інформаційний ризик.

Суб'єкт досліджень. Методи моделювання та оцінки ризиків.

Наукова новизна. На сьогоднішній день експертна оцінка використовується майже в усіх випадках коли необхідно провести оцінку ризиків на підприємстві. Ціль даної роботи показати, що можна зробити якісну оцінку ризиків з набагато меншими затратами людських ресурсів та часу.

Практичне значення. Проведення порівняння дозволяє наочно показати ефективність запропонованого методу. Отримані результати можна використати для подальшого розвитку нових методів оцінки на заміну старим.

1 ПОНЯТТЯ ІНФОРМАЦІЙНОГО РИЗИКУ ТА ОЦІНКИ РИЗИКУ

Для правильного розуміння поняття інформаційного ризику та оцінки інформаційного потрібно ввести поняття інформації, відкритої інформації та інформації з обмеженим доступом, інформаційної загрози, інформаційної системи, захист інформації та інші.

1.1 Поняття інформації

Інформація - це сукупність відомостей (даних), які сприймають із навколишнього середовища (вхідна інформація), видають у навколишнє середовище (вихідна інформація) або зберігають всередині певної системи. [1] Основними властивостями інформації є: конфіденційність (к), цілісність (ц), доступність (д).

Цілісність - неможливість модифікації інформації неавторизованим користувачем.

Конфіденційність - інформація не може бути отримана неавторизованим користувачем.

Доступність - полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.[2]

За змістом інформація поділяється на такі види:

1. інформація про фізичну особу;
2. інформація довідково-енциклопедичного характеру;
3. інформація про стан довкілля (екологічна інформація);
4. інформація про товар (роботу, послугу);
5. науково-технічна інформація;
6. податкова інформація;
7. правова інформація;
8. статистична інформація;

9. соціологічна інформація;
10. інші види інформації.

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. [1]

1.2 Поняття інформаційної загрози

Інформаційна загроза - це сукупність факторів, які створюють небезпеку для конституційних прав і свобод особистості, державної таємниці, зберігання цінної для суспільства інформації, від несанкціонованого доступу і розповсюдження.

Розглядаються зовнішні і внутрішні загрози ІБ, а також заходи і засоби протистояння і боротьба проти несанкціонованого доступу до інформації.

Зовнішні загрози:

1. інформаційному простору;
2. інформаційному суверенітету;
3. внутрішній стабільності;
4. діяльності державного або недержавного органів і фірм.

Внутрішні загрози:

1. національній безпеці;
2. для впливу на свідомість суспільства;
3. доступу до інформаційних ресурсів країни;[3]

Прямі збитки - поточна вартість витрат на відтворення, заміщення або відшкодування ринкової вартості об'єкта оцінки без урахування неотриманих майбутніх вигод. [4]

1.3 Інформаційна система та захист інформації

Інформаційна система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Сучасне розуміння інформаційної системи передбачає використання комп'ютера як основного технічного засобу обробки інформації. Комп'ютери, оснащені спеціалізованими програмними засобами, є технічної базою та інструментом інформаційної системи.

Виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації. [5]

1.4 Інформаційний ризик

Інформаційний ризик - це небезпека виникнення збитків або збитку в результаті застосування компанією інформаційних технологій. Іншими словами, інформаційні ризики пов'язані із створенням, передачею, зберіганням і використанням інформації за допомогою електронних носіїв і інших засобів зв'язку у інформаційній системі.[6]

Залишковий ризик - ризик, що залишається після оброблення ризику. Залишковий ризик є прийнятим ризиком організації. Ризики можуть бути

прийняті, якщо, наприклад, оцінено, що ризик є невеликим або вартість оброблення ризику є нерентабельною для організації.

Прийняття ризику - рішення прийняти ризик.

Аналізування ризику - систематичне використання інформації для ідентифікації джерел та кількісного оцінювання ризиків.

Оцінка ризику - загальний процес аналізування ризику та оцінювання ризику.

Оцінювання ризику - процес порівняння кількісно оціненого ризику із заданими критеріями ризику для встановлення його значимості.[4]

Висновки до розділу 1

Отже інформаційний ризик – це імовірність виникнення втрат в зв’язку з зловмисним або випадковим виводом з ладу елементів інформаційної системи або викрадення інформації з інформаційної системи.

Оцінка ризику – це визначення даної імовірності.

2 МЕТОДИ МОДЕЛЮВАННЯ ТА ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ

Основними способами знаходження вразливостей в системі є такі способи: статичний аналіз кожного елементу, перевірка шляхом створення фіктивних атак, отримання інформації про вразливості від розробника ПО або моделювання ризиків.

Саме моделювання ризиків дозволяє продумати методи захисту системи ще в процесі її проектування. Моделювання ризиків – це неперервний процес, який допомагає знаходити та зменшувати кількість загроз в вашіq системі шляхом прийняття певних дій.

Перевага моделювання інформаційних ризиків полягає в тому, що ми отримуємо розуміння реальних атак, чітко визначаємо зв’язок компонентів системи, отримуємо сценарії та ймовірності використання вразливостей та отримуємо розуміння впливу на систему проведення атаки.

На сьогоднішній день існує багато різних методологій для моделювання інформаційних ризиків. Основними є:

1. STRIDE
2. PASTA
3. Trike
4. VAST
5. OCTAVE

Коротко про кожен я розповім далі.

2.1 Методології моделювання інформаційних ризиків

2.1.1 STRIDE

Методологія STRIDE була розроблена та введена корпорацією Microsoft в 1999 році та використовується для опису та узагальнення ризиків по їх спільним характерним признакам, наприклад: ціль атаки, спосіб проведення атаки, вразливості, що використовуються для проведення атаки тощо, на продукти компанії Micrsoft.

Слово STRIDE – це абревіатура слів Spoofing, Tampering, Repudation, Information disclosure, DoS, Elevation of Privilege.(Таблиця 2.1)

Таблиця 2.1 – Розшифрування абревіатури STRIDE

Назва	Ціль атаки	Визначення
Spoofing	Автентифікація	Видання атакуючого за іншого користувача
Tampering	Цілісність	Модифікування або видалення інформації
Repudation	Аудит	Виконання шкідливих дій без загрози розкриття
Information Disclosure	Конфіденційність	Розкриття конфіденційних даних
DoS	Доступність	Пошкодження або видалення інформації
Elevation of Privilege	Авторизація	Викрадення або підміна даних користувача для отримання повноважень

2.1.2 PASTA

Процес моделювання атаки і аналізу загроз (PASTA) є відносно новою методологією моделювання загроз і являє собою семирівневу, орієнтовану на ризик методологію. Він забезпечує семи-етапний процес узгодження бізнес-цілей і технічних вимог з урахуванням аналізу впливу бізнесу і вимог. Мета

методу - забезпечити динамічну ідентифікацію загрози, підрахунок і процес підрахунку очок. Як тільки модель загрози буде завершена, експерти з питань безпеки розроблять детальний аналіз виявлених загроз. Ця методологія призначена для забезпечення орієнтованого погляду, з боку зловмисника, на систему і її інфраструктуру, з яких експерти з безпеки можуть розробити певну стратегію дії.

2.1.3 Trike

Ідея методології Trike у використанні моделі загроз як інструменту управління ризиками. Тут моделі загроз використовуються для забезпечення аудиту безпеки. Моделі загроз засновані на «моделі вимог». Модель вимог встановлює визначений зацікавленими сторонами «прийнятний» рівень ризику, присвоєний кожному класу активів. Аналіз моделі вимог дає модель загрози, з якою перераховуються загрози, і присвоюються значення ризику. Завершена модель загрози використовується для побудови моделі ризику, заснованої на активах, ролях, діях і розрахованої схильності до ризику.

2.1.4 VAST

VAST – це абревіатура від слів Visual, Agile і Simple Threat modeling. Основним принципом цієї методології є необхідність масштабування процесу моделювання загроз по всій інфраструктурі і її інтеграція в методологію розробки Agile. Методологія спрямована на забезпечення дієвих результатів для особливих потреб різних зацікавлених сторін: архітекторів застосунків і розробників, співробітників сфери захисту інформації і керівників вищої ланки. Методологія забезпечує схему візуалізації додатків та інфраструктури, так що створення і використання моделей загроз не вимагають спеціальних знань по предмету безпеки.

2.1.5 OCTAVE

OCTAVE – це також абревіатура від слів The Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology була однією з перших, створених спеціально для моделювання загроз кібербезпеки. Розроблена в Інституті програмного забезпечення Університету Карнегі-Меллона (SEI) у співпраці з CERT, методологія моделювання загроз OCTAVE зосереджена на оцінці організаційних (нетехнічних) ризиків, які можуть виникнути в результаті порушення даних. Використовуючи цю методологію моделювання загроз, ідентифікуються інформаційні активи організації, а на наборах даних вони містять атрибути прийому, засновані на типі даних, що зберігаються. Мета полягає в тому, щоб усунути плутанину щодо масштабів моделі загрози і зменшити надмірну документацію для активів, які або погано визначені, або знаходяться поза сферою дії системи. Хоча OCTAVE-моделювання загроз забезпечує надійне, орієнтоване на активи уявлення і організаційну обізнаність про ризики, документація може стати об'ємною. Цей метод найбільш корисний при створенні корпоративної системи захисту, орієнтованої на ризик. Цей метод дуже добре налаштовується для конкретних цілей безпеки і середовища ризику для організації.

2.2 Програмне забезпечення для моделювання інформаційних ризиків

Часто для виконання моделювання інформаційних ризиків використовують програмне забезпечення спрямоване на створення моделі системи та визначення вразливих місць. Найрозповсюдженішими такими програмами є:

- Microsoft threat modeling tool – безкоштовна програма що була створена корпорацією Microsoft для методології STRIDE, дозволяє створити діаграму потоків в системі та генерує детальний звіт в форматі html про всі можливі вразливості вашої системи.
- Mozilla threat modeling tool – безкоштовний онлайн застосунок від компанії Mozilla для моделювання інформаційних ризиків

- OWASP Threat Dragon - вільне, відкрите програмне забезпечення для онлайн-моделювання загроз, що включає системні діаграми та механізм автоматичного генерування загроз.
- MyAppSecurity - пропонує перший комерційно доступний засіб для моделювання загроз - ThreatModeler . Він використовує методологію VAST, на основі PFD і ідентифікує загрози на основі настроюваної всебічної бібліотеки загроз. Він призначений для спільного використання для всіх зацікавлених сторін організації.
- IriusRisk - пропонує як домашню, так і комерційну версію застосунку. Цей застосунок зосереджується на створенні та підтримці живої моделі загроз. Він керує процесом, використовуючи повністю настроювані анкети та бібліотеки шаблонів ризиків і з'єднує інші різні інструменти (OWASP ZAP, BDD-Security, Threadfix ...) для розширення можливостей автоматизації процесу моделювання ризиків.
- securiCAD - є інструментом моделювання загроз і управління ризиками скандинавської компанії foreseeti. Призначений для управління кібербезпекою компанії, від CISO, для інженерів з безпеки та технічного персоналу. securiCAD проводить автоматизовані симуляції атаки для поточних і майбутніх інформаційних архітектур, визначає та кількісно оцінює ризики, які цілісно включають структурні уразливості, і надає підтримку прийняття рішень на основі отриманих результатів. securiCAD пропонується в комерційних і домашніх виданнях.
- SD Elements by Security Compass - це платформа управління вимогами безпеки програмного забезпечення, яка включає автоматизовані можливості моделювання загроз. Набір загроз створюється шляхом заповнення короткої анкети про технічні деталі та драйвери програми. Контрзаходи зображені у вигляді завдань для розробників, які потрібно виконати для побудови захисту.[7]

2.3 Методи оцінки інформаційних ризиків

Для оцінки інформаційних ризиків використовують різні методи такі, як:

- Статистичний метод
- Метод експертного оцінювання
- Аналітичний метод
- Метод чутливості моделі
- Аналіз сценаріїв
- Метод аналога
- Аналіз доцільності витрат
- Метод імітаційного моделювання
- Метод моделювання Монте-Карло
- Рейтинговий метод
- Нормативний метод
- Дерево рішень
- Метод коригування норми дисконту[8]

В роботі були використані метод експертної оцінки та метод DREAD, що запропонований в методології STRIDE.

2.3.1 Метод експертної оцінки

Метод використовують для оцінки ризику при досліджені проблем, які виходять за межі формальних математичних поставок задач. Визначення ступеня ризику шляхом експертного оцінювання використовують за браку статистичної інформації в минулому періоді, або коли проводиться оцінка ризиків напряму підприємницької діяльності, що не має аналогів, а це, як правило, також не дає можливості аналізувати минулі показники. Експертне оцінювання вважається більш суб'єктивним, порівняно з іншими методами.

Основна ідея цього методу полягає у використанні інтелекту людей та їх здатності знаходити рішення слабо формалізованих задач.

Метод використовується у двох варіантах: метод "круглого столу" – припускає особисту зустріч експертів і метод заочного анкетування – виключає особисту зустріч експертів.

Методика проведення експертного оцінювання:

1) Формування мети оцінювання;
2) Постановка задачі;
3) Створення групи управління процесом оцінювання;
4) Опис форми отримання необхідних результатів;
5) Підбір експертів та визначення їх компетентності;
6) Складання анкет опитування;
7) Вибір методу отримання інформації;
8) Безпосереднє опитування експертів;
9) Обробка результатів і складання звіту для прийняття рішення.

Завдяки методу експертного оцінювання група експертів відокремлює складові комплексу ризиків, що піддаються управлінню, та робить висновки про ймовірність виникнення ризиків та ступінь їх впливу на діяльність фірми.

Переваги методу: можливість оцінки тих видів ризику, ймовірність генерації яких іншими методами оцінити неможливо; простота розрахунку.

Недоліки методу: здобуті результати носять суб'єктивний характер, що зумовлює відсутність гарантій вірогідності отримання незалежної експертної оцінки; невисока точність оцінки.[9]

2.3.2 Метод оцінки DREAD

DREAD є частиною системи для оцінки ризиків комп'ютерних загроз безпеки, які використовуються в компанії Microsoft, також в даний час вони використовуються OpenStack та іншими корпораціями, як частина методолгії моделювання інформаційних ризиків STRIDE, OWASP та інших. Він надає мнемоніку для оцінки ризику загрози безпеки за допомогою п'яти категорій.

Слово DREAD є абревіатурою від слів Damage potential, Reproducibility, Exploitability, Affected users, Discoverability. (Таблиця 2.2)

Таблиця 2.2 – Розшифрування абревіатури DREAD

Назва	Значення
Damage potential (DP)	Потенційна шкода - оціночний розмір нанесеної шкоди
Reproducibility (R)	Повторюваність - складність проведення повторної атаки
Exploitability (E)	Складність проведення першої атаки
Affected users (A)	Приблизна можлива кількість атакованих користувачів
Discoverability (D)	Відкритість - складність знаходження вразливості

Переваги методу: дозволяє використовувати не тільки суб’єктивну оцінку його складових, а також статистичні данні, точність оцінки знаходиться на досить високому рівні.

Недоліки методу: необхідна досить точна модель загроз та чітка цінність ресурсів.

2.4 Модель порушника

Модель порушника – це всебічна структурована характеристика порушника, яка використовується сумісно з моделлю загроз для розробки політики безпеки інформації. В Україні прийнята така структура моделі порушника:

Категорія осіб, до якої може належати порушник:

1) внутрішні порушники;
2) користувачі,
3) інженерний склад,
4) співробітники відділів, що супроводжують ПЗ,
5) технічний персонал, що обслуговує будинок,

6) співробітники служби безпеки,
7) керівники;
8) зовнішні порушники.

Мета порушника:

1) отримання необхідної інформації;
2) отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами;
3) нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Повноваження порушника в АС:

1) запуск фіксованого набору задач (програм);
2) створення і запуск власних програмних засобів;
3) керування функціонуванням і внесення змін у конфігурацію системи;
4) підключення чи зміна конфігурації апаратних засобів.

Технічна оснащеність порушника:

1) апаратні засоби;
2) програмні засоби;
3) спеціальні засоби.

Кваліфікація порушника:
для аналізу загроз завжди приймається висока кваліфікація.[10]

Висновки до розділу 2

Отже результатом аналізу можливих загроз є модель загроз– абстрактний структурований опис загроз.

Для моделювання ризиків можна використовувати безліч методологій та програм, що на них працюють. Для дипломної було обрано методологію STRIDE та програму Microsoft threat modeling tool яку досить легко освоїти

навіть початківцю в сфері інформаційної безпеки, а також дозволяє достатньо швидко та просто створити діаграму потоків вибраної мережі.

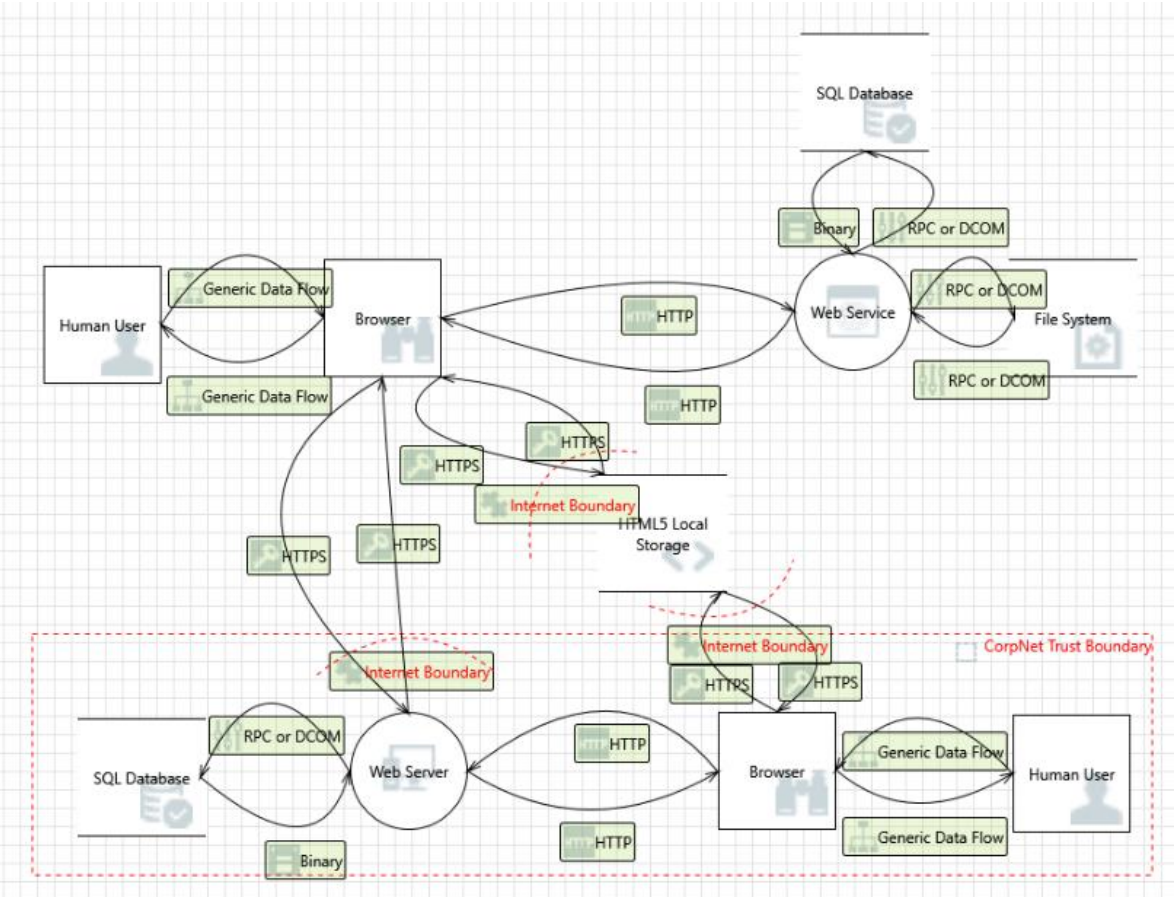
Для оцінки отриманих ризиків можна використовувати також велику кількість різних методів, як статистичних так і суб’єктивних. Кожен з них по своєму добре справляється з поставленою задачею, та я в роботі буде використано експертний метод оцінки, як самий розповсюджений на сьогоднішній день та модель DREAD, як ту що входить до методології STRIDE.

3 СТВОРЕННЯ МОДЕЛІ ТА ОЦІНКА РИЗИКІВ ТЕСТОВОЇ МЕРЕЖІ

Для початку виконання практичного завдання на практиці в компанії ТОВ «ISSP» мені було надано віртуальну мережу на віддаленому сервері, для якої я створював ризик-орієнтовані моделі загроз та оцінку існуючих ризиків. проводив оцінку інформаційних ризиків. Експертну оцінку ризиків для даної мережі мені надали співробітники компанії ТОВ «ISSP».

У програмі Microsoft Threat Modeling Tool я відтворив схему потоків для даної мережі і сформував звіт про інформаційні ризики даної системи (Рисунок 3.1).

Рисунок 3.1 – Діаграма потоків тестової мереж



В даній діаграмі потоків на кожному з’єднанні елементів виникають свої можливі ризики, для спрощення подання інформації я розділю ризики на різних елементах діаграми і опишу їх окремо.

3.1 Модель загроз та оцінка ризиків для першого елемента діаграми

Розглянемо перший елемент діаграми (Рисунок 3.2):

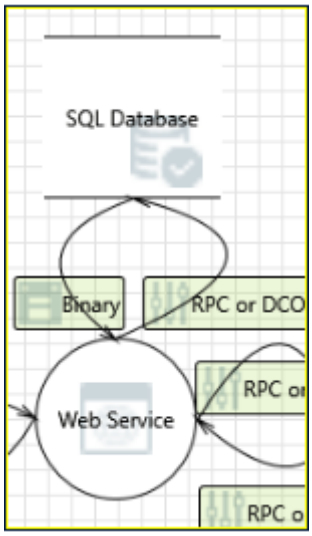


Рисунок 3.2 – З’єднання бази даних та веб сервісу

Таблиця ризик-орієнтованої моделі загроз для першого елемента (Таблиця 3.1)

Таблиця 3.1 – Ризик-орієнтована модель загроз для першого елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spoofing	Отримання доступу до трафіку між БД та Веб сервісом	Неконтрольований витік інформації	Прослуховування трафіку - К	Адмінстратор, технічний персонал, зовнішні або внутрішні користувачі
Information Disclosure	Отримання доступу до БД	Розсекречення інформації, що знаходиться в базі данних	Отримання, зміна або видалення секретної інформації - К, Ц і Д	Адмінстратор, розробник, зовнішні або внутрішні користувачі
Tampering	Проведення атаки типу SQL ін'єкція	Викрадення таємної інформації з БД	Отримання таємної інформації - К	Всі можливі порушники

Продовження таблиці 3.1

DoS	Відсутність балансування та фільтрації трафіку	Виведення з ладу БД	Унеможливлення коректної роботи системи - Д	Зовнішні та внутрішні користувачі

Таблиця експертної оцінки інформаційного ресурсу 1-го елемента (Таблиця 3.2)

Таблиця 3.2 – Експертна оцінка інформаційного ресурсу 1-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 1	2	2	2	1	2	2

Таблиця експертної оцінки вразливості 1-го елемента (Таблиця 3.3)

Таблиця 3.3 – Експертна оцінка вразливості 1-го елемента

Експертна оцінка вразливості (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	3	3	3	3	3
Information Disclosure	2	2	3	3	3	3
Tampering	3	2	3	2	3	3
DoS	3	3	3	3	3	3

Таблиця експертної оцінки можливості реалізації загроз для 1-го елемента (Таблиця 3.4)

Таблиця 3.4 – Експертна оцінка можливості реалізації загроз для 1-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	2	2	2

Продовження таблиці 3.4

Information Disclosure	2	1	1	1	1	1
Tampering	2	2	2	2	1	2
DoS	3	2	3	3	2	3

Таблиця оцінки ризиків першого елемента (Таблиця 3.5)

Таблиця 3.5 - Оцінка ризиків першого елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	3,2	Середня	3,5	Середня	2	середня	12	середня
Information Disclosure	4,8	середня	6,5	середня	1	низька	3	низька
Tampering	5,8	середня	6,5	середня	2	середня	8	висока
DoS	5,4	середня	9	висока	3	висока	12	середня

Дана таблиця (Таблиця 3.5) показує, що загалом оцінка за моделлю DREAD дає подібні результати з експертною оцінкою, в деяких випадках оцінка за моделлю DREAD надає ризикам більшого пріоритету ніж експертна, що може вплинути на побудову системи захисту і збільшити її ціну.

3.2Модель загроз та оцінка ризиків для другого елемента діаграми

Розглянемо другий елемент діаграми (Рисунок 3.3):

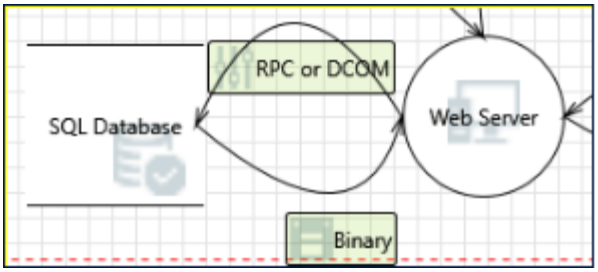


Рисунок 3.3 – З’єднання БД та Веб сервера

Таблиця ризик-орієнтованої моделі загроз для другогого елемента (Таблиця 3.6)

Таблиця 3.6 – Ризик-орієнтована модель загроз для другого елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spofing	Отримання доступу до трафіку між БД та Веб сервером	Перешкоджання коректного проходження трафіку між БД та Веб сервером	Прослуховування трафіку - К, перешкоджання трафіку - Д	Адмінстратор, зовнішні або внутрішні користувачі
Tampering	Веб сервер може бути ціллю для XSS атаки	Несанкціонований доступ до БД	Отримання доступу до трафіку між Веб сервером та БД	Зовнішні та внутрішні користувачі
Information Disclosure	Отримання доступу до БД	Розсекречення інформації, що знаходиться в базі данних	Отримання, зміна або видалення секретної інформації - К, Ц і Д	Адмінстратор, розробник, зовнішні або внутрішні користувачі
DoS	Відсутність балансування та фільтрації трафіку	Виведення з ладу БД	Унеможливлення коректної роботи системи - Д	Зовнішні та внутрішні користувачі

Таблиця експертної оцінки інформаційного ресурсу 2-го елемента (Таблиця 3.7)

Таблиця 3.7 – Експертна оцінка інформаційного ресурсу 2-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 2	2	1	2	2	2	2

Таблиця експертної оцінки вразливості 2-го елемента (Таблиця 3.8)

Таблиця 3.8 – Експертна оцінка вразливості 2-го елемента

Експертна оцінка вразливості ресурсу (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	1	1	1	1	1	1
Information Disclosure	2	1	1	1	1	1
Tampering	2	2	2	3	2	2
DoS	2	2	3	1	2	2

Таблиця експертної оцінки можливості реалізації загроз для 2-го елемента (Таблиця 3.9)

Таблиця 3.9 – Експертна оцінка можливості реалізації загроз для 2-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	2	2	2
Information Disclosure	2	1	1	1	1	1
Tampering	2	2	2	2	1	2
DoS	3	2	3	3	2	3

Таблиця оцінки ризиків другого елемента (Таблиця 3.10)

Таблиця 3.10 - Оцінка ризиків другого елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	4,8	середня	4	середня	2	середня	4	низька
Tampering	5,6	середня	7	висока	2	середня	4	низька
Information Disclosure	7,4	висока	9,5	висока	2	середня	8	середня
DoS	6	середня	8,5	висока	2	середня	8	середня

В даній таблиці (Таблиця 3.10) видно, що модель DREAD надає загрозам вищого пріоритету ніж експерти, це може бути пов’язано недоліками системи оцінювання експертної оцінки або недосвідченістю оцінюючого за моделлю DREAD (мене). Проте незважаючи на неспівпадіння модель DREAD показує непогані результати, адже вона не занижує ризик, що могло б призвести до компрометації системи.

3.3Модель загроз та оцінка ризиків для третього елемента діаграми

Розглянемо третій елемент діаграми (Рисунок 3.4):

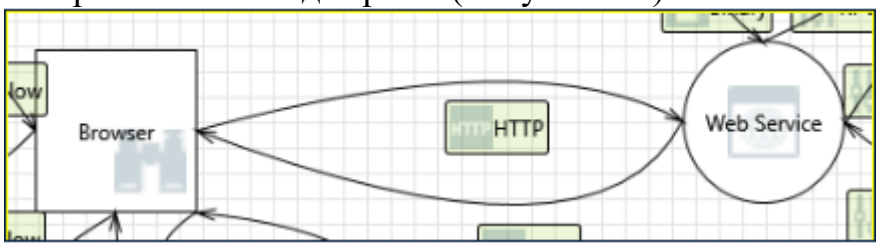


Рисунок 3.4 – З’єднання браузера та Веб сервісу

Таблиця ризик-орієнтованої моделі загроз для третього елемента (Таблиця 3.11)

Таблиця 3.11 – Ризик-орієнтована модель загроз для третього елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spoofing	Отримання доступу до трафіку між Браузером та Веб сервісом	Перешкоджання коректного проходження трафіку між Браузером та Веб сервісом	Прослуховування трафіку - К, перешкоджання трафіку - Д	Адмінстратор, зовнішні або внутрішні користувачі
Elevation of Privilege	Отримання додаткових привілеїв використовуючи підміну користувача	Отримання несанкціонованого доступу до веб сервісу	Отримання таємної інформації - К	Зовнішні користувачі, адміністратор, оператор

Таблиця експертної оцінки інформаційного ресурсу 3-го елемента (Таблиця 3.12)

Таблиця 3.12 – Експертна оцінка інформаційного ресурсу 3-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 3	3	1	2	2	2	2

Таблиця експертної оцінки вразливості 3-го елемента (Таблиця 3.13)

Таблиця 3.13 – Експертна оцінка вразливості 3-го елемента

Експертна оцінка вразливості ресурсу (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	2	2	2
Elevation of Privilege	2	3	1	2	2	2

Таблиця експертної оцінки можливості реалізації загроз для 3-го елемента (Таблиця 3.14)

Таблиця 3.14 – Експертна оцінка можливості реалізації загроз для 3-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	2	2	2
Elevation of Privilege	2	1	1	1	1	1

Таблиця оцінки ризиків третього елемента (Таблиця 3.15)

Таблиця 3.15 - Оцінка ризиків третього елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	4,4	середня	3	середня	2	середня	8	середня
Elevation of Privilege	3,6	середня	3	низька	1	низька	2	низька

З даної таблиці (Таблиця 3.15) можна побачити, що загалом модель DREAD та експертна оцінка дають майже однакові результати.

3.4Модель загроз та оцінка ризиків для четвертого елемента діаграми

Розглянемо четвертий елемент діаграми (Рисунок 3.5):

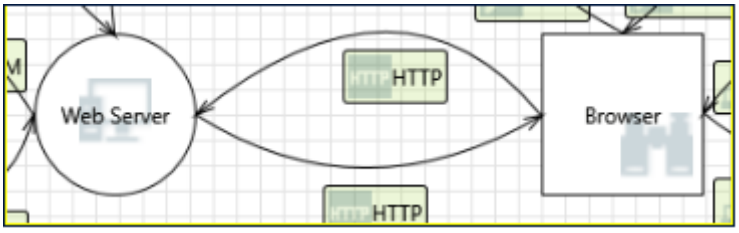


Рисунок 3.5 – З’єднання веб сервера та браузера

Таблиця ризик-орієнтованої моделі загроз для четвертого елемента (Таблиця 3.16)

Таблиця 3.16 – Ризик-орієнтована модель загроз для четвертого елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spoofing	Отримання доступу до трафіку між Браузером та Веб сервером	Перешкоджання коректного проходження трафіку між Браузером та Веб сервером	Прослуховування трафіку - К, перешкоджання трафіку - Д	Адмінстратор, зовнішні або внутрішні користувачі
Elevation of Privilege	Отримання додаткових привілеїв використовуючи підміну користувача	Отримання несанкціонованого доступу до веб серверу	Отримання таємної інформації - К, виведення з ладу серверу - Ц, Д	Зовнішні користувачі, адміністратор, оператор
Tampering	Проведення атаки типу XSS	Отримання особистої інформації користувачів (логінів, паролів)	Отримання повного доступу до інформації користувачів - К, Ц, Д	Зовнішні або внутрішні користувачі, розробник, абміністратор

Таблиця експертної оцінки інформаційного ресурсу 4-го елемента (Таблиця 3.17)

Таблиця 3.17 – Експертна оцінка інформаційного ресурсу 4-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 4	2	2	2	2	2	2

Таблиця експертної оцінки вразливості 4-го елемента (Таблиця 3.18)

Таблиця 3.18 – Експертна оцінка вразливості 4-го елемента

Експертна оцінка вразливості ресурсу (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	1	1	1	1	2	1

Продовження таблиці 3.18

Elevation of Privilege	2	2	1	2	2	2
Tampering	2	2	2	2	2	2

Таблиця експертної оцінки можливості реалізації загроз для 4-го елемента (Таблиця 3.19)

Таблиця 3.19 – Експертна оцінка можливості реалізації загроз для 4-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	1	1	1	1	2	1
Elevation of Privilege	2	2	2	3	2	2
Tampering	3	2	3	3	3	3

Таблиця оцінки ризиків четвертого елемента (Таблиця 3.20)

Таблиця 3.20 - Оцінка ризиків четвертого елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	4,2	середня	4	середня	2	середня	4	низька
Elevation of Privilege	4	середня	3,5	середня	2	середня	8	середня
Tampering	7	середня	8	висока	2	середня	12	середня

З даної таблиці (Таблиця 3.20) можна побачити, що загалом модель DREAD та Експертна оцінка дають однакові результати.

3.5Модель загроз та оцінка ризиків для п'ятого елемента діаграми

Розглянемо п’ятий елемент діаграми (Рисунок 3.6):

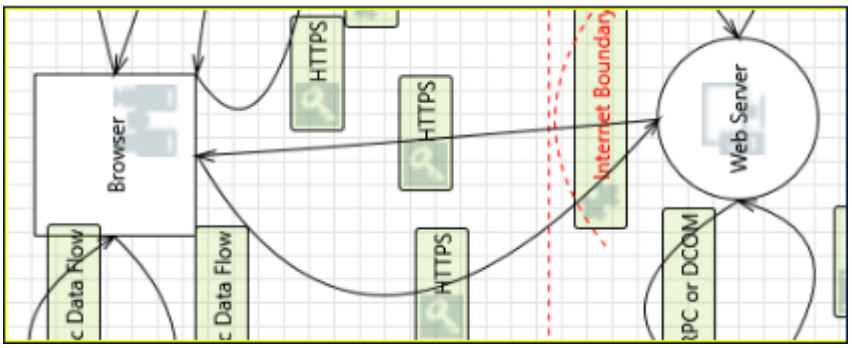


Рисунок 3.6 - З’єднання веб сервера та браузера, що виходить в мережу

Таблиця ризик-орієнтованої моделі загроз для п’ятого елемента (Таблиця 3.21)

Таблиця 3.21 – Ризик-орієнтована модель загроз для п’ятого елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spoofing	Отримання доступу до трафіку між Браузером та Веб сервером	Копіювання трафіку або отримання несанкціонованого доступу до Веб сервера зловмисником	Прослуховування трафіку - К, Отримання несанкціонованого доступу зловмисником - К, Ц, Д	Адміністратор, зовнішні або внутрішні користувачі
Elevation of Privilege	Виконання стороннього коду на стороні браузера	Отримання несанкціонованого доступу до веб серверу	Отримання таємної інформації - К, виведення з ладу серверу - Ц, Д	Зовнішні користувачі, адміністратор, оператор
Tampering	Проведення атаки типу XSS	Отримання особистої інформації користувачів (логінів, паролів)	Отримання повного доступу до інформації користувачів - К, Ц, Д	Зовнішні або внутрішні користувачі, розробник,

Продовження таблиці 3.21

				абміністратор
Repudation	Відсутність виявлення атак впродовж довгого часу в звязку довіреного з'єднання	Безконтрольна діяльність зловмисника	Отримання повного доступу до інформації користувачів - К, Ц, Д	Всі можливі порушники
DoS	Виведення з ладу Веб сервера	Унеможливлення нормальної роботи мережі	Виведення з ладу мережі - Д	Всі можливі порушники

Таблиця експертної оцінки інформаційного ресурсу 5-го елемента (Таблиця 3.22)

Таблиця 3.22 – Експертна оцінка інформаційного ресурсу 5-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 5	1	2	2	1	2	2

Таблиця експертної оцінки вразливості 5-го елемента (Таблиця 3.23)

Таблиця 3.23 – Експертна оцінка вразливості 5-го елемента

Експертна оцінка вразливості ресурсу (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	2	2	2
Elevation of Privilege	2	2	1	2	2	2
Tampering	3	2	2	2	2	2
Repudation	3	3	3	3	2	3
DoS	3	3	3	3	3	3

Таблиця експертної оцінки можливості реалізації загроз для 5-го елемента (Таблиця 3.24)

Таблиця 3.24 – Експертна оцінка можливості реалізації загроз для 5-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	2	2	2
Elevation of Privilege	1	1	1	2	1	1
Tampering	3	2	2	2	1	2
Repudation	2	2	2	2	2	2
DoS	3	2	3	3	2	3

Таблиця оцінки ризиків п’ятого елемента (Таблиця 3.25)

Таблиця 3.25 - Оцінка ризиків п’ятого елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	3,8	середня	4,5	середня	2	середня	8	середня
Elevation of Privilege	2,4	низька	3	низька	1	низька	4	низька
Tampering	5,2	середня	6	середня	2	середня	8	середня
Repudation	7,2	середня	8	висока	2	середня	12	середня
DoS	5,8	середня	9	висока	2	середня	18	висока

З даної таблиці (Таблиця 3.25) можна побачити, що загалом модель DREAD та експертна оцінка дають однакові результати.

3.6Модель загроз та оцінка ризиків для шостого елемента діаграми

Розглянемо шостий елемент діаграми (Рисунок 3.7):

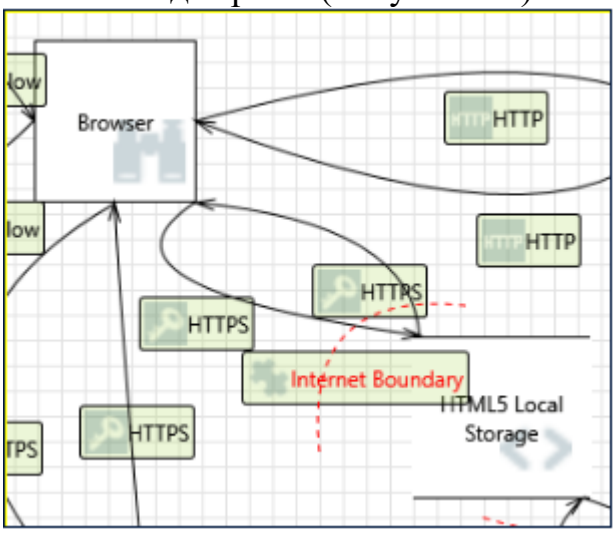


Рисунок 3.7 – З’єднання браузера та HTML5 local storage

Таблиця ризик-орієнтованої моделі загроз для шостого елемента (Таблиця 3.26)

Таблиця 3.26 - Ризик орієнтована модель загроз для шостого елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spoofing	Отримання доступу до трафіку між Браузером та БД	Копіювання трафіку зловмисником	Прослуховування трафіку - К	Адмінстратор, зовнішні або внутрішні користувачі, оператор, технічний персонал
Information disclosure	Слабкий захист інформації в HTML5 Local Storage	Отримання зловмисником таємної інформації	Отримання зловмисником таємної інформації - К	Всі можливі порушники
Tampering	Підміна трафіку між браузером та БД	Виведення з ладу БД	Унеможливлення нормальної роботи мережі - Д	Адміністратор, розробник
Repudation	Відсутність аудиту в HTML5 Local Storage в звязку довіреного з'єднання	Безконтрольна діяльність зловмисника	Отримання повного доступу до інформації в БД - К	Зовнішні або внутрішні користуваці
DoS	Зловмисник може отримати доступ до БД звязку довіреного з'єднання	Виведення з ладу БД	Унеможливлення нормальної роботи мережі - Д	Всі можливі порушники

Таблиця експертної оцінки інформаційного ресурсу 6-го елемента (Таблиця 3.27)

Таблиця 3.27 – Експертна оцінка інформаційного ресурсу 6-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 6	2	2	2	2	2	2

Таблиця експертної оцінки вразливості 6-го елемента (Таблиця 3.28)

Таблиця 3.28 – Експертна оцінка вразливості 6-го елемента

Експертна оцінка вразливості ресурсу (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	3	2	3	3	3	3
Information disclosure	3	3	1	3	3	3
Tampering	1	1	1	1	1	1
Repudation	1	1	1	1	2	1
DoS	3	3	3	3	3	3

Таблиця експертної оцінки можливості реалізації загроз для 6-го елемента (Таблиця 3.29)

Таблиця 3.29 – Експертна оцінка можливості реалізації загроз для 6-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	1	2	2	2	2
Information disclosure	1	1	1	2	1	1

Продовження таблиці 3.30

Tampering	2	1	2	2	2	2
Repudation	1	1	1	1	2	1
DoS	2	2	2	3	2	2

Таблиця оцінки ризиків шостого елемента (Таблиця 3.30)

Таблиця 3.30 - Оцінка ризиків шостого елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	4,2	середня	5	середня	2	середня	12	середня
Information disclosure	4,8	середня	7,5	середня	1	низька	6	низька
Tampering	5,6	середня	9	висока	2	середня	4	низька
Repudation	5	середня	4	середня	1	низька	2	низька
DoS	6,6	середня	9,5	висока	2	середня	12	середня

З даної таблиці (Таблиця 3.30) можна побачити, що знову ж таки навіть коли оцінки за моделлю DREAD та експертна відрізняються, оцінка за моделлю DREAD надає ризикам вищого пріоритету ніж експертна, що дає нам можливість побудувати надійну систему захисту, навіть якщо вона буде надлишковою.

3.7Модель загроз та оцінка ризиків для сьомого елемента діаграми

Розглянемо сьомий елемент діаграми (Рисунок 3.8):

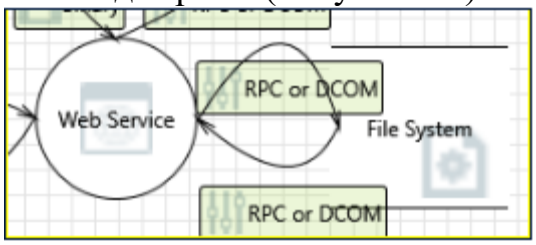


Рисунок 3.8 – З’єднання веб сервісу та файлової системи

Таблиця ризик-орієнтованої моделі загроз для сьомого елемента (Таблиця 3.31)

Таблиця 3.31 - Ризик орієнтована модель загроз для сьомого елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spoofing	Отримання доступу до трафіку між ОС та Веб сервісом	Неконтрольований витік інформації	Прослуховування трафіку - К	Адміністратор, технічний персонал, зовнішні або внутрішні користувачі
Information Disclosure	Слабкість систем шифрування	Розсекречення інформації	Отримання секретної інформації - К	Адміністратор, розробник, зовнішні або внутрішні користувачі
DoS	Відсутність балансування та фільтрації трафіку	Виведення з ладу ПК	Унеможливлення коректної роботи ПК користувача - Д	Зовнішні та внутрішні користувачі

Таблиця експертної оцінки інформаційного ресурсу 7-го елемента (Таблиця 3.32)

Таблиця 3.32 – Експертна оцінка інформаційного ресурсу 7-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 7	2	2	2	2	2	2

Таблиця експертної оцінки вразливості 7-го елемента (Таблиця 3.33)

Таблиця 3.33 – Експертна оцінка вразливості 7-го елемента

Експертна оцінка вразливості ресурсу (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	1	2	2

Продовження таблиці 3.33

Information disclosure	2	3	3	3	3	3
DoS	3	3	3	3	3	3

Таблиця експертної оцінки можливості реалізації загроз для 7-го елемента (Таблиця 3.34)

Таблиця 3.34 – Експертна оцінка можливості реалізації загроз для 7-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	2	2	2	2	2
Information disclosure	1	2	1	1	1	1
DoS	3	2	3	3	3	3

Таблиця оцінки ризиків сьомого елемента (Таблиця 3.35)

Таблиця 3.35 - Оцінка ризиків сьомого елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	5,4	середня	7,5	середня	2	середня	8	середня
Information disclosure	6,2	середня	8,5	висока	1	низька	6	низька
DoS	6,6	середня	7,5	середня	3	висока	18	висока

З даної таблиці (Таблиця 3.35) можна побачити, що знову ж таки навіть коли оцінки за моделлю DREAD та експертна відрізняються, оцінка за моделлю DREAD надає ризикам вищого пріоритету ніж експертна, що дає нам можливість побудувати надійну систему захисту, навіть якщо вона буде надлишковою.

3.8Модель загроз та оцінка ризиків для восьмого елемента діаграми

Розглянемо восьмий елемент діаграми (Рисунок 3.9):

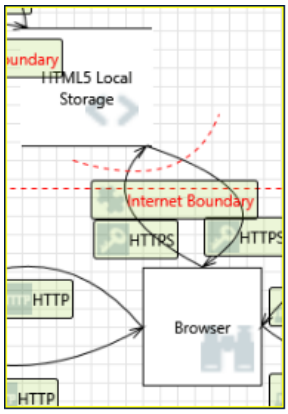


Рисунок 3.9 - З’єднання браузера та HTML5 local storage

Таблиця ризик-орієнтованої моделі загроз для восьмого елемента (Таблиця 3.36)

Таблиця 3.36 - Ризик орієнтована модель загроз для восьмого елемента

Ризик	Загроза	Наслідки	Мета (ресурс + порушення К, Ц, Д чи С)	Порушник
Spoofing	Отримання доступу до трафіку між Браузером та БД	Копіювання трафіку зловмисником	Прослуховування трафіку - К	Адмінстратор, зовнішні або внутрішні користувачі, оператор, технічний персонал
Information disclosure	Слабкий захист інформації в HTML5 Local Storage	Отримання зловмисником таємної інформації	Отримання зловмисником таємної інформації - К	Всі можливі порушники
Tampering	Підміна трафіку між браузером та БД	Виведення з ладу БД	Унеможливлення нормальної роботи мережі - Д	Адміністратор, розробник

Продовження таблиці 3.36

Repudation	Відсутність аудиту в HTML5 Local Storage в звязку довіреного з'єднання	Безконтрольна діяльність зловмисника	Отримання повного доступу до інформації в БД - К	Зовнішні або внутрішні користуваці
DoS	Зловмисник може отримати доступ до БД звязку довіреного з'єднання	Виведення з ладу БД	Унеможливлення нормальної роботи мережі - Д	Всі можливі порушники

Таблиця експертної оцінки інформаційного ресурсу 8-го елемента (Таблиця 3.37)

Таблиця 3.37 – Експертна оцінка інформаційного ресурсу 8-го елемента

Експертна оцінка інформаційного ресурсу (AV)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Ресурс 8	2	2	2	2	2	2

Таблиця експертної оцінки вразливості 8-го елемента (Таблиця 3.38)

Таблиця 3.38 – Експертна оцінка вразливості 8-го елемента

Експертна оцінка вразливості ресурсу (EF)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	3	2	3	3	3	3
Information disclosure	3	3	1	3	3	3
Tampering	1	1	1	1	1	1

Продовження таблиці 3.38

Repudation	1	1	2	1	1	1
DoS	3	3	3	3	3	3

Таблиця експертної оцінки можливості реалізації загроз для 8-го елемента (Таблиця 3.39)

Таблиця 3.39 – Експертна оцінка можливості реалізації загроз для 8-го елемента

Експертна оцінка можливості реалізації загрози (ARO)						
	Експерт 1	Експерт 2	Експерт 3	Експерт 4	Експерт 5	Оцінка
Spoofing	2	1	2	2	2	2
Information disclosure	1	1	1	2	1	1
Tampering	2	1	2	2	2	2
Repudation	2	2	2	2	2	2
DoS	2	2	2	3	2	2

Таблиця оцінки ризиків восьмого елемента (Таблиця 3.40)

Таблиця 3.40 - Оцінка ризиків восьмого елемента

Ризик	DREAD				Експертна			
	Оцінка ризика		Оцінка втрат		Оцінка ризика		Оцінка втрат	
Spoofing	6,8	середня	7,5	середня	3	висока	12	середня
Information disclosure	8	висока	7,5	середня	3	висока	12	середня
Tampering	4,6	середня	7,5	середня	2	середня	4	низька
Repudation	5,2	середня	3	низька	2	середня	4	низька
DoS	5,6	середня	8	середня	2	середня	12	середня

З даної таблиці (Таблиця 3.40) можна побачити, що загалом модель DREAD та Експертна оцінка дають однакові результат.

Висновки до розділу 3

Моделі ризиків створені за допомогою методології STRIDE були високо оцінені експертами з компанії ТОВ «ISSP» за їх точність та чіткість.

Щодо оцінки ризиків за допомогою моделі DREAD то вона майже скрізь співпала з експертною. Деякі розбіжності можна пояснити недосвідченістю або помилками в зборі статистичних даних.

Загалом в роботі вдалось продемонструвати, що оцінка за моделлю DREAD нічим не поступається експертній.

ВИСНОВКИ

Загалом моделювання ризиків за допомогою методології STRIDE значно полегшує роботу експерту адже дозволяє об’єднати подібні ризики в один клас та зменшити об’єми дослідження та оцінювання мережі. Щодо оцінки ризиків експертом та за моделлю DREAD в деяких випадках оцінка майже повністю співпадає, а в місцях де оцінки не співпадають, модель DREAD надає ризикам вищого пріоритету. Це дає нам розуміння, що можливо система захисту побудована на основі рекомендацій оцінки за моделлю DREAD буде надлишковою, проте вона буде надійною. Можливо, якби оцінку за моделлю DREAD проводив експерт, то результати були б набагато кращі. Також не можна не звернути увагу на об’єм роботи що доводиться виконувати при експертній оцінці. Експертам потрібно проводити однакові оцінки паралельно а потім порівнювати їх, на відміну від моделі DREAD, де всю роботу виконує лише один спеціаліст спираючись на статистичні данні. Також на розбіжності в якості оцінки сильно впливають формули по яким вона і проводиться та точність оцінювання. Нижче наведені формули розрахунку ризику та очікуваних витрат за моделлю DREAD (Таблиця 5.1) та експертом (Таблиця 5.2)

Таблиця 5.1 – Формули оцінки DREAD

DREAD		
Ризик	(DP + R + E + A + D)/5	0 - 10
Очікувані втрати	(DP + A)/2	0 - 10

Таблиця 5.2 – Формули оцінки експертної

Експертна оцінка		
Ризик	AV	1- низький, 2- середній, 3- високий
Очікувані втрати	AV*EF*ARO	1 - 6 низький, 7 - 13 середній, 14 - 27 високий

Ризик в моделі DREAD розраховується на основі даних про систему та її вузли, їх вразливості та атаки, що проводились на подібні системи раніше.

На відміну від експертної оцінки, де розрахунок ризику покладається на суб’єктивну думку експерта, що його оцінює.

Я вважаю, що експертна оцінка ризиків і досі залишається найкращим методом для вирішення даної задачі, проте в досить невеликих мережах, де об’єм роботи не буде перевищувати декількох днів, а необхідна кількість експертів для проведення якісної оцінки буде не високою (не більше 5). Для великих корпоративних внутрішніх мереж краще використовувати методологію STRIDE, адже вона дозволить зробити оцінку швидше і дешевше, а також не потрібно буде наймати «армію» експертів, які по завершенню оцінки будуть знати всю внутрішню архітектуру мережі і зможуть використати ці знання для нечесного заробітку.

Перелік джерел посилань

1. Поняття інформації. Про інформацію [Електронний ресурс] // zakon.rada.gov.ua. – 2017. – Режим доступу до ресурсу: https://
2. Поняття інформації. Види та властивості інформації. [Електронний ресурс] // ДПТНЗ. – 2012. – Режим доступу до ресурсу: https://gvpl.at.ua/publ/rizne/ponjattja_informaciji_vidi_ta_vlastivosti_informaciji/6-1-0-22.
3. Інформаційні загрози [Електронний ресурс] // StudFiles. – 2016. – Режим доступу до ресурсу: https://studfiles.net/preview/5649987/page:14/.
4. ISO/IEC 27001. // ГАЛУЗЕВИЙ СТАНДАРТ УКРАЇНИ. – 2010. – С. 2–4.
5. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] // Законодавство України. – 2014. – Режим доступу до ресурсу: https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
6. Інформаційні ризики [Електронний ресурс] // StudFiles. – 2016. – Режим доступу до ресурсу: https://studfiles.net/preview/5366708/page:4/.
7. ИТ РИСКИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. // Современные наукоемкие технологии. – 2014. – №7. – С. 183–185
8. Кисилева И. А. Информационные риски: методы оценки и анализа [Електронний ресурс] / Ирина Анатольевна Кисилева // Журнал "ITPortal". – 2017. – Режим доступу до ресурсу: https://cyberleninka.ru/article/v/informatsionnye-riski-metody-otsenki-i-analiza.
9. Герасимчук Н. А. Методи аналізу та моделювання ризику [Електронний ресурс] / Надія Андріївна Герасимчук // Навчальні матеріали онлайн. – 2015. – Режим доступу до ресурсу: https://pidruchniki.com/86196/ekonomika/metodi_analizu_modelyuvannya_riziku.

10. Поняття про модель загроз та модель порушника [Електронний ресурс] // StudFiles. – 2016. – Режим доступу до ресурсу: https://studfiles.net/preview/5992570/page
11. Понятие информационного риска [Електронний ресурс] // StudFiles. – 2016. – Режим доступу до ресурсу: https://studfiles.net/preview/5366710/page:2/.