Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Загнітка Костянтина Миколайовича

на здобуття ступеня вищої освіти Бакалавра

Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.200106.20.01.08 ПЗ

Виконав студент 4 курсу група КБ-20-1 Костянтин ЗАГНІТКО
Керівник доцент Віра ТІТОВА
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

12 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Загнітку Костянтину Миколайовичу

1 Тема роботи Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі

Керівник роботи Віра ТІТОВА

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 12.06.2024

3 Вихідні дані до роботи спроектувати та розробити інформаційно-аналітичну систему оцінки ризиків інформаційної безпеки комп'ютерної мережі, створити моделі інформаційної безпеки, визначити основні ризики, загрози, вразливості та необхідні заходи захисту інформації, оцінити ефективність розробленої системи

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз предметної області, огляд існуючих методів, обробка теоретичної інформації. Вибір і обґрунтування методів та засобів виявлення інформаційних загроз. Розробка моделей інформаційної безпеки. Створення системи оцінка ризиків та оцінка її ефективності. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
«Топологічна схема мережі», «Модель інформаційної безпеки веб-серверу», «Моделі інформаційної безпеки бази даних», «Модель інформаційної безпеки корпоративної електронної пошти», «Модель інформаційної безпеки облікових записів»

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	Виконано
Ознайомлення з предметною областю	Лютий	Виконано
Дослідження існуючих рішень	Лютий	Виконано
Постановка задачі	Березень	Виконано
Визначення загальних принципів рішення задачі	Березень	Виконано
Деталізація принципів рішення задачі	Квітень	Виконано
Розробка проєктних рішень	Квітень	Виконано
Апробація проєктних рішень	Травень	Виконано
Оформлення пояснювальної записки згідно вимог	Травень	Виконано
Оформлення графічної частини	Червень	Виконано
Захист КР	Червень	

Студент Костянтин ЗАГНІТКО

Керівник кваліфікаційної роботи Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі».

Автор роботи: Загнітко Костянтин Миколайович.

Керівник роботи: Тітова Віра Юріївна.

Пояснювальна записка: 76 сторінок, 1 додаток, 28 рис., 2 табл., 47 джерел.

Графічна частина: 5 презентаційних слайдів.

СИСТЕМА ОЦІНКИ РИЗИКІВ, МЕТОДИКА ОЦІНКИ РИЗИКІВ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМП'ЮТЕРНА МЕРЕЖА

Мета кваліфікаційної роботи полягає у створенні інформаційно-аналітичної системи оцінки ризиків інформаційної безпеки комп'ютерної мережі.

Для досягнення поставленої мети було досліджено предметну область, зібрано та проаналізовано теоретичну інформацію про існуючі методи оцінки ризиків у сфері інформаційних технологій. У процесі реалізації системи було створено набір методів та засобів для виявлення загроз, розроблено моделі інформаційної безпеки, на основі яких було створено інформаційно-аналітичну систему оцінки ризиків. Створену систему було апробовано і оцінено ефективність реалізованої методики.

28 травня 2024 р. Загнітко

ANNOTATION

Course project: Information-analytical system of information security risk assessment of a computer network.

Author of the work: Zahnitko Kostiantyn Mykolaiovych.

Supervisor: Titova Vira Yuriivna.

Amount: 76 pages, 1 appendix, 28 figures, 2 tables, 47 sources.

Graphic part: 5 presentation slides.

RISK ASSESSMENT, RISK ASSESSMENT METHODOLOGY, INFORMATION SECURITY, COMPUTER NETWORK.

The purpose of the qualification work is to create information and analytical system for assessing the risks of information security of a computer network.

To achieve this goal, the author researched the subject area, collected and analyzed theoretical information about existing methods of risk assessment in the area of information technology. In the process of system implementation, a set of methods and tools for detecting threats was created, and information security models were developed, on the basis of which an information-analytical system for risk assessment was created. The system was tested and the effectiveness of the implemented methodology was approbated and evaluated.

28 травня 2024р. Загнітко

ЗМІСТ

					КРБКБ.200106.20.01.08 ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розробив		Загнітко К.М.	Загнітко	10.06.24	Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі Пояснювальна записка	Літера	Аркуш 6 / Аркушів 76
Перевірив		Тітова В.Ю.		10.06.24		н	
Н.контр.		Мостовий С. В.		12.06.24		ХНУ, КБ-20-1	
Затвер.		Кльоц Ю. П.		12.06.24			

ВСТУП

По всьому світі відбувається стрімкий розвиток та впровадження інформаційних технологій, які вже стали невід'ємною частиною повсякденного життя. На даний час комп'ютерні мережі є основним засобом передачі даних і комунікації та відіграють ключову роль у різних сферах функціонування бізнесу та державних установ. Поєднання великої кількості пристроїв у локальні та глобальні мережі створює як переваги, так і нові загрози. Виникає необхідність надійного захисту основних властивостей інформації, що передається по мережі та зберігається на її вузлах.

Разом із зростанням кількості та складності інформаційних систем, та використовуваних у них технологій, виникає все більше інформаційних ризиків, пов'язаних із безпекою та надійністю використання цих мереж.

У таких умовах оцінка ризиків комп'ютерної мережі стає важливим етапом у процесах управління інформаційною безпекою та прийняття рішень. Цей процес є надзвичайно необхідним, оскільки своєчасна ідентифікація та оцінка ризиків дозволяє запобігти значним фінансовим втратам, забезпечити безперервність бізнес-процесів, захистити конфіденційність, цілісність та доступність інформації.

Проведення оцінки інформаційних ризиків мережі, дає ряд переваг: визначення адекватної суми витрат на захист інформації і коректний її розподіл, встановлення пріоритету заходів безпеки, визначення ключових активів, загроз та вразливостей, розуміння поточного стану захисту інформації та можливих наслідків для організації.

Метою моєї кваліфікаційної роботи є розробка інформаційно-аналітичної системи для оцінки ризиків комп'ютерної мережі, що дозволить покращити управління інформаційної безпеки для організацій.

1 ЗАСОБИ АНАЛІЗУ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття ризиків інформаційної безпеки

Ризик – це поєднання ймовірності виникнення загрози, ймовірності того, що використання загрози призведе до виникнення несприятливого впливу і тяжкості отриманого впливу[1].

Відповідно у сфері інформаційних технологій ризик інформаційної безпеки – це ризик для операцій організації (включаючи її призначення, функції, репутацію та імідж), її активів, певного кола осіб, інших організацій, пов’язаний із використанням інформаційних систем [2].

Також інформаційний ризик можна охарактеризувати як ймовірність виникнення збитків, неотримання доходу, додаткових витрат, що виникають через зовнішні або внутрішні події, хибні чи неадекватні внутрішні процеси, зміни стану інформаційного середовища, пов’язаний з використанням та функціонуванням інформаційних систем та їх управлінням або порушенням основних властивостей інформації [3].

Інформаційний ризик виникає при використанні інформаційних систем та технологій за допомогою яких інформація збирається, створюється, одержується, поширюється, використовується та інше за допомогою електронно-обчислювальної техніки, носіїв інформації, засобів зв’язку та програмного забезпечення.

Крім розуміння визначення інформаційного ризику необхідно розуміти і інші поняття безпосередньо пов’язані з ним. Ідентифікація ризику – це процес пошуку та опису ризику, що включає виявлення джерел ризику, небажаних подій, їх причин та можливих наслідків. Оцінювання ризику – це такий єдиний процес ідентифікації ризику, його аналізу і визначення величини цього ризику (в значеннях прийнятний або неприйнятний). Аналіз ризику – розуміння характеру ризику та рівня ризику. Прийняття ризику – обґрунтоване рішення

погодитися з ризиком у процесі його обробки чи без нього. Обробка ризику - процес, що має на меті зміну ризику [4].

1.2 Існуючі методи та алгоритми оцінювання ризиків інформаційної безпеки, їх порівняльний аналіз

Оцінювання ризиків інформаційної безпеки проводиться для виявлення загроз, з якими може зіткнутися досліджувана інформаційна система, її дані, мережеві зв'язки та обладнання, і для оцінювання потенційних наслідків, якщо відбудеться реалізація цих ризиків [5]. Проведення оцінки ризиків дозволяє організації та її керівництву зрозуміти, які активи є ключовими та становлять найбільший ризик [6]. Вибір чи формулювання конкретної методології оцінки ризиків є ключовою частиною управління інформаційною безпекою. Оцінка ризиків дозволяє керівництву організації встановити пріоритети усунення ризиків, терміновість їх усунення і скільки коштуватимуть зусилля з їх зменшення [7].

Більшість існуючих методів оцінки ризиків використовують математику, статистику і програмне забезпечення для аналізу інформаційних активів [8]. Відпрацьовані механізми оцінки ризиків інформаційної безпеки відіграють важливу роль у рутинній повсякденній діяльності осіб, які є відповідальними за прийняття рішень в управлінні інформаційною безпекою [9].

Існує величезна кількість методів оцінки ризиків інформаційної безпеки. Наявні методи можна умовно поділити на п'ять типів [10]:

- якісні;
- кількісні;
- на основі активів;
- на основі вразливостей;
- на основі загроз.

Якісна оцінка ризиків (англ. Qualitative risk assessment) базується на експертній думці. У якісних методах використовуються експертні судження для класифікації ризиків на основі імовірності і їх впливу [11].

Методологія якісної оцінки ризику безпеки виконується шляхом розмови з представниками різних відділів або підрозділів організації і запитань про те, як на їхні операції вплине та чи інша несприятлива подія (хакерська атака, злам, вихід із ладу обладнання, тощо). Такі співбесіди мають показати експерту, які частини інформаційної системи є критично важливими, а які ні [12]. У цьому методі для вираження судження створюється рейтингова шкала, що базується на шкалі низький-середній високий [13].

До основних переваг якісного аналізу ризиків необхідно віднести те, що цей тип аналізу [14]:

– дозволяє зосередитися на ризиках, що мають високий пріоритет;

– створює основу для подальшого більш поглибленого кількісного аналізу інформаційних ризиків;

– підходить для проектів та організацій будь-якого розміру, складності, стадії, життєвого циклу;

– гнучкий та швидкий.

Негативними сторонами якісного аналізу є, те що:

– досвід спеціалістів які будуть проводити оцінку вплине на результати;

– можлива невизначеність в результатах через абсолютні змінні.

Кількісна оцінка ризику (англ. Quantitative risk assessment) – це формальний, систематичний, статистичний метод оцінки ризику, що використовує об’єктивні дані, що можуть бути виміряні, для визначення вартості активу, імовірності збитку і інших пов’язаних ризиків [15].

Кількісний аналіз ризиків має такі переваги [16]:

– опис ризиків кількісно, використовуючи конкретні числа або діапазони, на відміну від якісних неоднозначних описових термінів, таких як «високий», «низький» і подібних;

– результат проведення аналізу досліджуваного об’єкту, чи вивід імітаційної моделі не є суб’єктивними, тому що не залежать від спеціаліста, що проводить аналіз;

– можливість відобразити ступінь складності мережі, що підлягає оцінюванню, розробка складної моделі відповідно до реальності, що точно передбачає результати;

– гнучкість моделі, що дозволяє досліджувати і аналізувати різні сценарії ризику та варіанти його усунення;

– забезпечення засобами дослідження спільного впливу ризиків.

Однак кількісна оцінка має і недоліки [16, 17]:

– аналітичні результати аналізу вимагають ретельної, кваліфікованої інтерпретації, що часто потребує розуміння статистичних принципів, інакше можливе неправильне тлумачення результатів;

– велика залежність від якості зібраних даних;

– результати можуть мати фальшиву точність через ряд даних зібраних для аналізу, особливо тих, які важко піддаються об’єктивному виміру;

– покладання на історичні дані, хоча стан справ щодо захисту інформації у сфері інформаційних технологій постійно змінюється;

– використання прогнозів або припущень замість надійних історичних або експериментальних наборів даних;

– небезпека хибної довіри, якщо результатам моделі приймаються без достатнього критичного осмислення;

– необхідність використання спеціалізованих програмних засобів, які можуть бути дуже дорогими, мати незручний функціонал, бути складними у використанні та інтеграції з існуючими інструментами організації;

– виникнення залежності від експерта, що проводить аналіз за допомогою спеціалізованих інструментів.

Іноді виділяють напівкількісну оцінку ризиків (англ. Semi-quantitative risk assessment) – це такий підхід до аналізу і оцінки ризиків, у якому поєднуються

якісні і кількісні елементи оцінки ризиків [18]. Частина аспектів оцінювання ризиків проводиться кількісними методами з використанням математики і статистики, решта – з використанням суджень експертів.

При використанні напівкількісних методів спеціалісти хочуть переконатися, що вони надають тлумачення того, як проводилися їхні розрахунки та були зроблені висновки, щоб уникнути неправильного тлумачення результатів [19].

Оцінка ризиків на основі активів (англ. Asset-Based risk assessment) традиційно використовуються в організаціях для оцінки інформаційних ризиків [6, 20]. Даний підхід є популярним, тому що легко узгоджується із структурою та діяльністю інформаційного відділу компанії. При оцінюванні ризиків на основі активів створюється реєстр активів компанії і далі відповідно для кожного активу визначається необхідний захист.

Організація, що використовує досягнення інформаційних технологій має такі типи матеріальних інформаційних активів:

– апаратні засоби: робочі станції, сервери різного призначення, мережеве обладнання;

– мережа організації;

– носії даних;

– інші фізичні активи.

Але значно більшу частину становлять нематеріальні активи:

– різноманітні бази даних;

– програмне забезпечення;

– знання працівників;

– інтелектуальна власність;

– авторські права;

– інші інформація, дані, тощо.

Підхід заснований на активах може допомогти організаціям, що мають виконувати жорсткі нормативні вимоги встановлені законом у певних сферах

діяльності, такі як фінанси чи медицина [21].

Оцінка ризиків на основі вразливостей (англ. Vulnerability-based risk assessment) передбачає оцінку ризиків шляхом виявлення високо-пріоритетних ризиків через пошук відомих слабких місць, вразливостей і потенційних загроз [22]. Під вразливістю необхідно розуміти слабку сторону інформаційної системи, що виникає через помилки в системі, непередбачену функціональність, неналежний захист або помилкові дії користувача, якими може скористатися зловмисник для здійснення успішної атаки [23]. Цей підхід до оцінки ризиків охоплює більше ризиків, ніж суто оцінка на основі активів, але оскільки базується на основі відомих вразливостей, може не охопити весь спектр загроз [6, 24].

Оцінка ризиків на основі загроз (англ. Threat-Based Risk Assessment) є популярним підходом через здатність визначати пріоритети і можливості спрощення автоматизації використовуючи каталоги відомих загроз, які можна поповнювати з відкритої інформації про кіберінциденти. Алгоритм оцінки ризиків на основі загроз має підтримуватися джерелами даних і моделлю даних, які орієнтовані на загрози. Поширені методології проведення оцінки ризиків такі, як STRIDE і OCTAVE засновані на загрозах [25].

Після огляду типів методології оцінки ризиків щодо використання інформаційних технологій, необхідно розглянути деякі відомі методи, які широко використовуються у сфері захисту інформації, а саме:

– STRIDE;
– OCTAVE;
– Rapid Risk Assessment;
– FAIR.

Методологія моделювання загроз STRIDE розробили у компанії Microsoft два інженери: Лорен Конфельдер і Преріт Гарг у 1999 році. Її призначення виявляти потенційні вразливості і можливі загрози для продуктів організації. STRIDE має мету гарантувати відповідність вимогам конфіденційності,

цілісності та доступності. Для відповідності викликам сучасності були створені розширені версії, такі як STRIDE-per-Element та STRIDE-per-Interaction [26].

Компанія Microsoft надає у відкритому доступі опис методики і її застосування [27, 28]. Назва методології була обрана для кращого мнемонічного запам’ятовування типів вразливостей. Перелічимо головні загрози згідно методології:

– spoofing – підробка особи, що відбувається коли зловмисник намагається видати себе за іншу особу;

– tampering – підробка даних, тобто інформація або дані, що змінюється без дозволу;

– repudiation – загроза відречення, коли зловмисник відмовляється визнавати свою причетність до зловмисних дій у системі;

– information disclosure – розкриття інформації, яке ще має назву витік інформації, відбувається при ненавмисному розкритті даним неавторизованим користувачам;

– denial of service – атака на відмову в обслуговуванні, яка робить недоступним користувачу доступ до ресурсів;

– elevation of privileges – підвищення привілеїв, через яке авторизований або неавторизований користувач може отримати доступ до інформації, яку він права переглядати не має.

Перевагами даної методології є:

– гнучкість і адаптивність структури методології, що дозволяє використовувати її у різноманітних випадках, для організацій різного розміру, у різних галузях;

– можливість розставити пріоритети у необхідному порядку і сфокусуватися на найважливішому ризику з точки зору ймовірної небезпеки або згідно особливостей галузі у якій працює організація;

– легкість розуміння і навчання працівників;

– поділ великої кількості загроз на шість зрозумілих розділів;

Але STRIDE має і недоліки:

– відсутність нетехнічних загроз, наприклад, соціальної інженерії, фішингу;

– суб'єктивність;

– необхідність постійного обслуговування і оновлення результатів оцінки методології для відображення змін у структурі, архітектурі, засобах інформаційної системи;

– витратність ресурсів для складних систем;

– більш орієнтований на розробку програмного забезпечення, тому гірше підходить для інших сфер.

OCTAVE (Operationally Critical Threat Asset, and Vulnerability Evaluation methodology) – це фреймворк для виявлення і управління ризиками інформаційної безпеки, що визначає комплексний метод оцінки, який дозволяє організації ідентифікувати її інформаційні активи, важливі для діяльності організації, загрози для даних активів, вразливості, що наражають активи на небезпеку. Поєднуючи активи, загрози та вразливості, організація починає розуміти, яка інформація є під загрозою і розробляти і реалізовувати власну стратегію захисту для зменшення ризику інформаційних активів [29]. Фреймворк у даному визначенні надається у значенні основної базової структури, набору основних елементів, правил, взаємозв'язків, які необхідні для опису і розуміння цілої системи чи концепції.

Методології OCTAVE були створені для Міністерства оборони США і показали свою ефективність. Зараз ця методологія є відкритою. Фреймворк став доступний з 1999 року, кілька разів оновлювався, були випущені версії для середніх та малих організацій [30].

Оригінальний метод був призначений для великих організацій:

– у яких понад 300 співробітників;

– у яких співробітники організовані в багаторівневу ієрархію;

– які мають власну інформаційну інфраструктуру і несуть

відповідальність за неї;

– які мають можливість запускати інструменти оцінки вразливостей;

– які можуть інтерпретувати результати оцінки ризиків.

OCTAVE було започатковано Університетом Карнегі-Мелона (США) і в подальшому розроблялася також Командою реагування на комп'ютерні надзвичайні ситуації Інституту розробки програмного забезпечення (CERT SEI).

У 2003 році було розроблено OCTAVE-S для невеликих організацій, у яких менше 100 співробітників, у яких гнучка ієрархія. У 2007 році було випущено OCTAVE Allegro – фреймворк, який призначений для всіх організацій, особливо для тих, що зосереджені насамперед на інформаційних активах. У цій версії були зменшено багато вимог, щоб зробити використання простішим.

У методі OCTAVE усе організовано на трьох основних аспектах, що дозволяє працівникам організації створити повну картину потреб організації у сфері управління інформаційною безпекою.

По-перше необхідно створити профілі загроз на основі активів, відбувається організаційна оцінка. Для цього команда, що проводить аналіз визначає важливі для організації інформаційні активи і вивчає, що на момент проведення дослідження робиться для захисту цих активів. Після цього активи знову переглядаються і обираються найбільш важливі активи для організації (критичні активи). Нарешті команда визначає загрози для кожного із критичних активів і створює профіль загроз для цього активу.

Другим етапом стає дослідження вразливостей інфраструктури. Наявні інформаційно-комп'ютерні системи оцінюються з точки зору захисту інформації, перевіряється мережа організації, тестується доступ до неї та її частин, кожен компонент перевіряється на стійкість до мережевих атак, вивчається, який компонент інформаційних технологій, пов'язаний з яким критичним активом.

На останньому третьому етапі розробляється план безпеки. Аналітична група, що проводила дослідження визначає ризики для критичних активів організації і приймає рішення, що з ними робити. На основі проведеного аналізу зібраних даних розробляється стратегія захисту інформації для організації і плани зменшення ризиків для критичних активів.

Швидка оцінка ризиків (англ. Rapid Risk Assessment) – це методологія швидкої оцінки ризиків, що допомагає формалізувати прийняття рішень за короткий проміжок часу. Процес є відтворюваним, послідовним з зрозумілими інформативними результатами. Рекомендується до використання компанією Mozilla в розділі документації щодо інформаційної безпеки [31] та організацією OWASP, що працює над підвищенням безпеки програмного забезпечення [32]. Метод є відкритим і має необхідну документацію [33]. Його метою є допомогти зрозуміти, як використовується оцінка і управління ризиками, та створити свою власну систему, коли офіційні стандарти є незручними або занадто складними для впровадження. Цей метод можна віднести до якісних.

Згідно цієї методики варто запускати першу швидку оцінку ризиків на етапі проектування нового елемента, хоча проводити і оновлювати її можна в будь-який час. Цим елементом може бути, що завгодно: нова програма, частина програми, інтеграція проекту з якимось інтернет сервісом, міграція на інший хостинг та інше. Рекомендується одразу записати прізвище відповідальної за цей елемент особи, створити діаграму потоку даних через цей елемент. Далі необхідно запросити відповідних людей на зустріч, зазвичай це мають бути працівники, які отримують вигоду від впровадження цього елементу, провідні інженери, які мають технічні знання та розуміються у захисті інформації, але в цілому не більше 5 осіб, інакше це сповільнить метод. У більшості випадків приймають участь дві особи. Спочатку необхідно обговорити ризики, а вже потім переходити до заходів безпеки. Також необхідно створити словник у якому перелічити усі види даних які будуть оброблятися чи зберігатися даним елементом. Далі обговорюються сценарії загроз і з’ясовується найгірший

сценарій. Результатом цього має бути визначений рівень впливу по шкалі від низького до максимального щодо фінансових проблем, проблем з репутацією, проблем з продуктивністю для малих груп працівників, проблем для усієї компанії чи користувацької бази.

FAIR або Факторний аналіз інформаційного ризику (англ. Factor analysis of information risk) – це кількісна модель аналізу інформаційного ризику, що дозволяє організаціям оцінити ризики характерні для їх інформаційного середовища. Дана модель створює математичну оцінку ризиків шляхом агрегування різних сценаріїв для кількісної оцінки потенційних збитків у грошовому еквіваленті [34].

Методику розроблено Інститутом Fair і було визнано Open Group, як міжнародний стандарт кількісної оцінки кіберризиків. На основі даної методики або запозичуючи в неї деякі елементи у світі розробляється багато власних методів оцінки ризиків, наприклад, вже розглянута швидка оцінка ризиків або [35].

Перевагами FAIR є:

– масштабованість;

– опублікований чіткий стандарт;

– надійна система класифікації загроз;

– можливість сконцентруватися, як на окремому ризику так і на поєднанні ризиків або цілих групах ризиків;

– можливість самостійно обирати пріоритети ризиків.

До недоліків відносяться:

– зорієнтованість на ймовірність реалізації загрози, а не на сам ризик;

– розробленість методу не як універсальний стандарт управління ризиками, а для розуміння взаємозв’язків ризиків організації;

– велика кількість специфічних даних, які необхідно зібрати для використанні у методі.

Частота і величина збитку в даному методі прив’язані до активу, тому

визначення вартості активу у цій методиці є ключовим. Визначаючи вартість необхідно врахувати такі збитки:

– продуктивності – недоотримання організацією доходів через нездатність надавати клієнтам товари чи послуги;

– реагування – будь-які ресурси, що були витрачені на реагування на ризик або загрозу після її виникнення для її усунення;

– заміни – трати спрямовані на заміну скомпрометованих активів;

– репутаційні – погіршення сприйняття бренду клієнтами, зниження рівня довіри акціонерами;

– конкурентної переваги – втрата частки ринку, втрачені витрати на досягнення конкурентної переваги, втрата інтелектуальної власності, частки ринку, інших можливостей;

– судові – витрати на судові процедури, штрафи та інше.

З точку зору даної методики загрози групуються на спільних ключових характеристик, виділяється, який вплив можуть вчиняти загрози щодо активу:

– доступ (access) – зчитування даних без належної авторизації;

– зловживання (misuse) – використовування активу без отримання прав або не за призначенням;

– розкриття (disclose) – загроза дозволяє отримати третім особам доступ до даних;

– модифікація (modify) – зміна даних або конфігурації активу;

– заборона доступу (deny access) – загроза не дозволяє законим користувачам отримати доступ до активу.

Такі дії по-різному впливають на різні активи. Наприклад, актив із конфіденційними даними може мати лише низький вплив на продуктивність у разі недоступності, але великий судовий, репутаційний і конкурентний вплив внаслідок розкриття.

Ризик розраховується по формулі, що має багато показників, такі як частота загрозливих подій, частота контактів, ймовірність дії, складність,

здатність до загроз, вразливість, вторинний ризик, первинну і вторинну величину втрати та інші.

1.3 Аналіз автоматизації оцінювання ризиків інформаційної безпеки

Автоматизація процесів оцінювання ризиків означає використання технологій та спеціалізованого програмного забезпечення, великих наборів даних, інших інструментів для оптимізації процесів виявлення та оцінювання ризиків. За допомогою ефективного аналізу та інтерпретації даних вдається виявляти закономірності, тенденції і потенційні ризики [36].

Розглянемо недоліки ручної оцінки ризиків [37]. Ручне оцінювання відбирає багато часу у працівників і є трудомістким процесом, тому може не встигати за темпом бізнесу, або за активністю інформаційних систем, що знаходяться під частими атаками у часи сплеску зловмисної активності. Людські помилки допущені при введенні даних або проведенні обчислень приведуть до неточних або повністю хибних результатів. Ручне оцінювання є погано масштабованим і не підходить взагалі для сучасних великих компаній і при роботі з великим об’ємами даних.

Автоматизація оцінювання ризиків усуває недоліки ручної оцінки і дає багато переваг [37, 38, 39]:

– зростання швидкості, ефективності, точності;

– автоматичний і централізований збір даних;

– статистика та моніторинг у режимі реального часу;

– масштабованість;

– інтеграція з різними корпоративними системами;

– широкі аналітичні можливості комплексного аналізу даних, їх візуалізація;

– автоматична планова підготовка звітності;

– пріоритезація ризиків;

– налаштування та адаптивність відповідно до потреб організації;

– економія коштів у довгостроковій перспективі.

Вважаю необхідним привести деякі приклади наявних на ринку програмних засобів оцінки ризиків.

Scrut Automation – хмарний засіб управління ризиками. Підтримує більше 75 інтеграцій з системами організацій, підтримує різні стандарти, такі як ISO 27001 або SOC 2, та вимоги GDPR, CCPA, HIPAA та інші, тому дозволяє компанії швидко почати роботу і в подальшому слідкувати над відповідністю цим стандартам та вимогам [40].

Компанія Logicgate – теж має схожі продукти (Cyber Risk, Controls Compliance, Enterrprise Risk Management), які можуть перевіряти діяльність інформаційних систем компанії на відповідність стандартам та вимогам законодавства, підтримує багато фреймворків, що становлять собою різні методи роботи над оцінюванням ризиків, має великий каталог загроз, надає супутні послуги такі як навчання працівників або розробка методики спеціально під організацію [41].

Microsoft Security Assessment Tool (MSAT) – це програмний засіб, що за результатами анкетування оцінює систему безпеки аналізуючи вплив процесів, технологій та людського фактору. Крім отриманих результатів надаються детальні рекомендації по зниженню загроз. Питання в анкеті і рекомендації ґрунтуються на стандартах ISO 17799 та NIST-800.x [42].

OpenRMF – веб-система автоматизації кібервідповідності з відповідним набором програмних засобів, що дозволяє ефективно управляти ризиками. На даний час існує дві версії продукту: безкоштовна OpenRMF OSS з відкритим вихідним кодом, призначена для малих проектів або невеликих окремих активів та платна комерційна OpenRMF Professional [43]. Перевагою даного продукту, що він поставляється не тільки за методом «програмне забезпечення, як послуга», але має гнучку систему ліцензування і дозволяється встановлювати

на свої сервери на власний розсуд. Запускати продукт можна навіть в автономній мережі без підключення до інтернету.

Privacy Engineering Collaboration Space – це відкритий для громадськості онлайн-простір, в якому зібрані безкоштовні інструменти для управління ризиками та наведено приклади їх використання [44]. Розробляється і підтримується організацією NIST на основі її стандартів [45].

1.4 Постановка задачі

Для будь-яких організацій, особливо для бізнесу, який швидко розвивається, управління ризиками стає одним із ключових аспектів досягнення організації. Відповідно до зростання ролі інформаційних технологій у діяльності організації, компанії, установи, тощо зростає і роль управління саме інформаційними ризиками. Проводячи автоматизацію процесів управління інформаційними ризиками компанії оптимізують рутині операції, вивільняють ресурси, підвищують точність прийняття рішень.

Основна мета проведення оцінювання ризиків – це надати особам, які приймають рішення, тобто керівництву організації розуміння вразливостей організації, що дозволить їм прийняти коректні рішення спрямовані на розробку і впровадження робочих стратегій із зменшення ризиків [37].

Керівництво організації бажає швидкості і точності для своєчасного і обґрунтованого прийняття рішень. Справжній стан справ у сфері інформаційно-комунікаційних технологій є невідомим для більшості людей, що не є спеціалістами даного напрямку.

Незважаючи на те, що існує велика кількість методів оцінювання ризиків, більшість із них не можуть повністю задовольнити потреби конкретної організації. Причин є безліч: застарілість методів, не врахування специфіки діяльності організації, теоретичність методів, зорієнтованість методів на один

конкретний аспект оцінювання ризиків і т.д.

Більшість програм для автоматизації крім недосконалості методів, що використовуються для оцінки ризиків, додають свої недоліки. Дуже мало засобів орієнтовані на ризики інформаційної безпеки, переважна кількість розроблялася для ризиків у інших сферах: медичній, економічній, логістичній і потім були перероблені і пристосовані для застосування у кіберзахисті.

Крім того проблемами залишаються незручний функціонал, висока вартість цих програмних засобів, незручні умови ліцензування, можливість використання тільки за умовою «програмне забезпечення, як послуга», що призводить до залежності від конкретного розробника, складність інтеграції з існуючими системами організації і тому подібне.

Метою розробки дипломного проекту є розробити інформаційно-аналітичну систему оцінки ризиків інформаційної безпеки комп'ютерної мережі.

Розробка власної інформаційно-аналітичної системи для оцінювання ризиків робиться для вироблення власного алгоритму і набору засобів, що будуть враховувати особливості побудови і роботи сучасних комп'ютерних мереж і нові загрози їх діяльності. Нова модель має усунути недоліки існуючих методів і покращити якість оцінювання ризиків через врахування специфіки діяльності існуючих мереж інформаційно-комунікаційних технологій та особливостей їх проектування, архітектури. Інформаційно-аналітичний метод, що правильно визначає та оцінює активи, має грамотно класифікований та повний набір загроз, їх джерел та вразливостей, методику оцінки ймовірності реалізації загрози, неодмінно покращить якість оцінки ризиків.

2 МОДЕЛІ ТА МЕТОДИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Методи та засоби виявлення інформаційних загроз в комп'ютерних мережах

З розвитком інтернет-технологій, зросли розміри мереж, кількість вузлів, що задіяні у них, архітектурна і технічна складність цих мереж. Це вимагає створення багаторівневої моделі для побудови моделі виявлення загроз, щоб досягти покращення захисту інформаційної безпеки мережі.

Щоб виявити проблеми безпеки мережі та наявні загрози, необхідно мати повний класифікатор загроз інформаційної безпеки та необхідне програмне забезпечення для тестування та дослідження мережі та її вузлів.

Виявлення інформаційних загроз, вразливостей, через які загрози можуть реалізуватися та подальша оцінка ризиків є процесами оцінки інформаційної безпеки. У системі будуть використовуватися основні типи методів оцінювання загроз для активів:

– тестування;

– експертиза;

– інтерв'ювання.

Під час тестування за допомогою спеціально обраних інструментів порівнюється фактична та очікувана поведінка одного, декількох або ряду об'єктів оцінювання.

Експертизу можна охарактеризувати, як процес перевірки, огляду, інспекції, вивчення, інспекції об'єктів оцінювання. Наприклад, перегляд існуючої документації визначає чи встановлені політики і процедури є актуальними і комплексними.

Інтерв'ювання передбачає проведення дискусій, опитування, відповідних осіб або груп у організації, для якої проводиться оцінка ризиків, з метою кращого розуміння, отримання необхідних роз'яснень.

Оскільки будь-яка методика виявлення вразливостей вимагає ресурси, такі як: час, персонал, програмне забезпечення, обладнання, доступ к активам, то постає задача отримати достатньо ефективну, швидку та мало затратну по відношенню до ресурсів методологію.

Розробка задокументованої, легко відтворюваної методики пошуку вразливостей для спеціаліста, що проводить оцінювання ризиків дає ряд переваг:

– наявність чіткої структури та послідовності;
– мінімізація виникнення помилок у пошуку вразливостей;
– легкість дотримання;
– зрозумілість, поділ на етапи;
– врахування ресурсних обмежень;
– прискорення адаптації нового персоналу до даної методології;
– зниження необхідного на виконання робочого часу та інших витрат.

Існує велика кількість методів тестування та експертизи, які можуть використовуватися, але у даній системі будуть застосовуватися види, що можна згрупувати в такі категорії:

– методи ідентифікації та аналізу об’єктів;
– методи перевірки вразливостей;
– методи огляду.

Методи ідентифікації та аналізу використовуються для загального дослідження структури, архітектури мережі, наявних вузлів, підключених сторонніх мереж, визначення відкритих портів, а відповідно і запущених мережевих служб та сервісів, їх призначення. Немає жодної необхідності виконувати усі дії вручну, тому у моїй системі рекомендується для даної мети використовувати nmap.

Nmap Network Scanner – є популярною безкоштовною утилітою з відкритим вихідним кодом, що використовується багатьма спеціалістами з інформаційної безпеки та системними адміністраторами для виявлення хостів у

мережі і запущених служб шляхом аналізу відповідей на надісланні пакети [46, 47]. Наразі є кросплатформеним застосунком.

Він знадобиться нам для:

– інвентаризації мережі;

– виявлення відкритих портів на вузлах;

– аудиту безпеки фаєрвола;

– інших цілей, наприклад, виконання деяких скриптів середовища NSE.

Розглянемо приклади використання цієї утиліти для пошуку вразливостей. На рисунку 2.1 можна побачити приклад роботи з Nmap. З виводу програми розуміємо, що субдомену відповідає один ip-адрес, даний хост працює і на ньому запущені веб-сервер, служба віддаленого доступу, інструмент генерації мережевих пакетів nping та ще один відкритий порт, який можливо використовується шпигунським програмним забезпеченням.

```
┌──(user㉿kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-05 19:59 EEST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 12.77 seconds
```

Рисунок 2.1 – Сканування портів з Nmap

Одночасно із скануванням відкритих портів можна визначити операційну систему встановлену на об’єкті, конкретне програмне забезпечення і його версію, як показано на рисунку 2.2.

Середовище скриптів NSE надає широкі можливості для пошуку вразливостей, тестування а проникнення, отримання переліків ресурсів мережі.

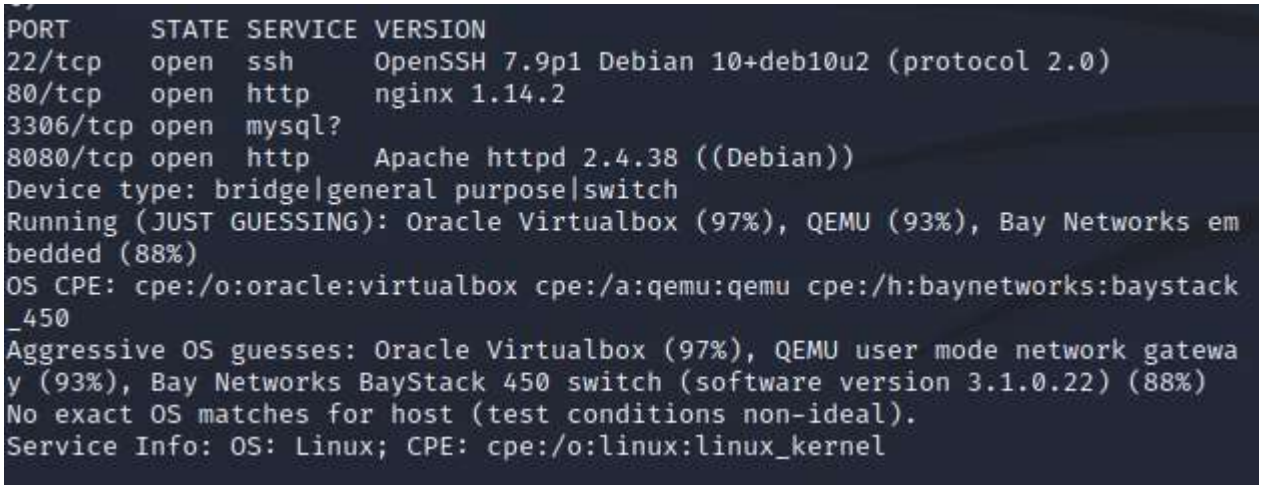


Рисунок 2.2 – Визначення встановленої операційної системи та версій програм за допомогою Nmap

На рисунку 2.3 показано дію скрипту для визначення методі автентифікації протоколу SSH, застарілі протоколи недоступні, віддалений доступ можливий лише за допомогою паролю чи ключа.

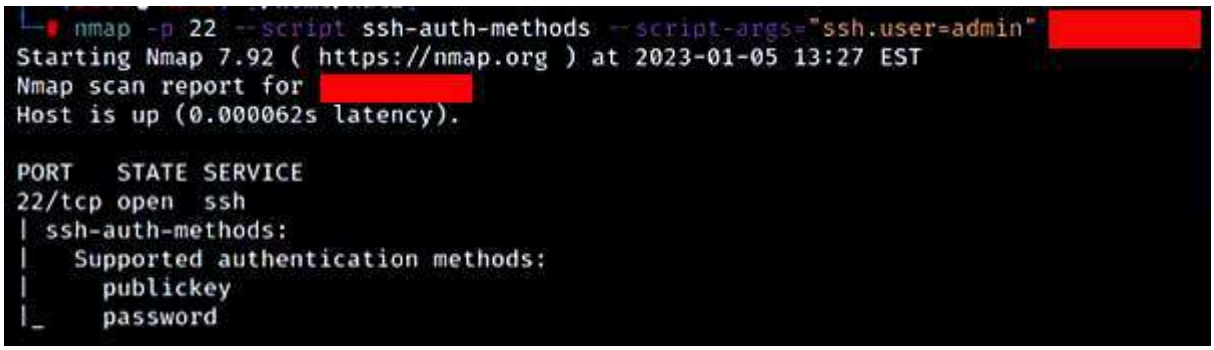


Рисунок 2.3 – Визначення методів авторизації SSH

Яскравим прикладом автоматичної ідентифікації об’єктів, буде сканування веб-серверу для пошуку усіх доступних сторінок і каталогів. Важливо переконатися, що на веб-сервері не зберігається інформація, для зберігання якої він не призначений. Така перевірка необхідна, щоб не стався витік інформації.

З цією метою варто використовувати OWASP DirBuster – безкоштовна багатопотокова програма призначена для пошуку каталогів та імен файлів веб-

серверу. Відрізняється від аналогів простотою у використанні, ефективністю пошуку, 9-ма коректно складеними сучасними словниками, що встановлюються разом із програмою.

Пошук усіх сторінок веб-серверу продемонстровано на рисунку 2.4. Можна зробити висновок, що це нещодавно встановлений сервер із стандартним базовим набором сторінок.

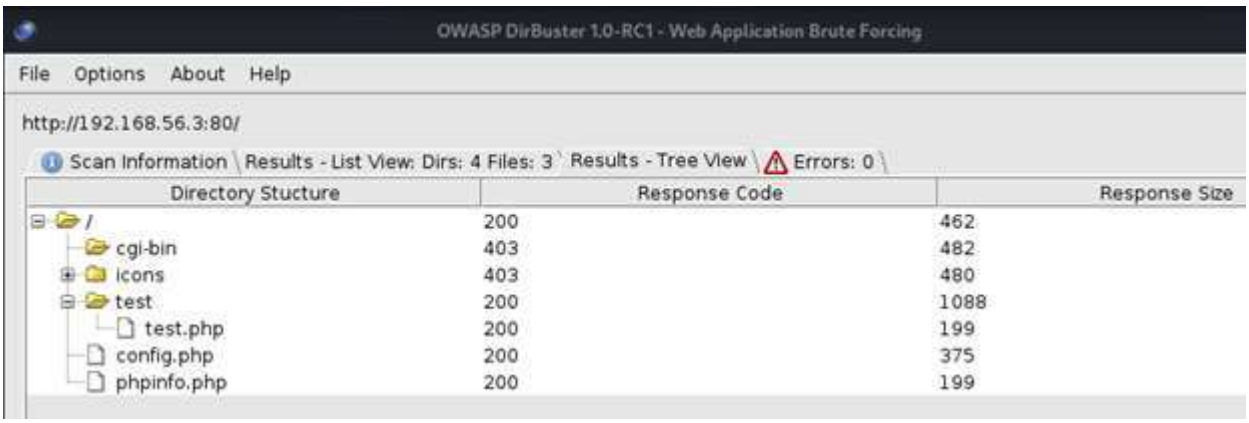


Рисунок 2.4 – Пошук сторінок і каталогів веб-серверу

Веб-сервер – це комплекс програмного та апаратного забезпечення, що працює за клієнт-серверною архітектурою для зберігання, генерації і доставки веб-контенту користувачам по мережі.

Наразі підприємства та інші організації широко використовують велику кількість різноманітних веб-серверів для задоволення своїх потреб, тому їх оцінці вразливостей необхідно приділяти відповідну увагу.

Присутність веб-сайту компанії в інтернеті дозволяє рекламувати себе і надавати інформацію про продукти. Веб-сайти наразі часто становляться веб-додатками – повноцінним програмним забезпеченням, яке може використовуватися клієнтами організації, підрядниками або працівниками. Зберігання і обробка даних на них стає все більш складною, і постійно відбувається впровадження нових технологій : розміщення у хмарі, віртуалізація та контейнеризація.

Тому для спрощення веб-розробки більшість організацій почали використовувати системи керування контентом (CMS). Цей інструмент керування цифровим і веб-контентом складається з двох основних складових: програми керування вмістом (CMA), тобто інтерфейс призначений для користувача, що дає можливість виконувати дії над наповненням сайту без втручання веб-розробника; і програми доставки вмісту (CDA), що відповідає за роботу сайту.

Результати збору інформації про сайт під системою керування контентом WordPress за допомогою утиліти Cmseek показані на рисунку 2.5.

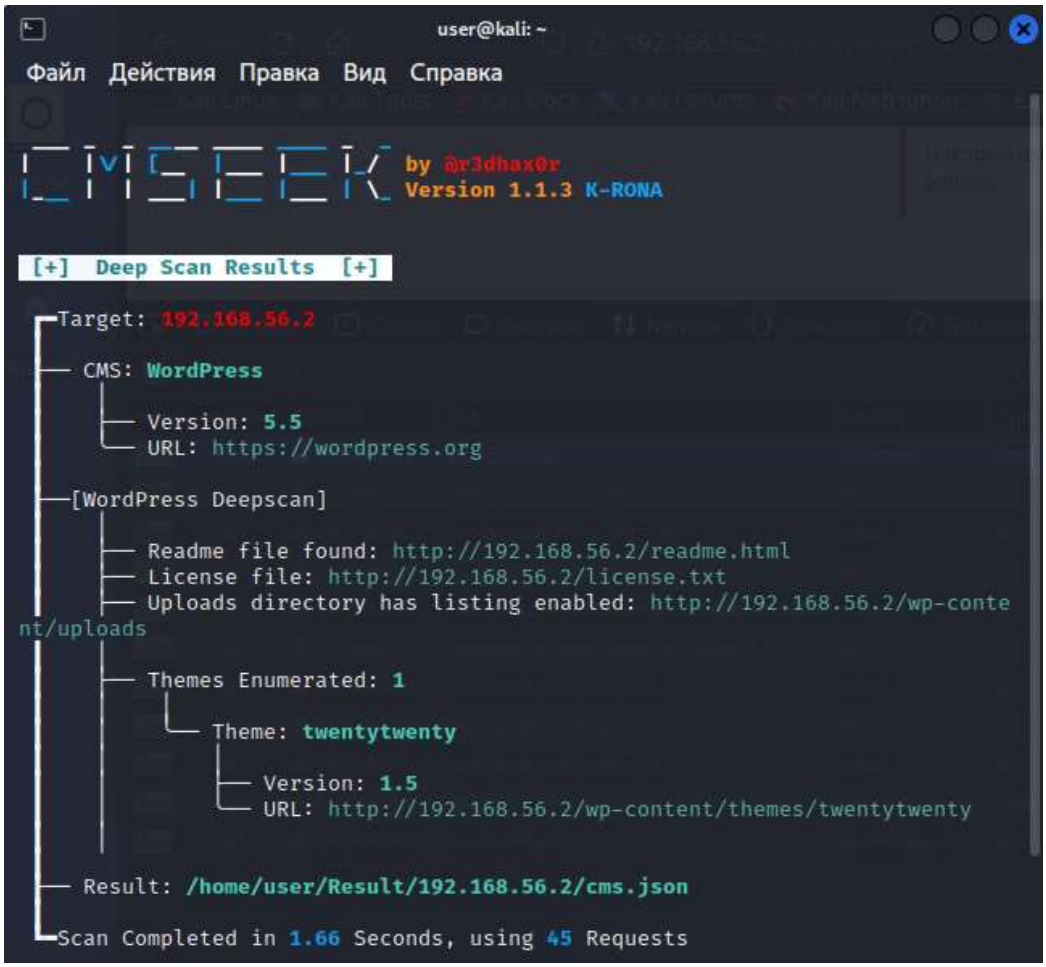


Рисунок 2.5 – Збір інформації про сайт під управлінням CMS

Із встановленням CMS виникають проблеми: застарілість версій, відомі вразливості для ряду систем, необхідність встановлення спеціальних засобів

захисту, повільність у роботі, проблеми сумісності.

Для отримання уявлення про те, який трафік рухається по мережі організації, для його подальшого аналізу на можливі аномалії або небезпечні ознаки слід використати сніфер WireShark. Це потужний, безкоштовний, кросплатформний аналізатор пакетів із графічним інтерфейсом та відкритим вихідним кодом.

Зразок дослідження одного кадру із відфільтрованої частини трафіку зображено на рисунку 2.6.

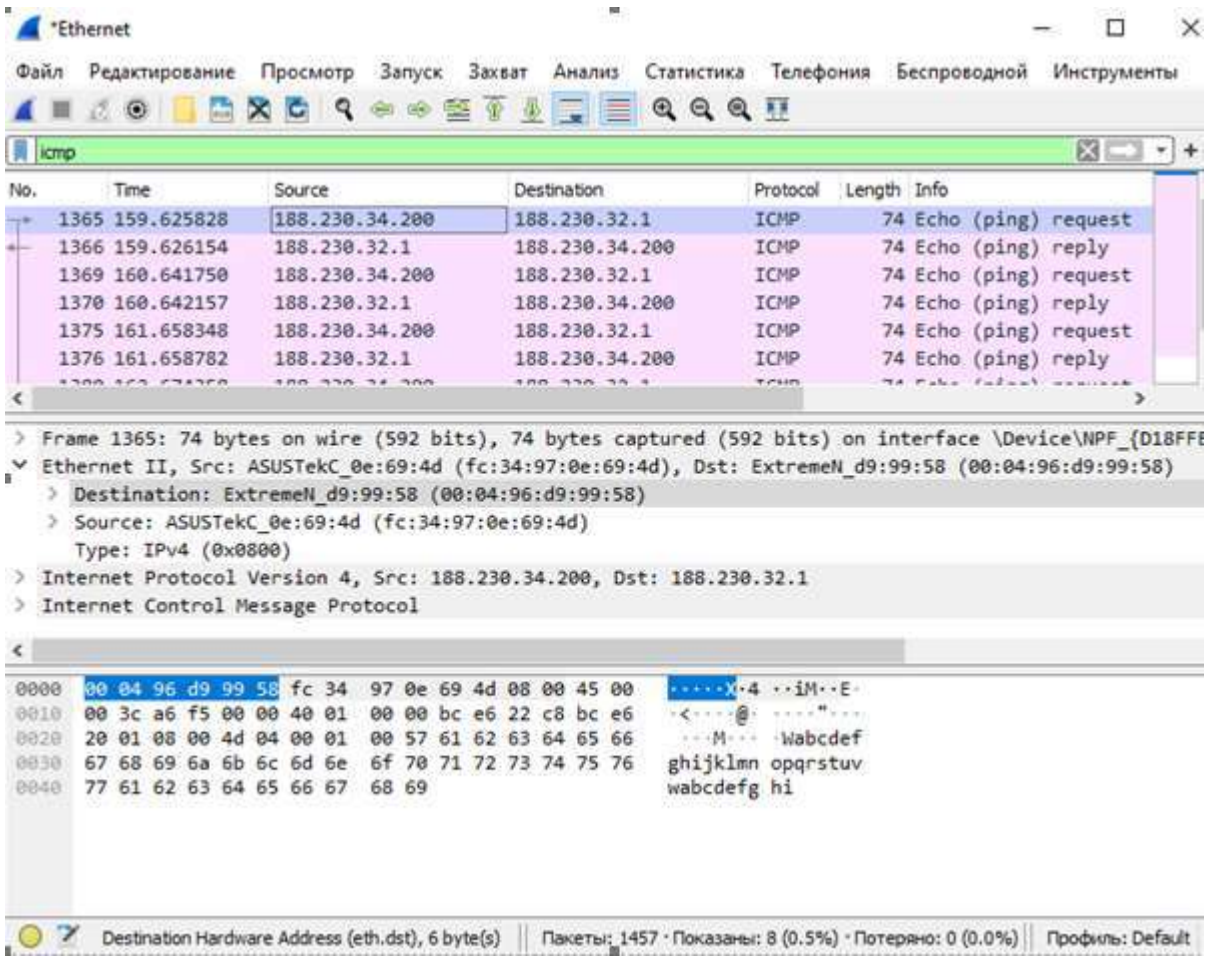


Рисунок 2.6 – Дослідження трафіку програмою WireShark

Розглянувши методи ідентифікації та аналізу, перейдемо до методів перевірки вразливостей об’єктів. Вони використовуються для перевірки існування чи відсутності конкретних вразливостей.

У цій системі буде випробовуватися:

– SQL-ін’єкція;

– злам паролів;

– тестування безпеки додатків.

Бази даних у більшості випадків є найціннішим активом організації, тому вимагають найретельнішого захисту. Дані, що зберігаються у базах можуть бути найрізноманітнішими: дані клієнтів, дані про продукти та послуги, бухгалтерські дані компанії, дані працівників, аналітичні дані, документація, історія транзакцій та інше. Бази даних зазвичай знаходяться на окремо призначених для них серверах, що називаються серверами бази даних. Інші служби, наприклад, веб-додатки отримують більшість інформації звертаючись через api до баз даних.

Одна з найчастіших загроз в інтернеті та найпоширенішою загрозою для баз даних є SQL-ін’єкція, принцип якої полягає в тому, що зловмисник вводить в параметри запиту спеціально сформовані рядки, що призведуть до розкриття інформації із бази даних.

Використаймо sqlmap – інструмент призначений для тестування на проникнення, що автоматизує процес виявлення та використання вразливостей SQL-ін’єкцій. Є безкоштовним, з відкритим вихідним кодом, з потужним механізмом виявлення загроз, широким набором налаштувань та багатьма іншими спеціальними функціями. Повністю підтримує більшість сучасних систем управління базами даних: MySQL, Microsoft SQL Server, PostreSQL, SQLite, Maria DB та інші.

На рисунку 2.7 показано процес тестування на вразливість до SQL-ін’єкцій програмою sqlmap. В даному випадку засіб сам визначає що поле не вразливе до error based injections і відбувається автоматичний вибір іншого методу - time-based blind injections. Далі починається процес посимвольного витягування усіх даних таблиці: назв таблиць, назв стовпців і усіх рядків.

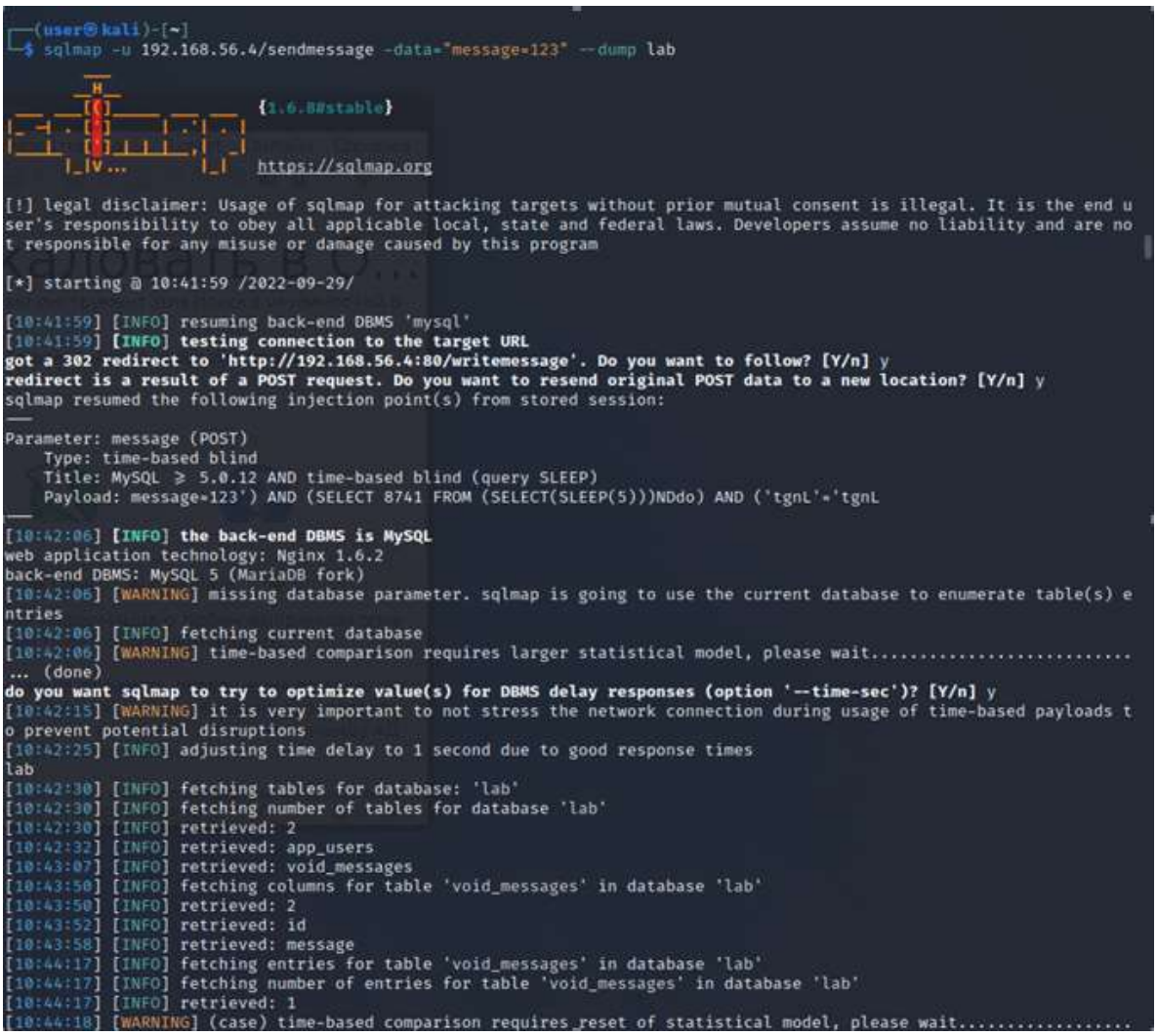


Рисунок 2.7 – Тестування вразливості до SQl-ін’єкцій

Як вже було зазначено веб-сервера є дуже поширеним і дорогим активом компанії. Одночасно із цим є величезна кількість видів вразливостей і відповідно загроз веб-серверам:

– DoS та DDoS;

– Brute Force Attack;

– Directory Traversal;

– XSS (Cross-site scripting);

– MITM;

– DNS Server Hikacking.

Для автоматизації перевірки веб-серверу на вразливості необхідно використовувати сканери вразливостей. На рисунку 2.8 показано сканування

сайту програмою OWASP ZAP. Було знайдено кілька недоліків у розробленому веб-сайті, які слід виправити, щоб покращити безпечність: встановити заголовок Content Security Policy та X-Content Type-Options. Різні сканери вразливостей використовують різні алгоритми та є орієнтованими на певні типи вразливостей, тому слід використовувати одночасно декілька із них, причому має бути встановлена найновіша доступна версія.

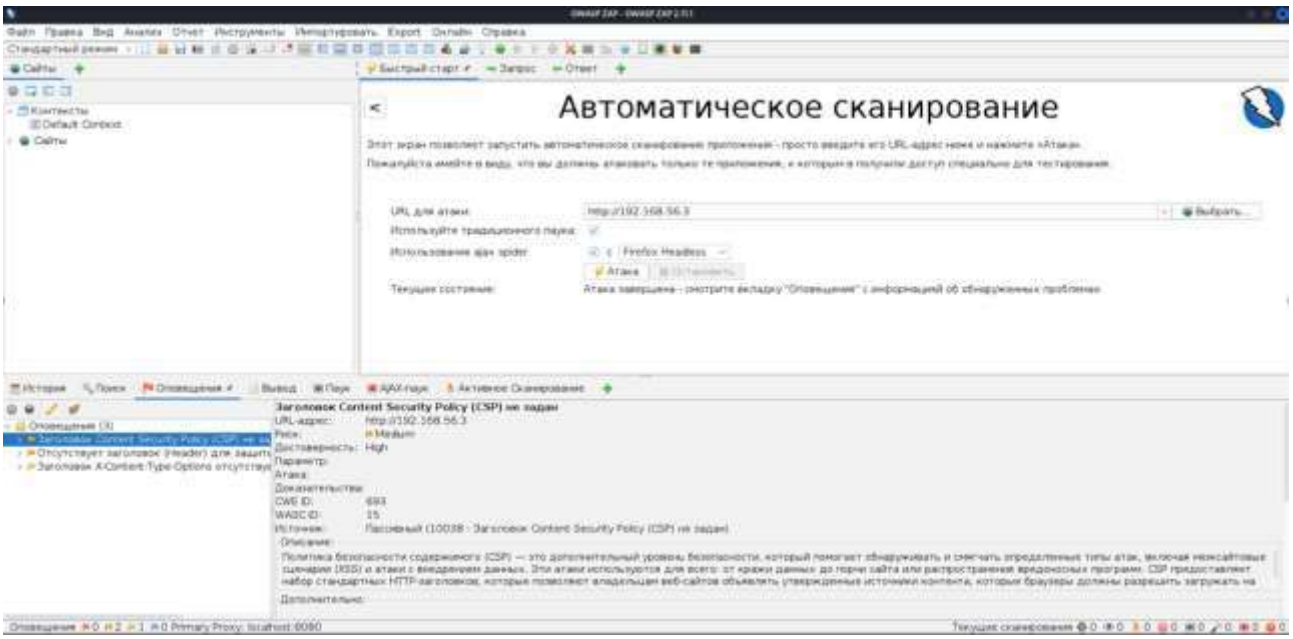


Рисунок 2.8 – Перевірка сайту програмою OWASP ZAP

На рисунку 2.9 показано результат сканування того ж самого веб-серверу, але сканером вразливостей Nikto. Можна побачити підтвердження вище сказаного, Nikto знаходить дві нові вразливості: не встановлений заголовок X Frame-Options для захисту від атаки clickjacking, та індексацію директорій, що не має бути доступна звичайним відвідувачам сайту.

Наступним етапом є тестування на злом паролів, його метою є перевірити чи працює на практиці встановлені політики щодо паролів. На даному етапі може бути виявлено, що, наприклад, нема обмеження по кількості спроб вводу неправильного паролю, паузи між спробами ввести пароль і т.д. Вибір

конкретного інструменту залежить від того, що саме перевіряється: служба віддаленого доступу, робоча станція, веб-сервер і т.д.

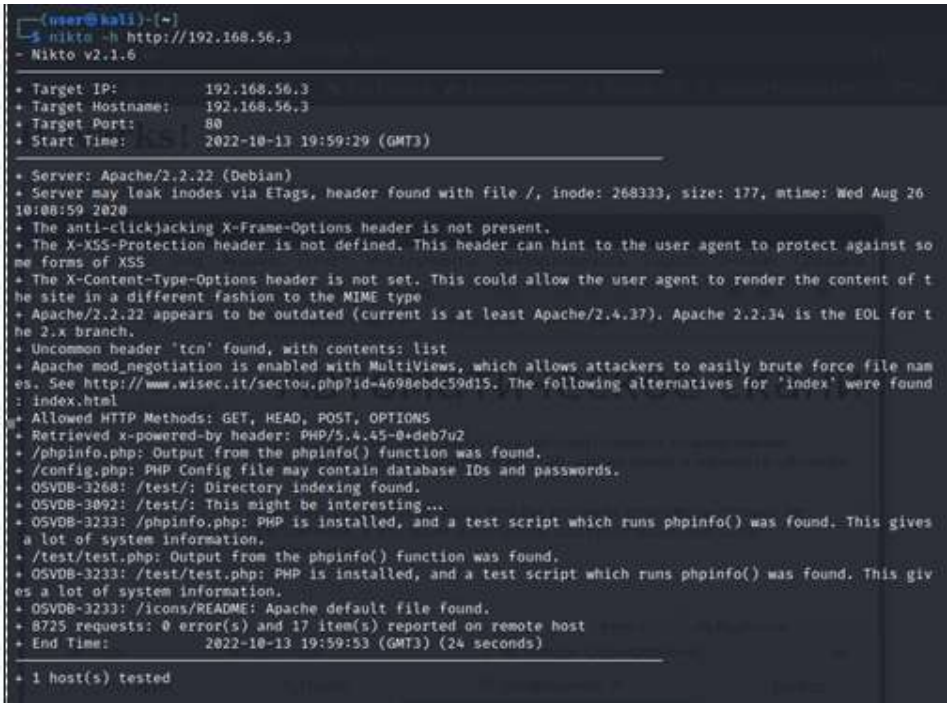


Рисунок 2.9 – Перевірка сайту сканером вразливостей Nikto

Атака на веб-сервер методом перебору за допомогою власноруч розробленого засобу показано на рисунку 2.10.

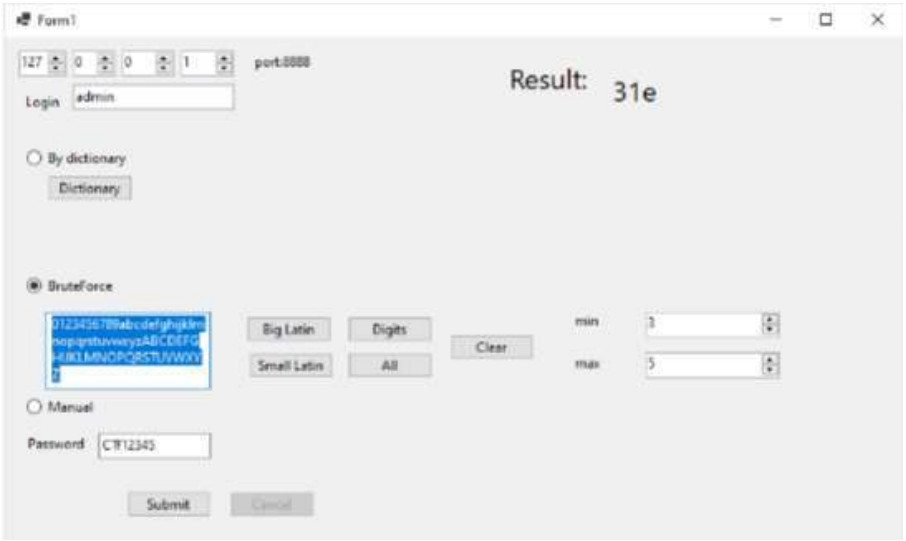


Рисунок 2.10 – Перевірка стійкості до атак методом перебору

Звичайно, час на розкриття паролю сильно залежить від його складності, довжини, відсутності у словниках, але політика безпеки організації має висувати вимоги не тільки до самого паролю, але й обмеження по часу між спробами, блокування після визначеної кількості невдалих спроб, вимагати зміни паролю через певний термін.

Із інструментів, що можна використати для даного типу тестувань, варто згадати THC Hydra, що може виконувати словникові атаки за понад 30 протоколами включаючи https, http, ftp, telnet, smb та інші. Ncrack теж є популярним інструментом, використовується для зламу паролів мережевої авторизації та автентифікації, що підтримує протоколи ssh. http(s), pop3, imap, різноманітні протоколи баз даних та інше.

Все більше організацій починають впроваджувати бездротові технології та пристрої інтернету речей. Тому необхідно перевіряти безпечність WiFi та інших з'єднань.

Бездротові технології вимагають захисту від атак на відмову в обслуговуванні, що досить легко здійснюється, від атак прослуховування, тому що сигнал є досить потужним і може бути перехоплений на великій відстані, можливої незаконної модифікація сигналу і здійснення атаки людина посередині та інші.

З пристроями інтернету речей ситуація значно гірше, вони часто не мають вбудованих функцій безпеки, не отримують необхідних оновлень для виправлення виявлених вразливостей.

У даній системі буде використовуватися програма aircrack-ng для виявлення і дослідження існуючих мереж, перевірки їх алгоритмів шифрування, визначення рівня потужності сигналу та перевірки на атаку до відмови і перебору паролів. Ця утиліта являє собою набір програм, які перехоплюють, аналізують, розшифровують, моніторять трафік, зламують ключі, здійснюють атаки на пристрої у мережі.

На рисунку 2.11 показано моніторинг і перехоплення спроб авторизації у

WiFi мережі програмою aircrack-ng.

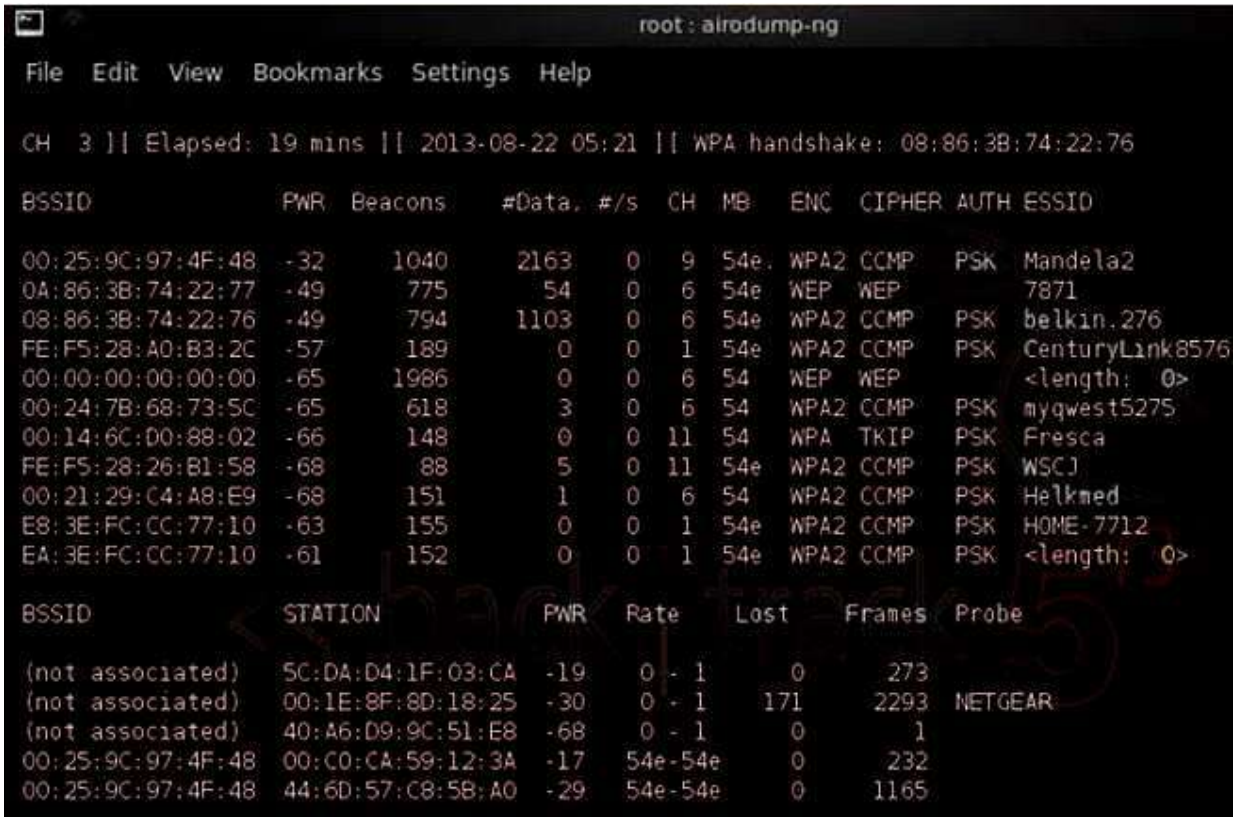


Рисунок 2.11 – Перевірка стійкості до атак методом перебору

Більшість із вказаних інструментів є вже встановленими в дистрибутиві Kali Linux – операційної системи, що використовуються спеціалістами та ентузіастами кібербезпеки для різноманітних цілей. Варто використовувати саме його, тому що він надає ряд переваг: велика колекція інструментів для тестування на проникнення «з коробки», безкоштовність, регулярність оновлень, документованість, гнучкі налаштування робочого середовища, отримання підтримки від активної онлайн-спільноти.

Методи огляду – це дослідження, що в більшості випадків проводяться вручну для оцінки систем, застосунків, політки безпеки з метою виявлення вразливостей. До них відносяться перегляд документації, конфігурацій, журналів, встановлених правил. Зібрана інформація використовується у методах оцінки загроз та ризиків.

Розглянемо перевірку журналів. Під час неї вивчається чи комплекс засобів захисту реєструє належну інформацію, чи дотримано політику безпеки організації щодо ведення журналів. Перегляд журналів може виявити проблеми, такі як спроби вторгнення або неправильно налаштовані служби.

Журнали можуть зберігатися у різних форматах і можуть використовуватися різні програми для їх перегляду. Іноді спеціалісту доведеться витратити час на ознайомлення із інтерфейсом програми та структурою журналу.

Наприклад, у організації, в якій створено комплексну систему захисту інформації для виконання вимог законодавства може бути встановлений програмний засіб Аудитор (входить до системи захисту інформації ЛОЗА-1), що є інструментом для введення і перегляду журналу реєстрацій подій безпеки. Приклад роботи з ним показаний на рисунку 2.12, розглядається подія успішного входу до облікового запису Windows.

Окремо жоден із методів (метод огляду, метод ідентифікації та аналізу цілей, метод перевірки вразливостей) не може надати повну картину безпеки мережі, тому використовується їх поєднання. Різні методи використовуються у різних обставинах, які найдоцільніше використовувати у конкретній ситуації для досягнення результату.

Варто вказати, що були розглянуті технічні методи, але існує багато нетехнічних методів, які теж мають бути використані на додаток. Прикладом є перевірка фізичної безпеки: чи захищене обладнання, чи можна обійти замки, охорону або інші засоби контролю.

Інший приклад становить ідентифікація активів, що можна здійснити або технічними засобами або за допомогою інвентаризації, фізичного обходу приміщень.

Необхідно зазначити, що експертиза зазвичай не впливає на діяльність реальної інформаційної системи, тоді як тестування передбачає практичну роботу з мережею організації і може вплинути на неї. Рівень потенційного

впливу залежить від конкретних інструментів і їх використання. Згадані вище інструменти і їх способи застосування не мають створити серйозних перешкод функціонуванню мережі.

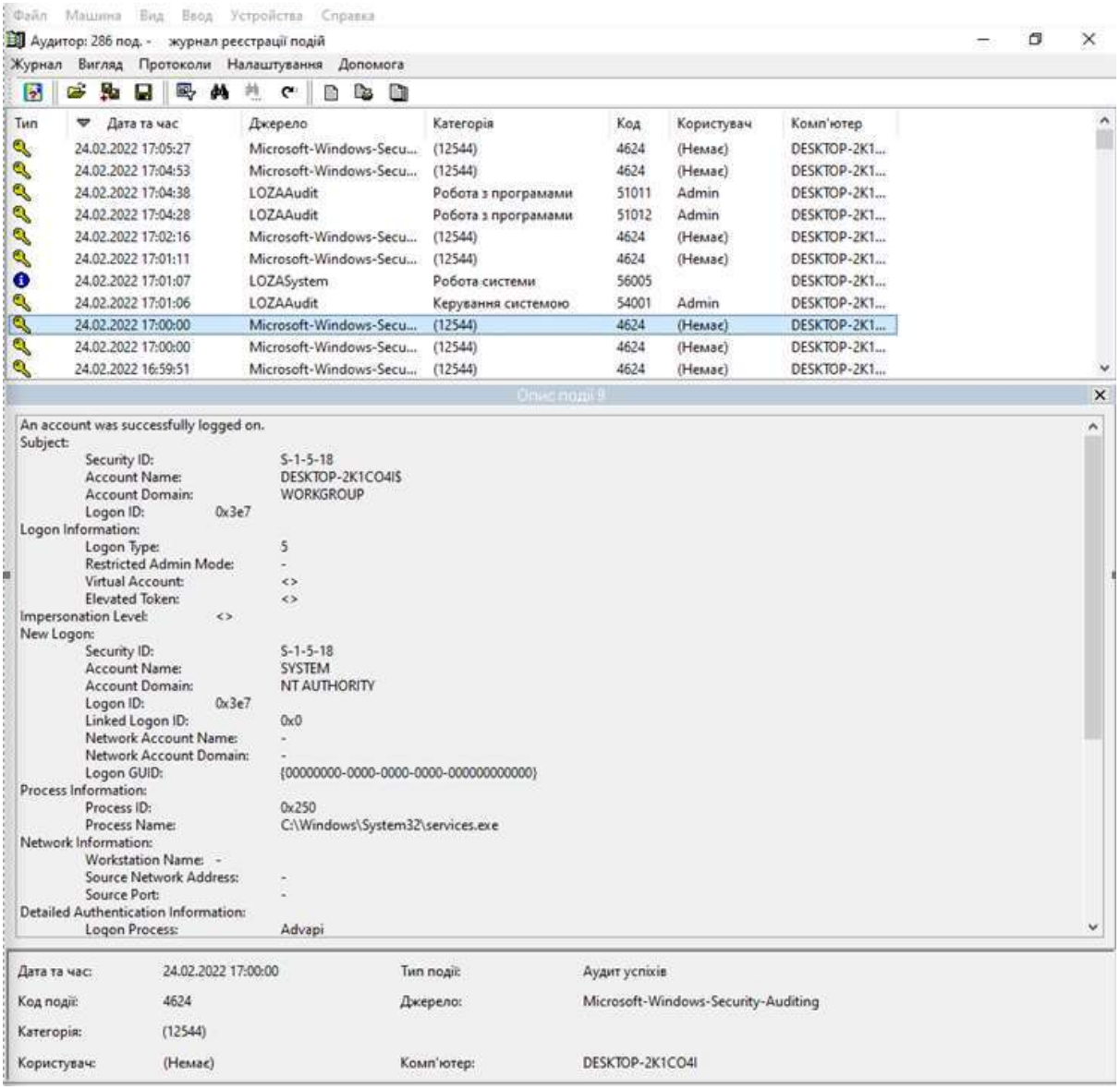


Рисунок 2.12 – Огляд журналів

Тестування на проникнення є необхідним інструментом, хоча має обмежене застосування, через обмеженість ресурсів, особливо використаного часу, на відміну від потенційного зловмисника, що може витратити стільки часу скільки забажає. Тестування дає можливість глянути з іншої точки зору, наскільки легко внутрішньому чи зовнішньому зловмиснику атакувати мережу.

Маючи обмеженість у ресурсах розроблена методика пошуку загроз та вразливостей зосереджується на найбільш поширених атаках і найважливіших активах, що підлягають захисту, використовуючи безкоштовні, але надійні та ефективні засоби.

2.2 Моделі інформаційної безпеки в комп'ютерній мережі

Побудова моделей інформаційної безпеки необхідна для розробки стратегій і конкретних заходів забезпечення інформаційної безпеки мережі. Їх потрібно використовувати для розуміння, аналізу ситуацій, планування заходів щодо управління інформаційною безпекою.

У розроблених моделях показані активи організації, ризики по відношенню до них, загрози та вразливості, які можуть мати місце і через, які загрози можуть реалізуватися.

Розглянемо модель інформаційної безпеки для усієї організації зображену на рисунку 2.13. На ній зображені лише найважливіші елементи. Ризики вказуються у прямокутниках із знаком червоного трикутника. Ризики були розділені на ризик втрати інформації, тобто порушення властивостей доступності або цілісності інформації, та ризик порушення конфіденційності інформації. Об'єднання було зроблене, тому що є велика кількість загроз та вразливостей, що порушують одночасно і цілісність і доступність інформації.

У колах із червоним попереджувальним трикутним знаком записуються можливі сценарії реалізації загроз. Очевидно, що більшість інформації буде викрадено або через злам інформаційної системи, або через скомпрометовані паролі.

Загрози або в деяких випадках джерело загрози позначається білою фігуркою людини, якщо це ненавмисна загроза, та білим прапорцем, якщо джерелом загрози не є людина і чорним силуетом, якщо це навмисна загроза.

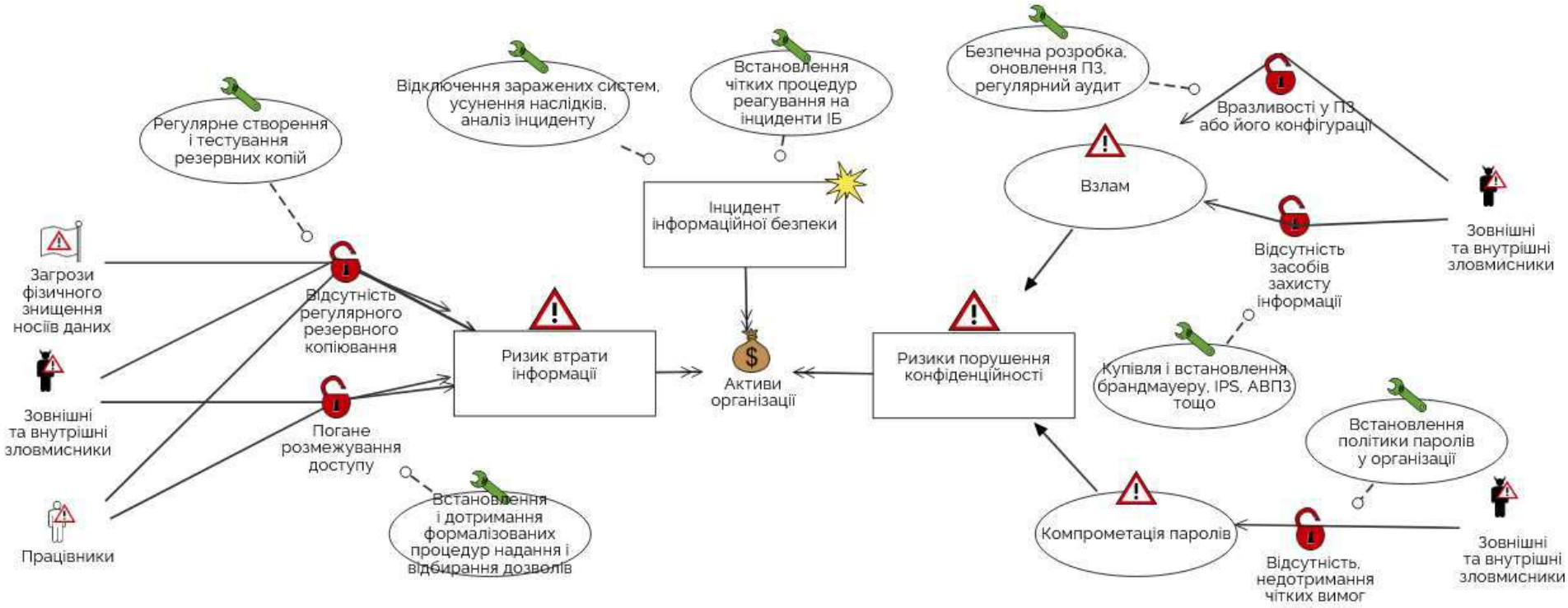


Рисунок 2.13 – Модель інформаційної безпеки для організації

Червоний відкритий замок символізує можливу вразливість. Вразливостей, через які конкретна загроза може реалізуватися може бути декілька. Біля кожної вразливості у пов’язаному із нею колі із зеленим ремонтним ключем надається рекомендація, як її усунути.

На даній схемі (рисунок 2.13) розглядаються базові вразливості і необхідні заходи, такі як: вимога регулярного резервного копіювання, встановлення комплексу засобів захисту, коректно налаштованих правил розмежування доступу інформації, визначення і дотримання формалізованої політики щодо паролів, яка містить у собі вимого щодо стійкості паролів, кількості спроб вводу, автоматичного блокування після певної кількості невдалих спроб, регулярної зміни паролю та інше. Також вкрай необхідним є впровадження і дотримання чіткого порядку дій при виявленні інциденту інформаційної безпеки.

У розробленій системі оцінці ризиків моделі інформаційної безпеки побудовані для кожного активу. Відповідно до активу і визначаються класи загроз з загального переліку загроз.

Були виділені такі класи загроз:

– загрози апаратному забезпеченню;
– загрози на рівні хосту;
– загрози на рівні дротових каналів комунікації;
– загрози на рівні бездротових каналів комунікації;
– загрози веб-серверів;
– загрози баз даних;
– загрози електронної пошти;
– загрози облікових записів;
– загрози мережевого рівня.

Почнемо детально розглядати побудовані моделі. Щоб мати працездатну мережу будь-яка компанія має мати певний набір робочого і мережевого обладнання: робочі станції, сервери, маршутизатори (роутери), комутатори,

брандмауери, бездротові точки доступу, планшети та інше. Звичайно, у типовій організації, більше ніж 90% вартості становлять інформаційні активи, але фізичне обладнання теж має свою вартість, і у деяких компаній, наприклад, хостинг-провайдерів, може навпаки складати більшу частину вартості. Вартість активу для організації на наступних етапах вплине на оцінку і розрахунок ризиків.

Від працездатності і стану апаратного забезпечення залежить стабільність функціонування інформаційної системи і безперешкодність інформаційних процесів у ній.

На рисунку 2.14 зображено побудовану модель інформаційної безпеки для апаратних складових: загальний ризик становить 13,8%.

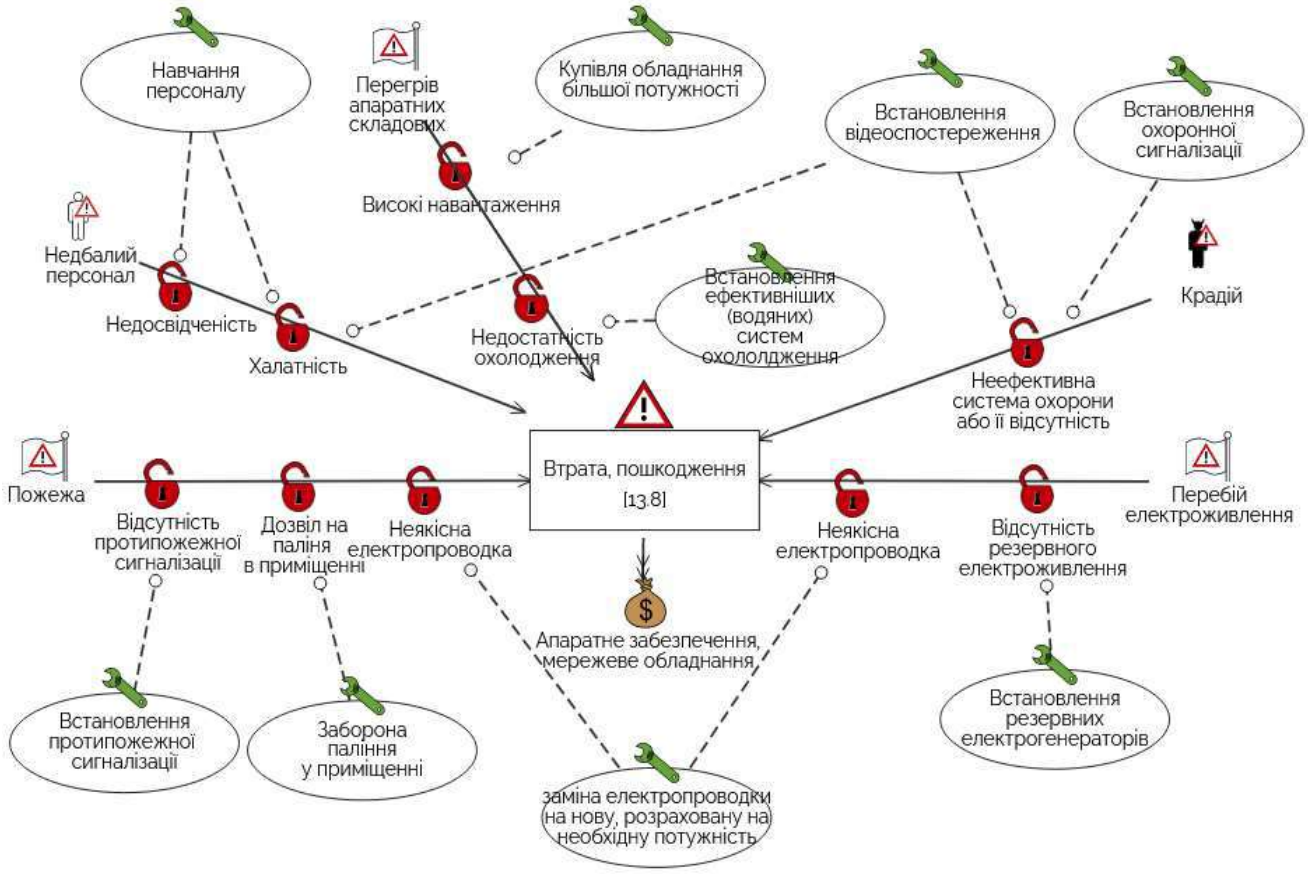


Рисунок 2.14 – Модель інформаційної безпеки для апаратного забезпечення

Принцип мереж в тому, що вони складаються з вузлів, інша назва яких у

контексті мережевої топології – хости. Ним може бути будь-який комп'ютер або сервер, але оскільки основні типи серверів розглядаються окремо, тут варто розуміти робочі станції, пристрої інтернету речей, інші використовувані пристрої з підтримкою мережевих технологій.

В даному випадку порушення можливості їхнього нормального використання призведе до простою працівників, витрати сил на усунення несправностей, втрати оброблюваних даних.

Повне уявлення про можливі загрози, вразливості та способи їх ліквідації можна отримати з рисунку 2.15.

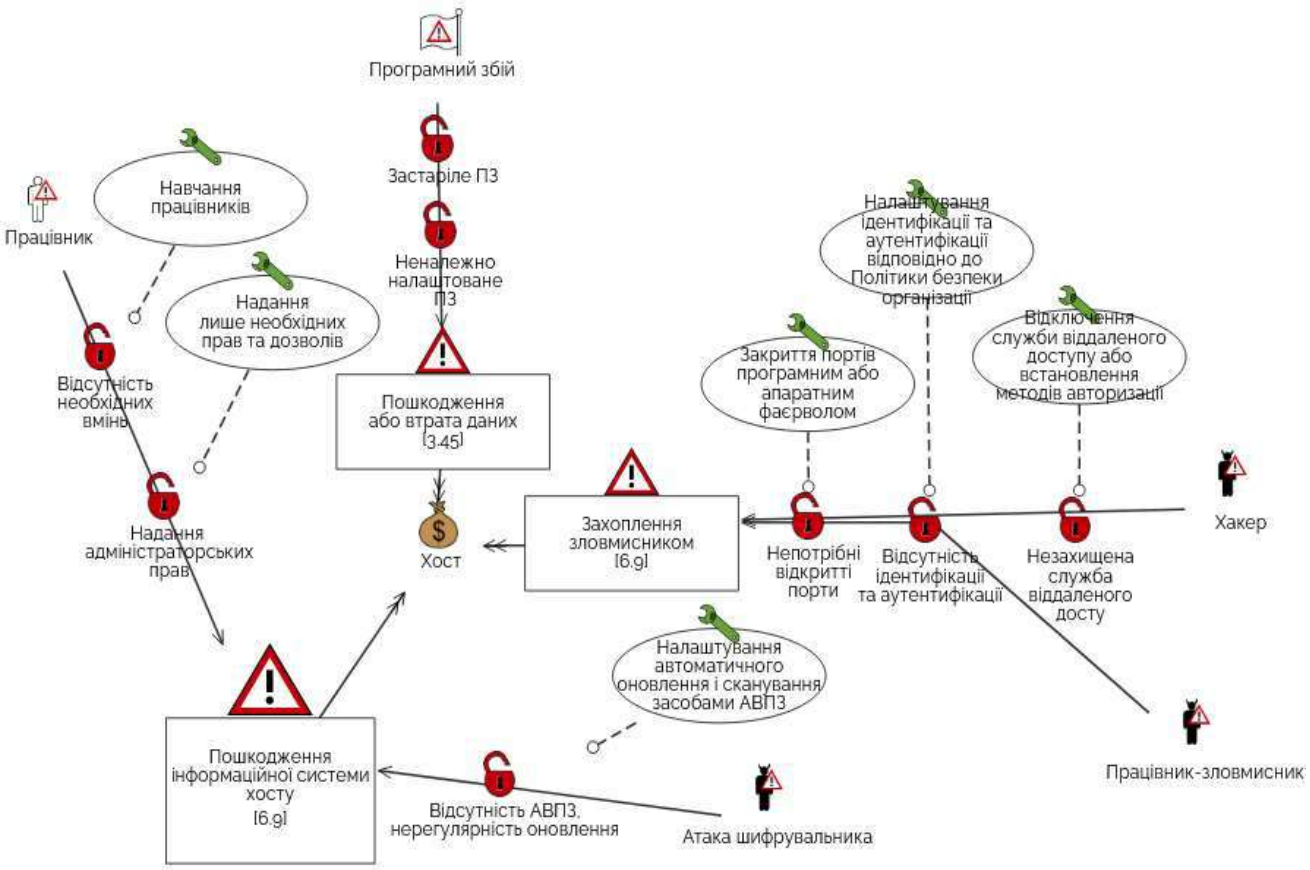


Рисунок 2.15 – Модель інформаційної безпеки на рівні хосту

Для внутрішнього або зовнішнього зловмисника захоплення одного пристрою дає точку з якої він може спробувати захопити інші більш цінні ресурси, зібрати інформацію про архітектуру мережі, визначити способи,

засоби і рівень захисту мережі, отримати конфіденційну інформацію, до якої він права доступу не має.

На рисунку 2.15 на відміну від попереднього виділено декілька більш конкретних ризиків і відповідно обчислена ймовірність кожного із них. Загальний ризик для хостів організації можна вважати сумою ризиків пошкодження або втрати даних, пошкодження інформаційної системи хосту, захоплення зловмисником, що буде становити 17,25%.

Перейдемо тепер до розгляду каналів зв'язку, що забезпечують діяльність мережі. На рисунку 2.16 модель інформаційної безпеки для дротової мережі організації. Дротові з'єднання за допомогою мідних, оптоволоконних або коаксіальних кабелів забезпечують зв'язок між пристроями як у локальній мережі (LAN), так і забезпечують з'єднання з інтернетом (WAN). Обрив зв'язку може позбавити пристрій, підмережу, або повністю мережу організації нормального функціонування. Саме тому необхідно потурбуватися про безпеку своїх комунікацій та наявність резервного підключення. Для таких компаній, як інтернет-провайдери, дротові канали комунікацій є одним із ключових активів, і забезпечення нормального функціонування є їх головним бізнес-завданням. Інші компанії часто не звертають належної уваги на даний актив, доки не понесуть збитків, через простій бізнесу.

Станом на сьогодні активно розвиваються і впроваджуються в життя по всьому світу бездротові технології зв'язку. Маючи переваги у вигляді простоти підключення пристроїв, зручності експлуатації, розширюваності, швидкості встановлення, можливості використання мобільних пристроїв та пристроїв інтернету речей, є й значні проблеми у сфері інформаційної безпеки безпроводових мобільних технологій.

Якщо порівнювати з точки оцінювання ризиків дані типи зв'язку, то ризики у разі використання бездротових технологій зв'язку зростають: ризик недоступності з 6,9% до 10,35%, а ризик перехоплення трафіку зростає з 3,45% до 6,9%.

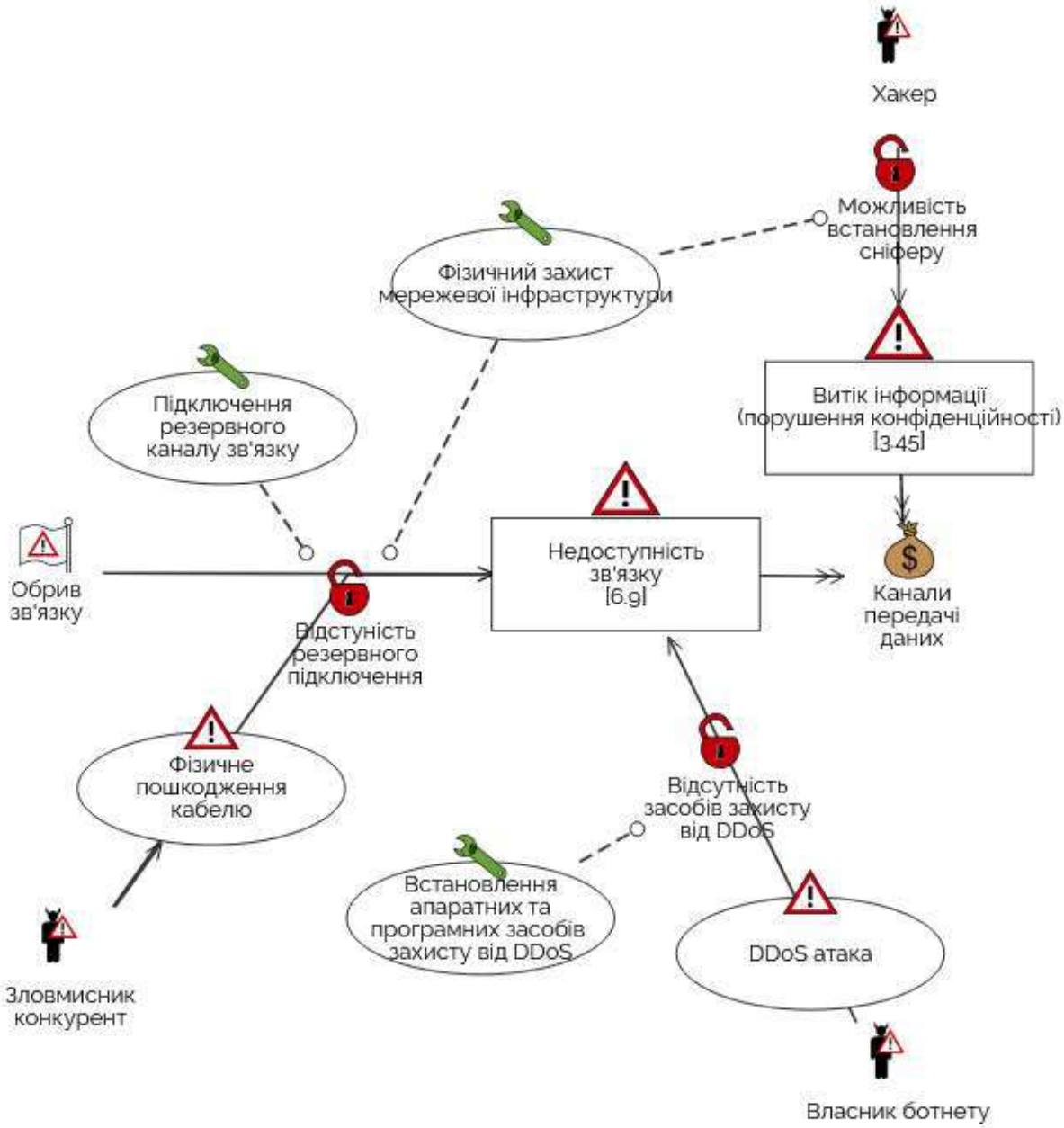


Рисунок 2.16 – Модель інформаційної безпеки для дротових комунікацій

Загрози, вразливості, рекомендації щодо використання цього типу зв’язку можна побачити на рисунку 2.17. Звичайно, якщо компанія не використовує бездротовий зв’язок його буде виключено із розрахунку ризиків.

Для забезпечення захисту інформації у більшості програмного забезпечення використовуються механізми ідентифікації, аутентифікації та авторизації. Паролям, які є основним методом аутентифікації має приділятися відповідна увага. Облікові записи до яких належать логіни та паролі, або інші

способи доступу виділені в окремий актив, тому що становлять велику цінність для зловмисника.

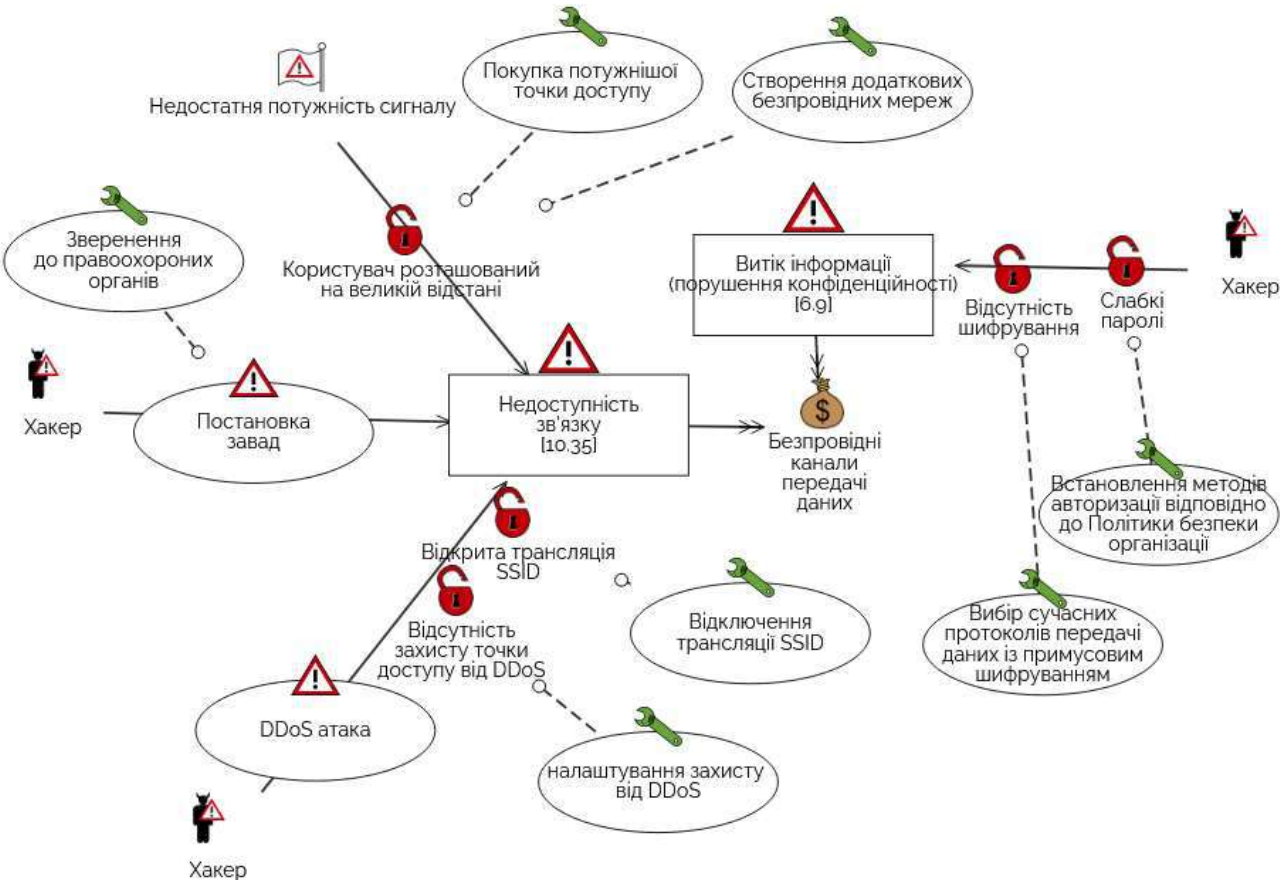


Рисунок 2.17 – Модель інформаційної безпеки для бездротових комунікацій

В організації мають бути встановлені конкретні вимоги до паролів і механізмів автентифікації, що використовуються у компанії щодо:

– довжини паролю;

– складності паролю;

– неповторюваності паролю;

– частоти зміни паролю;

– автоматичного блокування після декількох невдалих спроб.

Варто звернути уваги, що якщо не буде встановлено механізмів забезпечення даних вимог, то більшістю працівників вони будуть проігноровані. Також посилювати захист необхідно не лише для облікових

записів адміністраторів і керівництва, а для усіх працівників.

Модель інформаційної безпеки по відношенню до облікових записів, показано на рисунку 2.18, якщо не вживати ніяких заходів, то ризик зламу облікових записів є досить високим.

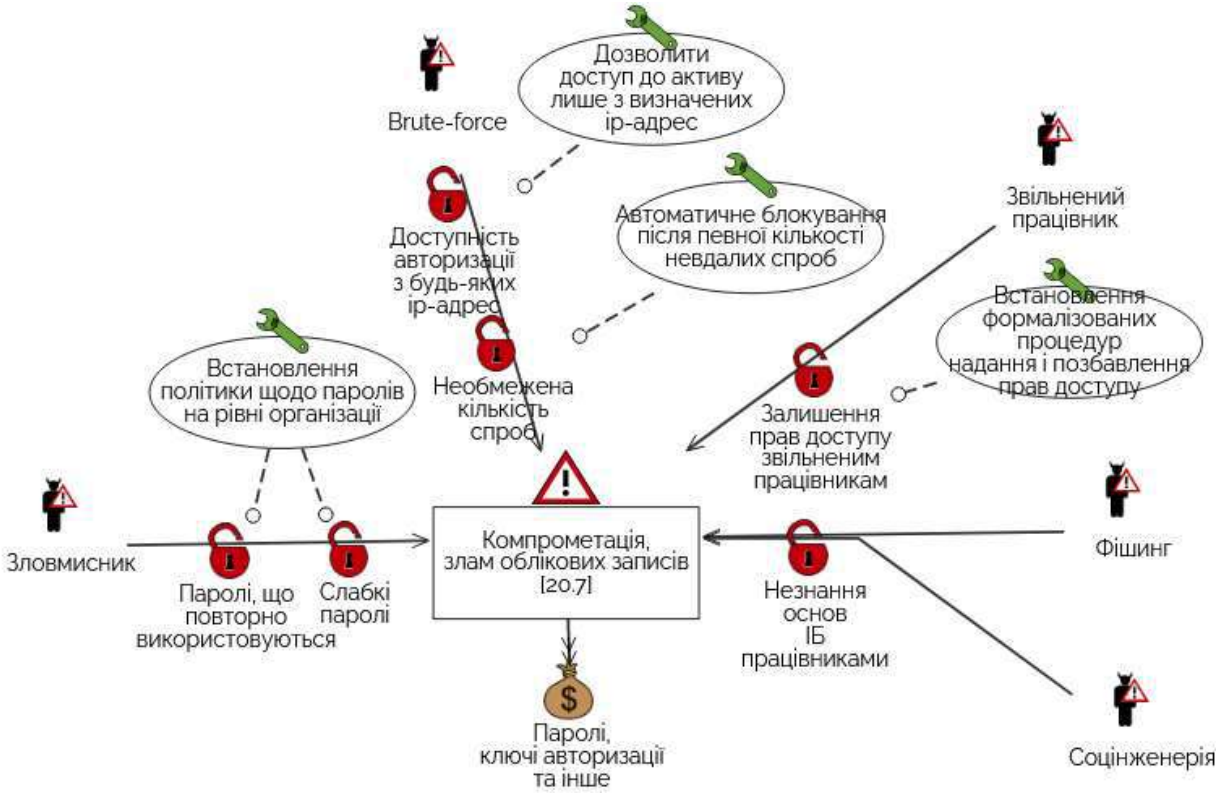


Рисунок 2.18 – Модель інформаційної безпеки для облікових записів

Обговоривши механізми авторизації, обговоримо необхідність використання методів авторизації, тобто процесів, що визначать рівень доступу користувача до ресурсів. Несанкціонований доступ часто відбувається через, те що користувачу надається більше прав ніж йому необхідно. Також необхідно слідкувати і вчасно забирати права у звільненого або переведеного на іншу посаду працівника.

Як було сказано у попередньому підрозділі, більшість компаній мають веб-сервера, вони є дуже цінним і вразливим активом, тому їх безпеці необхідно приділяти відповідну увагу. Модель інформаційної безпеки веб-серверів можна побачити на рисунку 2.19.

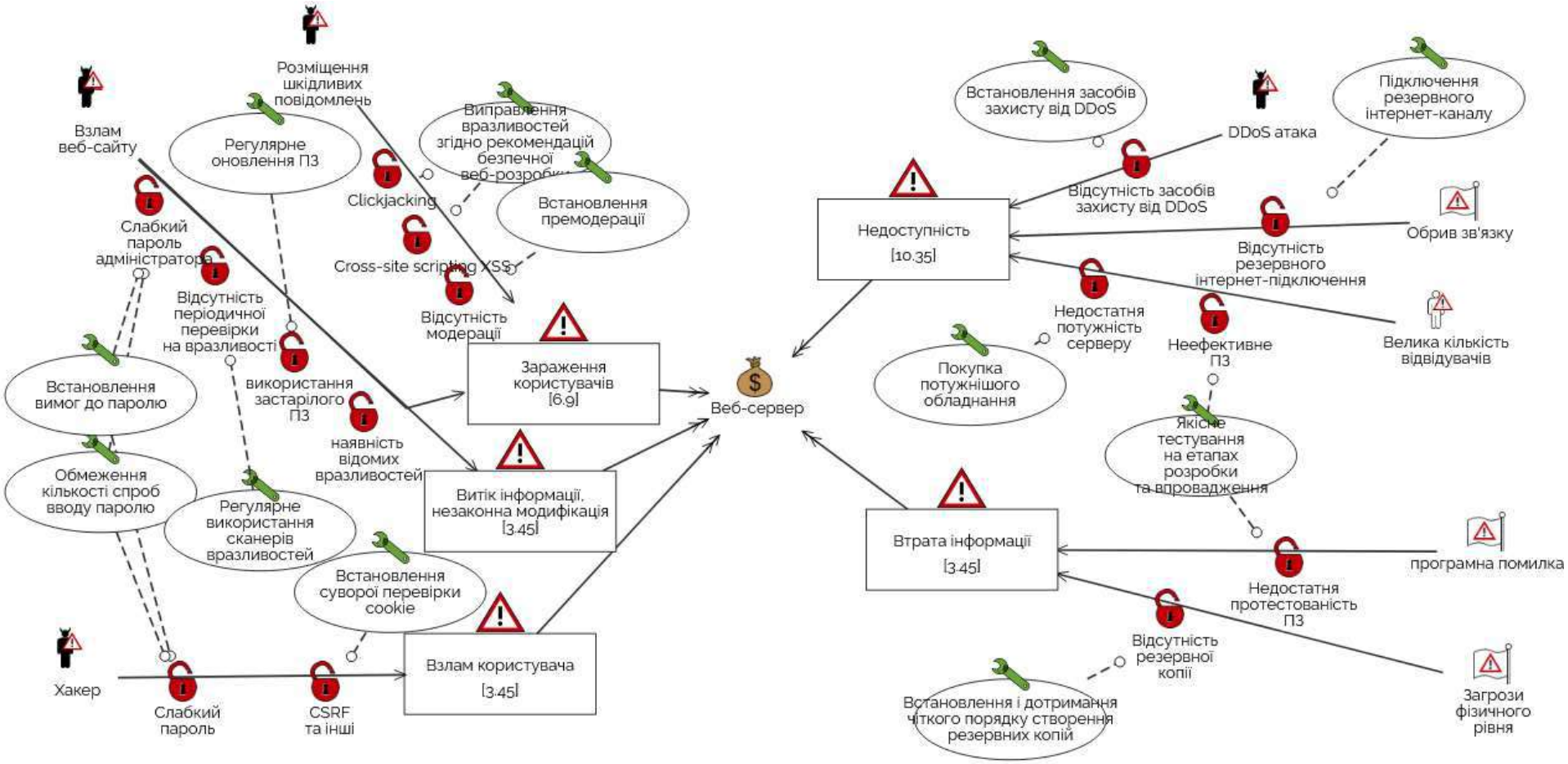


Рисунок 2.19 – Модель інформаційної безпеки веб-серверу

Важливість даного активу зростає, якщо веб-додатки в інтернеті розміщені на серверах є основним продуктом компанії, наприклад, IT-стартапу, або якщо сайт є основним джерелом генерації клієнтів та продаж.

Жодна компанія не може обійтися без баз даних. Саме у них зберігаються основні інформаційні активи організацій. Модель інформаційної безпеки щодо баз даних показано на рисунку 2.20.

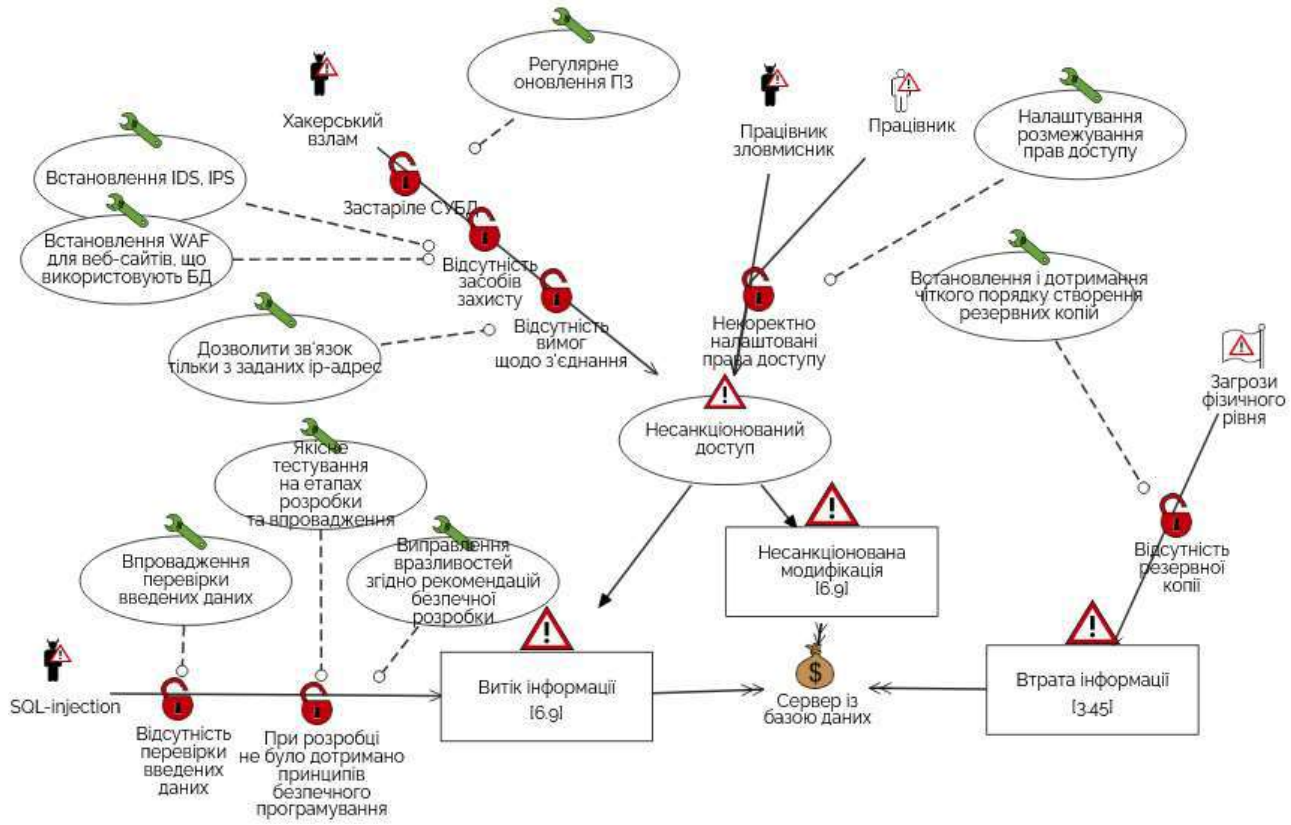


Рисунок 2.20 – Модель інформаційної безпеки для бази даних

Побудована модель включає в себе, як загрози, що виникають внаслідок використання систем управління баз даних з застосуванням найпоширенішої мови запитів до баз даних SQL, такі як SQL-injection, так і загрози, які зустрічаються і до інших типів активів, такі як несанкціонований доступ внаслідок неправильно налаштованого розмежування доступу, чи хакерський взлам через використання вразливостей застарілого програмного забезпечення. На схемі показано, що якщо буде реалізовуватися сценарій несанкціонованого

доступу, наслідком може стати порушення усіх властивостей інформації, а отже повна втрата активу, що у випадку важливої бази даних іноді може стати причиною банкрутства компанії, у тому числі і внаслідок репутаційних та юридичних збитків.

Станом на сьогодні електронна пошта залишається одним із основних засобів спілкування для більшості організацій. Основні протоколи та технології, що використовуються зараз були розроблені у 2000-х роках, тому її безпека є одним із важливих аспектів її використання. Побудовану модель інформаційної безпеки для даного активу, можна побачити на рисунку 2.21.

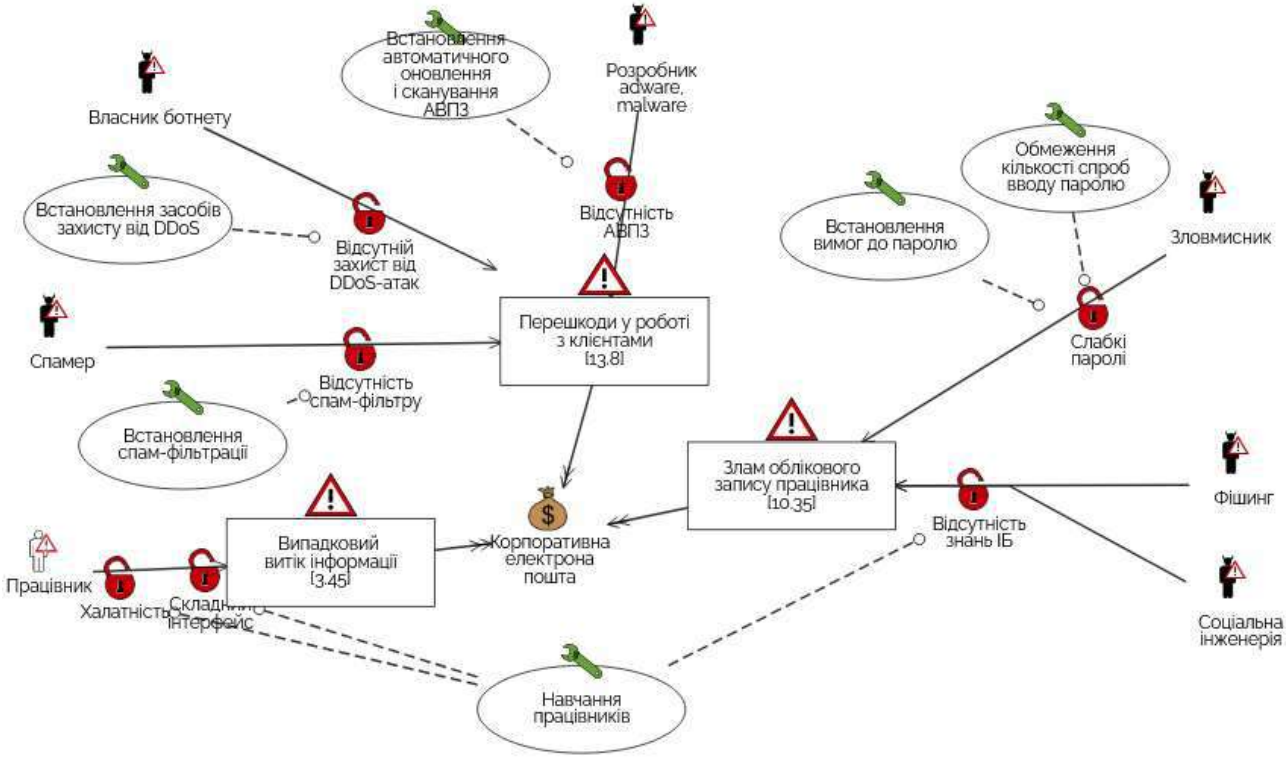


Рисунок 2.21 – Модель інформаційної безпеки для електронної пошти

Можна зробити висновок, що використання електронної пошти вимагає, як встановлення різноманітних засобів захисту: спам-фільтрів, антивірусного програмного забезпечення, систем шифрування за потреби, так і навчання працівників основам інформаційної безпеки.

Більшість підприємств та установ використовують не тільки власну

мережу, а й підключення до інтернету. Доступ до інтернету відкриває, як переваги його використання, так і нові зовнішні загрози. Для захисту від зовнішніх віддалених зловмисників мережу організації необхідно захистити брандмауером (фаєрволом).

Цей пристрій є одним із ключових для забезпечення безпеки мережі та розміщених у ній інформаційних систем. При виборі брандмауеру необхідно врахувати його можливості з потужністю трафіку у мережі. Враховуючи, що фаєрволи мають різний функціонал і можуть замінити собою деякі пристрою. Купівля брандмауера може бути вигідною, наприклад, навіть найдешевші моделі можуть замінити у тому числі роутер та дати можливість створення VPN-з'єднань для віддалених працівників або офісів.

На рисунку 2.22 подано модель інформаційної безпеки з використанням фаєрвола для мережі організації. Основними рекомендаціями є:

– поділ мережі на підмережі;
– встановлення списків керування доступу;
– створення демілітаризованої зони;
– вчасне оновлення прошивки фаєрволу.

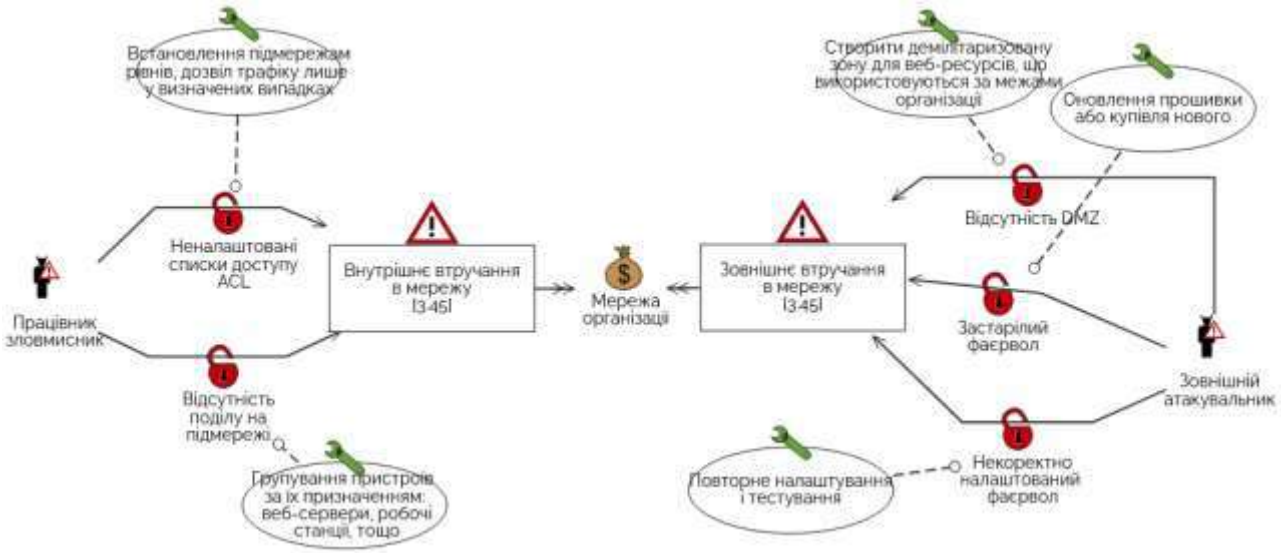


Рисунок 2.22 – Модель інформаційної безпеки на рівні мережі організації

Розглянуті моделі інформаційної безпеки були створені для зручної демонстрації і розуміння мережевих загроз, вразливостей, ризиків та їх взаємозв'язків. Надані пояснення потрібні для розуміння контексту побудови моделей. Зібраний у даному розділі матеріал необхідний для реалізації інформаційно-аналітичної системи оцінки ризиків інформаційної безпеки комп'ютерної мережі.

2.3 Обґрунтування вибору методу оцінювання ризиків інформаційної безпеки в комп'ютерних мережах

Якісні методи оцінки ризиків можуть використовуватися, як проміжний етап в процесі розробки і реалізації рішення щодо системи оцінювання ризиків, але вони не дають достатньої інформації про рівень ризику. Остаточні висновки можна зробити лише в результаті проведення кількісних розрахунків.

Основною задачею для використання кількісного методу є числове вимірювання можливого впливу ризиків використання комп'ютерних мереж на організацію-замовника оцінки. Виражатися воно має в конкретному грошовому вигляді.

Кількісну величину ризиків можна досить точно обрахувати використовуючи математичний апарат теорії ймовірності і методи математичної статистики.

Для цього необхідно мати абсолютне значення можливого ризику, що буде дорівнювати вартості активу для діяльності організації. Вартість активу буде визначатися за методом OCTAVE Allegro, спрощеною та оновленою методикою OCTAVE. Перевагами оцінювання активів за даною методологією є:

– простота методу;

– доступні покрокові інструкції;

– адаптивність і гнучкість.

Після здійснення ідентифікації та визначення вартості активів, для розрахунку ризику у розробленій системі використовується статистичний метод. Для його використання знадобиться програмування математичних формул. Ризик розуміється як спосіб оцінки ймовірності отримати певний негативний результат, по відношенню до всіх можливих результатів. Ймовірність ризику для активу є сумою ймовірностей реалізації загроз для даного активу через вказані вразливості.

Перевагами і причинами обрання статистичного методу є:

– простота реалізації методу;

– легкість розрахунків;

– адекватність формалізації уявлень про ризики;

– грошова форма вираження ризиків;

– гнучкість методу;

– можливість покрокового включення або виключення змінних у розроблену модель для більш точних результатів.

У сфері захисту інформації відбувається постійний розвиток нових технологій, а отже з’являються нові загрози, вразливості, тенденції атак, тому аналіз статистичних даних по подіям, що були у минулому є недоцільним. В розробленій системі оцінки ризиків використовується теоретичний аналіз структури причинно-наслідкових зв’язків інформаційних та мережевих процесів, на основі побудованих моделей інформаційної безпеки, розглянутих у попередньому підрозділі.

2.4 Висновки

У даному розділі були розглянуті методи виявлення інформаційних загроз в комп’ютерних мережах та необхідні для цього засоби. Було відібрано

ряд інструментів, що рекомендуються для використання і надані приклади їх застосування у методах тестування та експертизи мережі.

Активи були поділені на категорії і до кожної були визначені загрози. Побудовані моделі інформаційної безпеки зручно дають уявлення про існуючі ризики, загрози, вразливості, методи їх усунення та взаємозв’язки між ними. Пророблена робота створює основу для власне реалізації інформаційно-аналітичної системи оцінки ризиків.

Обраний метод оцінювання ризиків був обґрунтований, були вказані причини вибору і його переваги.

3 РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Структура системи

Для того, щоб здійснити на практиці інформаційно-аналітичне оцінювання ризиків, необхідно зрозуміти структуру розробленої системи.

Діяльність системи по оцінюванню ризиків відбувається внаслідок отримання замовлення від організації, що потребує оцінки стану інформаційної безпеки для своєї мережі. Здійснити замовлення оцінювання може власник, начальник, інша уповноважена особа організації. Відповідно, саме замовнику і буде надаватися результат.

Проводити оцінювання ризиків буде експерт, який обізнаний з даною методикою і який має усі необхідні для проведення оцінювання засоби. Особисті якості експерта не мають впливати на результат, оскільки, як було розглянуто раніше вироблена покрокова методика дозволяє послідовно з мінімальним використанням ресурсів провести оцінювання.

Структуру системи, послідовність дій при оцінці, особи, що приймають участь у ній, досліджувані активи та необхідні інструменти показано на рисунку 3.1. На зображені вказано, що експерт використовує описані у попередньому розділі методи інтерв'ювання, тестування та експертизи. Також схематично показано основні дії та над якими елементами їх необхідно виконати. Якщо розглядати інтерв'ювання, то бачимо, що маючи необхідні анкети (у тому числі для визначення вартості активів згідно методики OCTAVE Allegro) експерт проводить опитування працівників, зображених у жовтому колі. Обробивши результати інтерв'ювання оцінювач вносить дані до програми, що обробляє зібрані дані. Тестування проводиться щодо таких активів: веб-серверів, серверів баз-даних, та стійкості до зламу облікових записів. На даній схемі усюди у стрілках з зеленою рамкою вказано дії експерта.

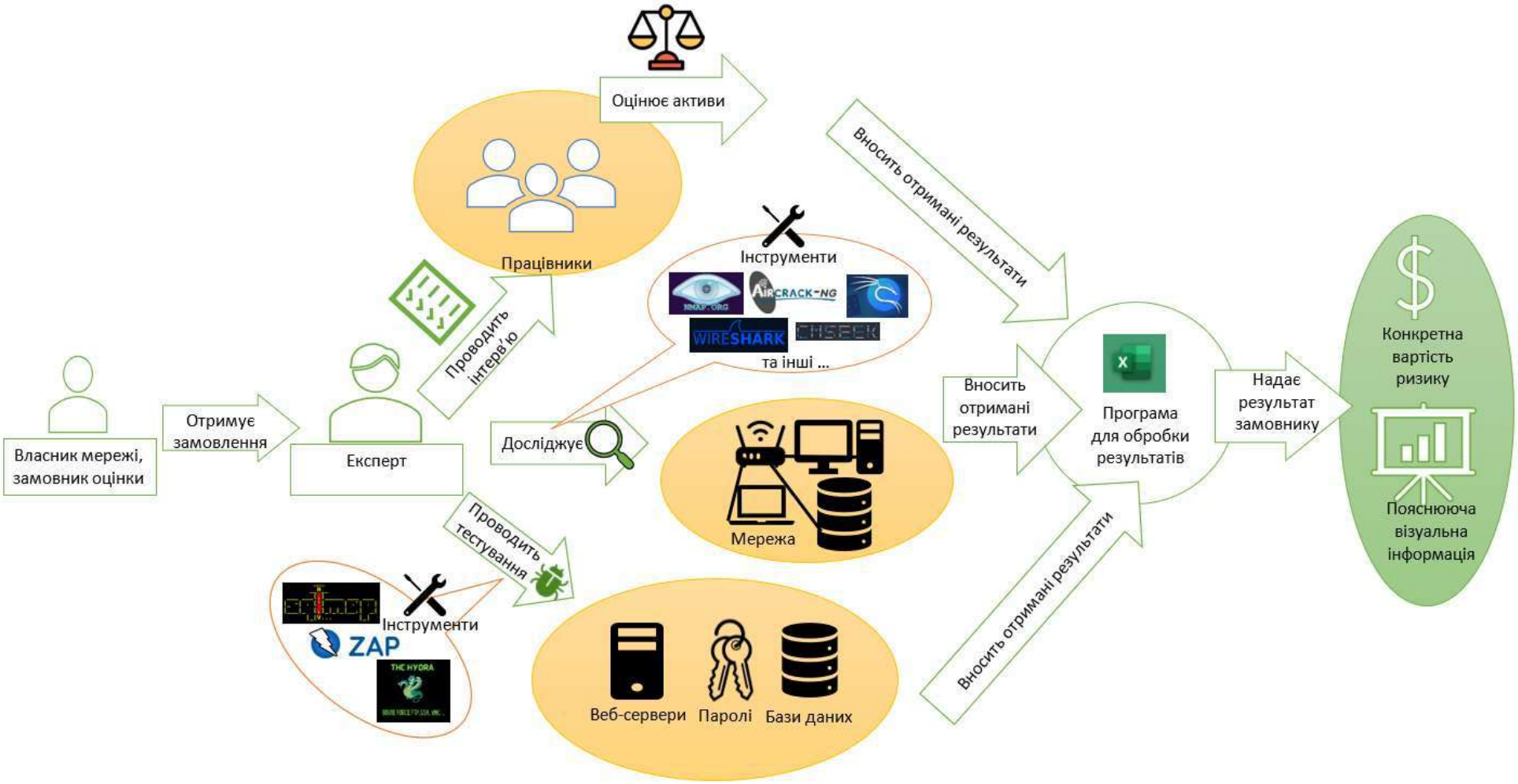


Рисунок 3.1 – Структура системи оцінювання ризиків

У оранжевій виносці зображені деякі логотипи використовуваних програмних засобів, що використовуються експертом у даних дослідженнях. Набір цих інструментів, їх можливості, мета і область застосування та інші аспекти практичного застосування вже були детально розглянуті у попередньому розділі.

Зібрану інформацію експерт вручну вносить до анкети і таблиць програми, що обраховує ризики. Отриманий результат оцінювання експерт надає замовнику.

Результатом оцінювання ризиків є виражена грошова сума ризику, яку може понести організація при існуючому стані інформаційної безпеки. Відповідно до вже розглянутих у роботі активів, визначається сума ризику для кожного активу. Інформація про ризики подається також у візуальному вигляді для наочної демонстрації та її кращого сприйняття.

Отриманий результат дозволяє розробити стратегію і плани по керуванню ризиками і забезпеченню стану інформаційної безпеки. Для цього можна використовувати розроблені у роботі моделі інформаційної безпеки.

Якщо організація-замовник нехтує інформаційною безпекою, то проведена оцінка дає можливість керівництву зрозуміти, які ризики несе використання незахищених інформаційно-комунікаційних систем у вигляді можливих втрат та визначити суму коштів, які варто витратити на організаційні заходи та технічні засоби захисту інформації.

У випадку коли установа-замовник вживає заходів щодо управління інформаційною безпекою, то отриманий результат показує оцінку ефективності існуючих заходів безпеки, дає можливість розставити пріоритети у заходах безпеки та оптимізувати затрати на інформаційну безпеку сфокусувавшись на найбільш значущих областях та уникаючи непотрібних витрат.

Результати оцінки ризиків надають керівництву компанії об’єктивні дані для прийняття вмотивованих і обґрунтованих рішень щодо захисту інформації, що є в нинішній час важливою складовою захисту репутації, дотримання

нормативних вимог, підвищення конкурентоспроможності і т.д.

Вважаю необхідним розглянути математичні формули по яким проводяться розрахунки. Оцінка ризиків проводиться на основі взаємозв'язків ризиків, загроз і вразливостей.

Для реалізації системи було створено множину загроз. Дані загрози можуть реалізовуватися через вразливості. На ймовірність ризику щодо активу впливає відношення кількості загроз у відповідному класі загроз до загальної кількості загроз. Через одну вразливість може реалізуватися декілька загроз, так само і одна загроза може реалізуватися через одну із декількох вразливостей. Можна зробити висновок, що загрози і вразливості пов'язані між собою типом зв'язку «багато до багатьох».

Розглянемо детально формули по яким здійснюються розрахунок ризику. У формулі 3.1 розраховується ризик щодо конкретного активу:

$$R_a = \sum_{i=1}^{n} A \cdot P_i , \tag{3.1}$$

де A – це вартість активу; P_i – це ймовірність реалізації i-тої загрози, n – це кількість загроз для даного активу.

Ймовірність реалізації загрози залежить від того, чи є вразливості для її реалізації, що визначається з наданих на запитання відповідей анкети розробленої програми. Розрахунок імовірності реалізації загрози проводиться за формулою:

$$P = \sum_{j=1}^{k} N_j \cdot \frac{P_{розр}}{k}, \tag{3.2}$$

де N_j – значення, яке показує ступінь знешкодження загрози, приймає мінімально можливе значення нуля при надійно вжитих заходах, приймає

максимально можливе значення одиниці при відсутності запобіжних дій, для деяких вразливостей приймає значення у діапазоні від мінімального до максимального при частковому захисті; $P_{розр}$ – теоретично розраховане значення ймовірності реалізації даної загрози; k – кількість вразливостей, через які дана загроза може реалізуватися.

Отже після розгляду формул (3.1) та (3.2), можна перейти до обчислення загального ризику для мережі:

$$R = \sum_{i=1}^{n} R_i , \tag{3.3}$$

де R_i – це ризик для і-того активу, n – кількість активів мережі для яких проводиться обчислення.

Використовуванні формули виведені із математичного апарату теорії ймовірностей та основних понять теорії ризиків.

3.2 Реалізація методу оцінювання ризиків інформаційної безпеки в комп'ютерних мережах

Для програмної реалізації математичної складової оцінки ризиків було вирішено розробити програму у вигляді електронної таблиці Microsoft Excel. Оскільки пакет офісних програм Microsoft Office є широко використовуваним у більшості компаній, проводити дії з такою електронною таблицею буде зручним і зрозумілим для більшості потенційних користувачів. На даний час у компаніях електронні таблиці застосовуються для вирішення найрізноманітніших завдань.

Розробка додатку у вигляді автоматизованої електронної таблиці надає ряд переваг у розробці:

– простота і швидкість розробки;

– великий вбудований набір формул, інструментів та засобів для розрахунків та аналізу даних;

– широкі можливості візуалізації даних у вигляді графіків, діаграм для наглядної демонстрації;

– рішення є кросплатформним з можливістю використання через браузер за допомогою хмарних сервісів.

Окремо розглянемо переваги електронної таблиці порівняно з класичними комп'ютерними програмами з точки зору користувача при роботі з ними:

– інтуїтивно зрозумілий інтерфейс;

– багатокористувацький доступ з використанням хмарних офісів;

– легкість внесення змін у разі необхідності без знання мови програмування та необхідності декомпіляції.

Для захисту від людських помилок при введені даних та для зручності використання, можливості введення відповідей на питання було обмежено готовими варіантами організованими у список. Поля, що передбачають введення числових даних приймають лише ціле невід'ємне число. Це було реалізовано за допомогою стандартного функціоналу перевірки даних Microsoft Excel.

Після надання відповіді на питання, відповідна клітинка підсвічується червоним або зеленим кольором відповідно до того чи є це правильним з точки зору інформаційної безпеки. Для питань, що передбачають більше варіантів відповідей, ніж «Так» або «Ні» встановлено більш широко кольорову гаму. Цього результату було досягнуто через створення і налаштування правил умовного форматування.

У розробленій анкеті питання поділені на підпункти, які по змісту залежать від головного питання. Наприклад, якщо в організації не проводиться навчання працівників, то не є логічним надавати відповідь на підпункт про

регулярність, в даному випадку у списку буде присутній лише один пункт «Ні». Для вирішення даної ситуації були використані взаємозв’язані списки.

Зовнішній вигляд анкети у розробленій програмі можна побачити на рисунку 3.2.

Пункт	Підпункт	Питання	Відповідь
По результатам інтерв'ювання та огляду:			
1	Чи встановлено Політику інформаційної безпеки в організації?		Так
1	1	Чи призначено відповідальних осіб?	Ні
1	2	Чи відомий її зміст усім працівникам?	Ні
1	3	Наявні конкретні обов'язки із забезпечення режиму ІБ?	Ні
2	Чи встановлено Політику щодо паролів?		Так
2	1	Присутня вимога щодо довжини паролю не менше 8 символів	Так
2	2	Наявність вимоги щодо складності паролю (Великі, малі, цифри, спецсимвол)	Так
2	3	Наявне автоматичне блокування після невдалих спроб	Так / Ні
2	4	Заборона повторного використання паролів	Так
2	5	Встановлено вимогу регулярної зміни паролю	Ні
2	6	Визначені вимоги, щодо забезпечення виконання даної політики	Так
2	Чи є порядок реагування на кіберінциденти та план відновлення?		Так
3	При розробці та/або експлуатації ПЗ приділяється увага принципам безпечної розробки?		Так
4	Чи є встановлені правила створення і тестування резервних копій?		Так
5	Чи встановлені правила розмежування доступу?		Так
5	1	Працівнику надаються лише необхідні права і дозволи?	Так
5	2	Наявні формалізовані процедури управління правами доступу?	Ні
5	3	Надання і відбирання прав проводиться вчасно?	Ні
6	Чи встановлено політику ведення, збереження і перегляду журналів?		Так
6	1	Журналювання засобами захисту та ПЗ ведеться у достатньому обсязі	Так
6	2	Регулярний перегляд журналів для аналізу інцидентів ІБ	Ні
7	Проводиться навчання працівників?		Так
7	1	Регулярність?	Щоквартально
7	2	Навчання правильної роботи з використовуваним ПЗ	Ні
7	3	Навчання протидії фішингу	Так
7	4	Навчання протидії соціальній інженерії	Ні
7	5	Навчання основам ІБ	Так
7	6	Навчання правилам створення і використання паролів	Так
7	7	Вироблення відповідального ставлення до обв'язків	Ні

Рисунок 3.2 – Вигляд анкети у розробленій програмі

Підпункти виділяються сірим кольором, якщо внаслідок відповіді на

головне питання вони виключаються з розгляду. Такий випадок трапляється, наприклад, у запитанні про бездротові мережі. Якщо в мережі організації відсутні бездротові комунікації, то пов’язані з ними ризики виключаються із загального розрахунку і оцінки.

Розроблена електронна таблиця за змістом розподілена на декілька аркушів, а саме:

– аркуш для введення зібраної інформації;

– аркуш з діаграмами і графіками, що показують оцінку ризиків і стан інформаційної безпеки;

– додаткові аркуші з довідковою інформацією про загрози та для ведення нотаток.

Враховуючи особливості розробки програми у вигляді електронної таблиці, у деякий клітинках виконуються фонові розрахунки, тому для захисту коректної роботи програми від випадкового втручання, встановлено захист для аркушів, що дозволяє вносити зміни лише до тих клітинок, які призначенні для введення інформації.

На першому аркуші розмішується анкета для введення даних, розділена на дві частини. Перша частина для збору результатів по методам інтерв’ювання та огляду, а друга частина стосується результатів тестування та експертизи.

Збоку від анкети знаходиться таблиця, в відповідний стовбець цієї таблиці необхідно ввести вартість активів, у інших стовпцях автоматично буде розраховано ризики.

На другому аркуші розміщені діаграми та графіки, які згруповані у такі розділи:

– аналітика стосовно ризику вираженого у грошовому вимірі;

– аналітика по ризику вираженому у відсотковому вигляді;

– аналітика по стану інформаційної безпеки.

До складу розділу про аналітику ризику у грошовому вигляді включені такі діаграми та графіки:

– гістограма для порівняння вартості ризиків по активам;

– кругова діаграма для отримання уявлення про те, який відсоток від вартості усіх активів становить сумарний ризик;

– звичайна гістограма та гістограма з накопиченням про співвідношення вартості активу до його ризику;

– кругова діаграма для порівняння співвідношення вартості ризиків по активам між собою.

До складу розділу про аналітику про ризик, виражений у відсотках входять лінійна гістограма для отримання уявлення про ймовірність ризику стосовно кожного активу та кругова гістограма для порівняння величини даних ймовірностей між собою.

У розділі присвяченому аналітиці стану інформаційної безпеки міститься гістограма, що показує ефективність наявних вжитих заходів безпеки по кожному активу у процентах.

Розуміння, який актив є більш захищеним, а який менше, разом зі знанням про те який актив має найбільший ризик по вартості, дає можливість визначити слабкі місця, встановити пріоритети, визначити розмір бюджету на витрати по захисту інформації.

3.3 Оцінювання ефективності реалізованого методу

Для практичної перевірки результатів розробленої інформаційно-аналітичної системи оцінки ризиків комп’ютерної мережі було проведено оцінювання мережі відділення ПриватБанку під час проходження переддипломної практики.

На рисунку 3.3 зображено топологічну схему досліджуваної локальної мережі, з розподілом на підмережі. Саме для неї і буде проводитися тестова оцінка ризиків.

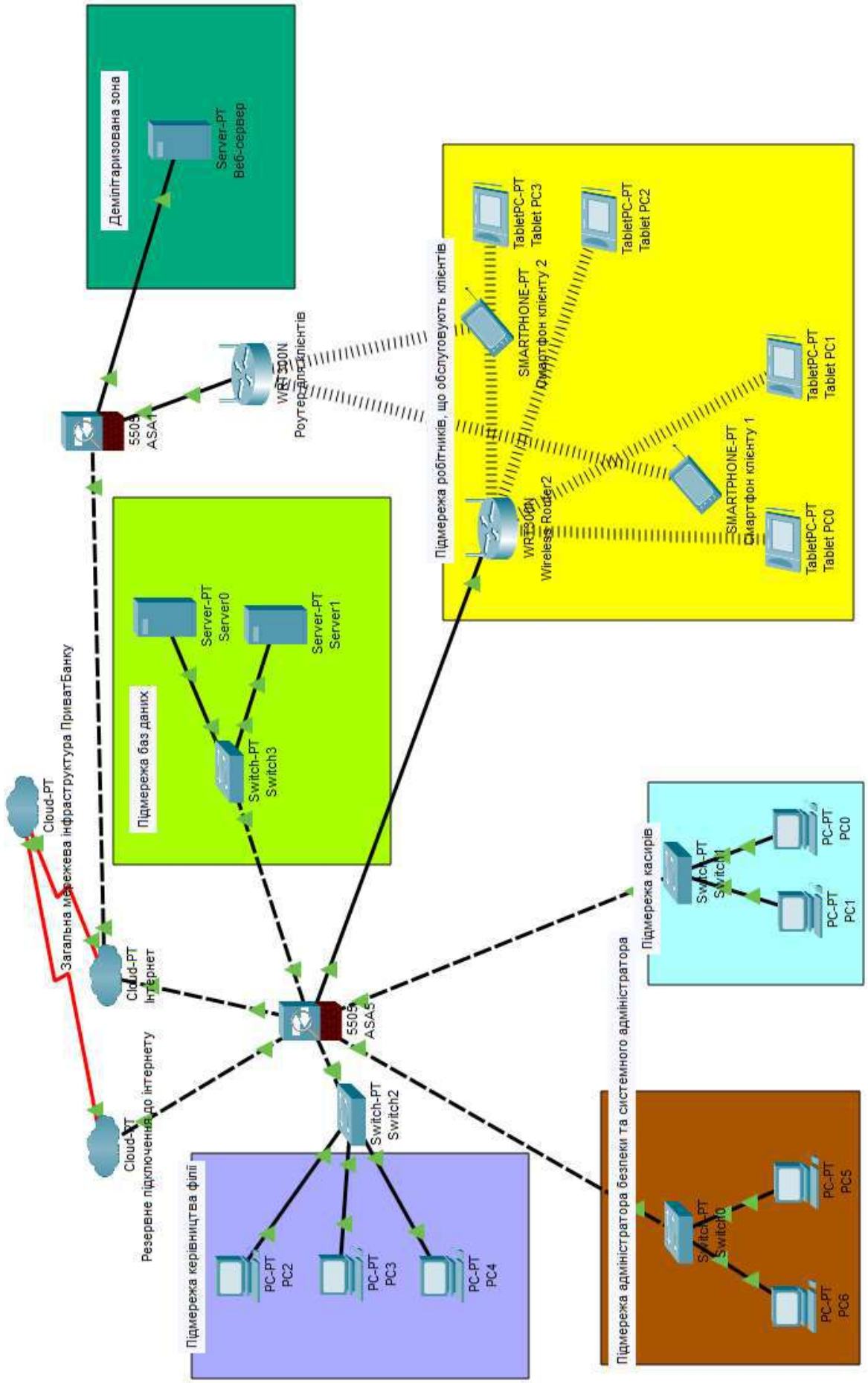


Рисунок 3.3 – Схема досліджуваної мережі

Після інтерв'ювання адміністратора інформаційної безпеки та інших призначених у робочу групу осіб були визначені вартості активів.

Таблиця 3.1 – Вартість активів

Назва активу	Вартість активу, грн
Апаратне забезпечення мережі	370000
Хости мережі	180000
Веб-сервери	300000
Бази даних	1500000
Електрона пошта	200000
Облікові записи	210000
Мережа	150000
Дротові комунікації	75000
Бездротові комунікації	50000

Апаратне забезпечення найлегше піддається кількісній оцінці, воно має конкретну грошову вартість. Оцінка хостів мережі в основному складається з вартості програмного забезпечення, яке встановлено на них, вартості часу простою цих хостів та затрат на відновлення їх працездатності. Веб-сервер є розробкою даної філії і призначений для підтримки деяких клієнтів юридичних осіб. Більшість інформації зберігається на віддалених серверах ПриватБанку, але частина інформації, яке необхідна для роботи передається у відділення і зберігається на місці. Звичайно, як і очікувалось, бази даних будуть найціннішим ресурсом. Недоступність бази даних призводить до простоїв у роботі, незаконна модифікація або інше пошкодження цілісності ставить під ризик подальшу діяльність з такою базою даних, а компрометація відомостей із неї призведе до репутаційних та юридичних втрат. Незважаючи на активне впровадження і перехід у відділенні на бездротові технології зв'язку, дротові комунікації оцінюються вище, тому що мають важливіше значення з точки зору

забезпечення безперебійності бізнес-процесів.

Після проведення необхідних досліджень, експертиз, тестувань і оброблення зібраної інформації було отримано наступні результати продемонстровані у таблиці 2.

Таблиця 3.2 – Результати оцінки ризиків

Актив	Ризик для активу, грн	Ризик для активу, %
Апаратне забезпечення	14886	4,02
Хости мережі	7657	4,25
Веб-сервери	20502	6,83
Бази даних	47437	3,16
Електрона пошта	15177	7,59
Облікові записи	8327	3,97
Мережа	1449	0,97
Дротові комунікації	0	0,00
Бездротові комунікації	1868	3,74

Загальна сума ризику складає 117301 гривню, що становить 3,86% від вартості активів. Необхідно враховувати, що стану коли ризик відсутній просто не буває. Даний рівень ризику є нормальним і підтверджує високий рівень вжитих заходів у ПриватБанку стосовно кібербезпеки.

Найбільшими по вартості є ризики щодо: баз даних, веб-серверів, електронної пошти та апаратного забезпечення. Найбільшу ймовірність реалізації ризику мають: електронна пошта, веб-сервер, хости мережі та апаратне забезпечення.

Гістограму, що демонструє співвідношення вартостей активів між собою та співвідношення вартості активу до вартості відповідного ризику, зображено на рисунку 3.4.

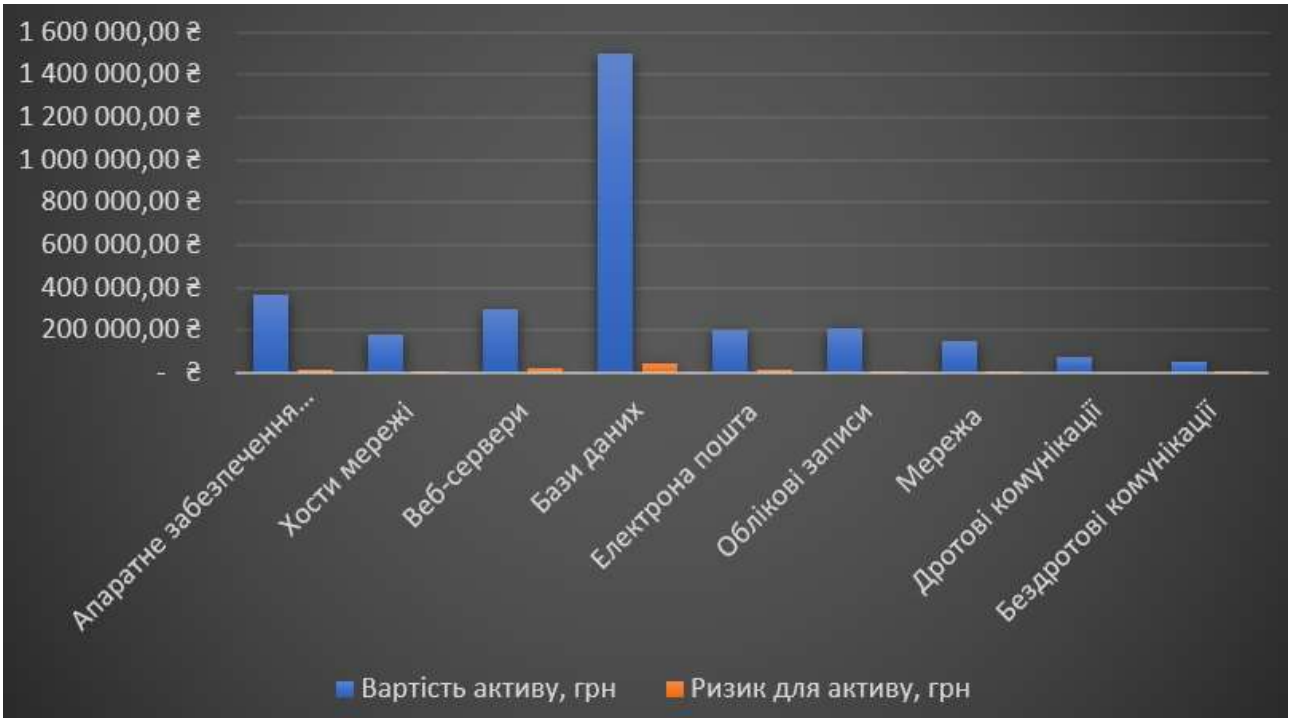


Рисунок 3.4 – Співвідношення вартостей активів та їх ризиків

Уявлення про співвідношення ризиків між собою, виражених у вартості, стосовно кожного активу, можна отримати з кругової діаграми зображеної на рисунку 3.5.

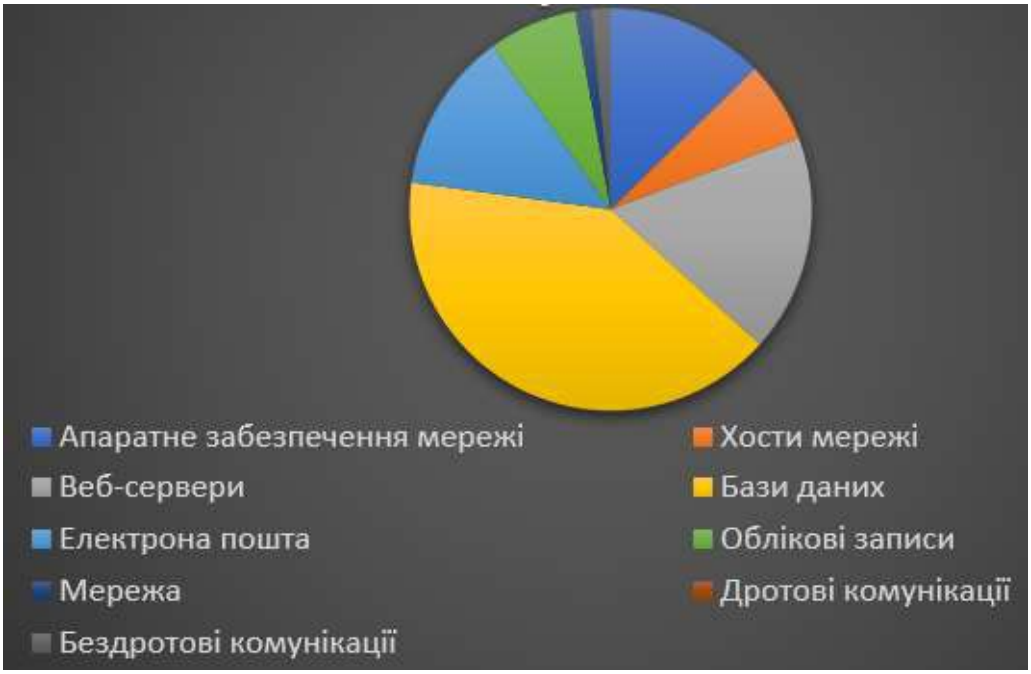


Рисунок 3.5 – Співвідношення вартостей ризиків по активам

Визначити слабкі місця та зрозуміти рівень інформаційної безпеки, виражений ефективністю наявних заходів безпеки по усуненню вразливостей і знешкодженню загроз можна з гістограми зображеної на рисунку 3.6.

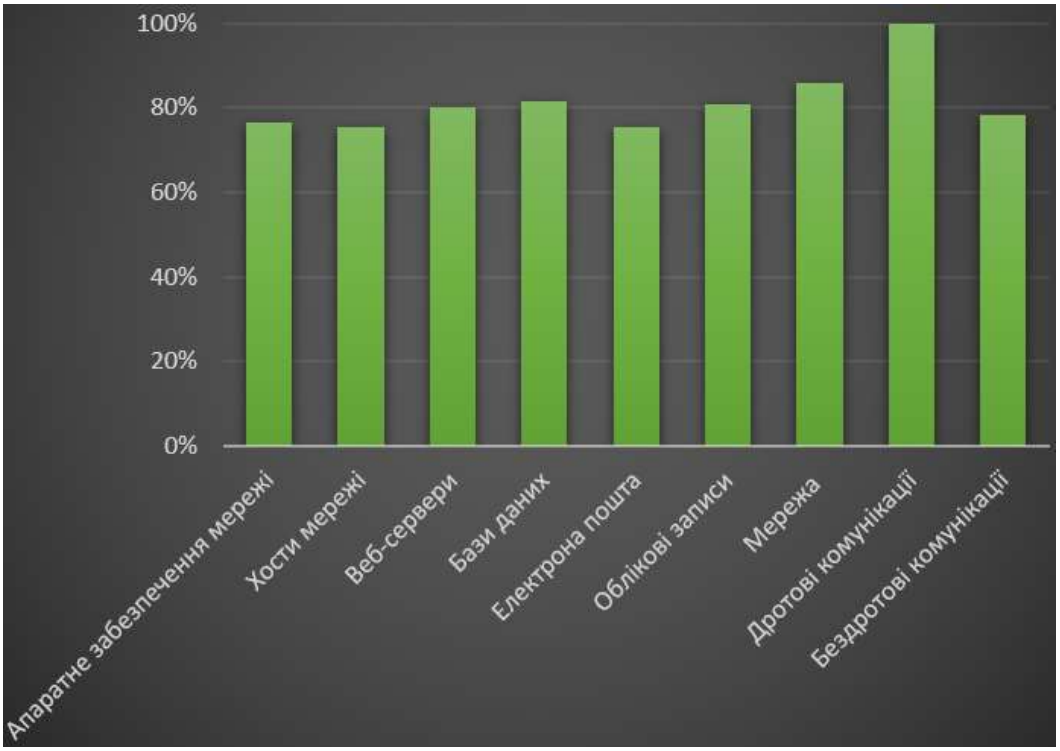


Рисунок 3.6 – Ефективність вжитих заходів безпеки

Рисунок 3.6 підтверджує, що у даній організації немає слабких місць, рівень захисту є стабільно високим для усіх активів. Банківській філії вдалося ефективно усунути більшість загроз.

З отриманих результатів проведеного оцінювання можна зробити висновок, що розроблена система є коректною і дає адекватні результати. Як і прогнозувалось, провідний банк України тримає високий рівень захисту інформації. Одним із слабких місць, як і більшості банківських установ, через специфіку їхньої діяльності, виявилось використання застарілого програмного забезпечення і складнощі з своєчасним встановленням оновлень. Для ще більшого зменшення ризику варто вирішити саме питання відмови від існуючих застарілих інформаційних систем з переходом на більш надійні нові

та знайти спосіб безперебійного для роботи організації та вчасного встановлення оновлень.

3.4 Висновки

У даному розділі детально розглянуто структуру розробленої інформаційно-аналітичної системи оцінювання ризиків щодо інформаційної безпеки комп’ютерної мережі, наведено короткі характеристики та аналіз її основних елементів.

Розроблена програма у вигляді електронної таблиці для виконання обчислень над зібраною інформацією і отримання результатів була детально розглянута, були вказані причини і переваги використовуваних рішень.

Створену систему було випробувано та підтверджено її ефективність.

ВИСНОВКИ

Оцінювання ризиків інформаційної безпеки комп'ютерних мереж є важливим і складним процесом для організацій. Для ефективного проведення оцінювання і отримання коректних результатів необхідне створення системи оцінки ризиків, що включає в себе розробку надійної методології і підбір необхідних інструментів.

В ході дипломної роботи були розглянуті різні види існуючих алгоритмів і методів оцінювання, наведено аналіз їх переваг та недоліків, досліджено актуальність проблеми оцінювання ризиків та доведено, що розробка інформаційно-аналітичної системи оцінки ризиків призначеної для комп'ютерних мереж, покращує якість оцінки ризиків.

Під час виконання роботи було створено моделі інформаційної безпеки, для яких визначено множини ризиків, активів, вразливостей, загроз, рекомендацій по необхідним заходам захисту інформації та встановлено взаємозв'язки між ними.

У роботі обґрунтовано вибір методу оцінювання ризиків, продемонстровано структуру системи, набір необхідних інструментів, реалізацію методу оцінювання.

В результаті роботи було створено інформаційно-аналітичну систему оцінки ризиків комп'ютерної мережі, випробувано на досліджуваній мережі і оцінено ефективність реалізованої системи.

Розроблена система є невимогливою до ресурсів, зручною, структурованою, послідовною, сучасною та має широкі можливості для подальшого оновлення, модернізації, вдосконалення згідно з новими потребами та вимогами.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. NIST SP 800-30 Rev. 1. Guide for conducting risk assessments. На заміну NIST SP 800-30; чинний від 2012-09-17. Вид. офіц. 2012. 95 с. URL: https://doi.org/10.6028/NIST.SP.800-30r1 (дата звернення: 01.03.2024).

2. Information security risk – Glossary. CSRC. NIST Computer Security Resource Center. CSRC. URL: https://csrc.nist.gov/glossary/term/information_security_risk (date of access: 01.03.2024).

3. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : Постанова Нац. банку України від 11.06.2018 р. № 64 : станом на 24 трав. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text (дата звернення: 01.03.2024).

4. ДСТУ ISO/IEC 27000:2019. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. На заміну ДСТУ ISO/IEC 27000:2017; чинний від 2019-11-01. Вид. офіц. 2019.

5. McGladrey K. How to Perform a Successful IT Risk Assessment. Hyperproof. URL: https://hyperproof.io/resource/it-risk-assessment/ (date of access: 14.03.2024).

6. Tunggal A. IT Security Risk Assessment Methodology: Qualitative vs Quantitative | UpGuard. Third-Party Risk and Attack Surface Management Software | UpGuard. URL: https://www.upguard.com/blog/risk-assessment-methodology (date of access: 16.03.2024).

7. Landoll D. Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. London: Taylor & Francis Group, 2021. 490 p.

8. Han C. Semi-quantitative Cybersecurity Risk Assessment by Blockade and Defense Level Analysis. Process Safety and Environmental Protection. 2021. URL:

https://doi.org/10.1016/j.psep.2021.09.028 (date of access: 28.03.2024).

9. Schmitz C., Sekulla A., Pape S. Asset-centric analysis and visualisation of attack trees. Graphical Models for Security - 7th International Workshop, GraMSec@CSF 2020, Boston, MA, USA, Virtual Conference, June 22, 2020, Revised Selected Papers. 2020. P. 45–64. URL: https://pape.science/paper/SSP20gramsec/ (date of access: 02.04.2024)

10. Information Security Risk Assessment / I. Kuzminykh et al. Encyclopedia. 2021. Vol. 1, no. 3. P. 602–617. URL: https://doi.org/10.3390/encyclopedia1030050 (date of access:04.04.2024).

11. Rausand M., Haugen S. Risk Assessment: Theory, Methods, and Applications. Hoboken: Wiley & Sons, Incorporated, John, 2020. 784 p.

12. Liberda E., Sly T. Qualitative Risk Assessment Methods. Assessment and Communication of Risk. 2023. P. 157–174. URL: https://www.researchgate.net/publication/372609732_Qualitative_Risk_Assessment_Methods (date of access: 10.04.2024).

13. Crotty J., Daniel E. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Applied Computing and Informatics. 2022. URL: https://www.researchgate.net/publication/366594576_Cyber_threat_its_origins_and_consequence_and_the_use_of_qualitative_and_quantitative_methods_in_cyber_risk_assessment (date of access: 10.04.2024).

14. Institute P. M. PMBOK Guide: The Project Management Body of Knowledge. San Francisco: Booksmith Publishing LLC, 2021. 368 p.

15. Kumar R. Quantitative safety-security risk analysis of interconnected cyber-infrastructures. Conference: 2022 IEEE 10th Region 10 Humanitarian Technology Conference (R10-HTC). 2022. URL: https://www.researchgate.net/publication/365106059_Quantitative_safety-security_risk_analysis_of_interconnected_cyber-infrastructures (date of access: 10.04.2024).

16. Hillson D. Quantitative Risk Analysis: Strengths and Weaknesses. PM World Journal. 2020. Vol. 9, no. 12. URL: https://pmworldlibrary.net/wp-content/uploads/2020/11/pmwj100-Dec2020-Hillson-quantitative-risk-analysis.pdf (date of access: 15.04.2024).

17. What's wrong with quantitative risk assessment? juliantalbot. URL: https://www.juliantalbot.com/post/what-s-wrong-with-quantitative-risk-assessment (date of access: 17.04.2024).

18. Freedom Path Financial. Understanding the Essence of Risk Assessment: Navigating Uncertainty with Precision. LinkedIn. URL: https://www.linkedin.com/pulse/understanding-essence-risk-assessment-navigating-undgf (date of access: 18.04.2024).

19. Cranenburgh N. Semi-quantitative risk assessment. REBOK Community. URL: https://rebok.engineersaustralia.org.au/wiki.html/semi-quantitative-risk-assessment-r51/ (date of access: 19.04.2024).

20. Edmond A. Which Risk Assessment methodology works for your organization? LinkedIn. URL: https://www.linkedin.com/pulse/which-risk-assessment-methodology-works-your-amel-edmond (date of access: 26.05.2024).

21. Shawgo E. 2 Approaches to Risk and Resilience: Asset-Based and Service-Based. Carnegie Mellon University, Software Engineering Institute's Insights (blog). 2023. URL: https://insights.sei.cmu.edu/blog/2-approaches-to-risk-and-resilience-asset-based-and-service-based/ (date of access: 19.04.2024).

22. George G., Thampi S. M. Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. Pervasive and Mobile Computing. 2019. Vol. 59. P. 101068. URL: https://doi.org/10.1016/j.pmcj.2019.101068 (date of access: 20.04.2024).

23. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions / Ö. Aslan et al. Electronics. 2023. Vol. 12, no. 6. P. 1333. URL: https://doi.org/10.3390/electronics12061333 (date of access: 26.04.2024).

24. What Are the Different Types of Risk Assessments? RiscOptics. URL:

https://reciprocity.com/resources/what-are-the-different-types-of-risk-assessments/ (date of access: 27.04.2024).

25. A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs / M. v. Haastrecht et al. Proceedings of the 16th International Conference on Availability, Reliability and Security. 2021. URL: https://dl.acm.org/doi/10.1145/3465481.3469199 (date of access: 28.04.2024).

26. Shevchenko N. Threat Modeling: 12 Available Methods. Carnegie Mellon University, Software Engineering Institute's Insights (blog). 2018. URL: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ (date of access: 02.05.2024).

27. The STRIDE Threat Model. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN (date of access: 02.05.2024).

28. Applying STRIDE. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee798544(v=cs.20) (date of access: 03.05.2024).

29. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process / R. A. Caralli et al. Fort Belvoir, VA: Defense Technical Information Center, 2007. URL: https://doi.org/10.21236/ada470450 (date of access: 06.05.2024).

30. Lachapelle E., Rama F. Risk Assessment with OCTAVE. ISO Training, Evaluation, and Certification. URL: https://pecb.com/whitepaper/risk-assessment-with-octave (date of access: 07.05.2024).

31. Security Assurance and Security Operations. Security Assurance and Security Operations. URL: https://infosec.mozilla.org/ (date of access: 07.05.2024).

32. OWASP Risk Rating Methodology | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security. URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (date of access: 07.05.2024).

33. RRA Methodology. RRA. URL: https://www.rra.rocks/docs/rapid_risk_assessment (date of access: 09.05.2024).

34. Jones J., Freund J. Measuring and Managing Information Risk: A FAIR Approach. Amsterdam: Elsevier Science & Technology, 2014. 408 p.

35. Добринін І. С., Мальцева Н. О. Вдосконалення методики факторного аналізу інформаційних ризиків. Системи обробки інформації. 2017. № 3(149). С. 146–150. URL: https://doi.org/10.30748/soi.2017.149.29 (date of access: 09.05.2024).

36. IT Risk Management Automation A Complete Guide. Berkeley: 5STARCooks, 2021. 308 p.

37. CyberArrow. Automating Risk Assessments: Saving Time and Improving Efficiency. LinkedIn. URL: https://www.linkedin.com/pulse/automating-risk-assessments-saving-time-improving-efficiency (date of access: 12.05.2024).

38. Автоматизація процесу управління ризиками - Visure Solutions. Visure Solutions. URL: https://visuresolutions.com/uk/risk-management-fmea-guide/automating-risk-management (дата звернення: 12.05.2024).

39. Risk Management Automation: What it is and how it can improve your cybersecurity? RiskOptics. URL: https://reciprocity.com/blog/what-is-risk-management-automation/ (date of access: 16.05.2024).

40. Comprehensive risk management - Scrut Automation. Scrut Automation. URL: https://www.scrut.io/products/risk-management (date of access: 16.05.2024).

41. Cyber Risk Management Platform | LogicGate Risk Cloud. LogicGate. URL: https://www.logicgate.com/solutions/it-security-risk/ (date of access: 16.05.2024).

42. Download Microsoft Security Assessment Tool 4.0 from Official Microsoft Download Center. Microsoft. URL: https://www.microsoft.com/en-us/download/details.aspx?id=12273 (date of access: 17.04.2024).

43. Soteria Software | FAQ. Soteria Software | Cyber Compliance Automation. URL: https://www.soteriasoft.com/products/faq.html (date of access: 20.05.2024).

44. GitHub - usnistgov/PrivacyEngCollabSpace: Privacy Engineering Collaboration Space. GitHub. URL: https://github.com/usnistgov/PrivacyEngCollabSpace/tree/master (date of access: 21.05.2024).

45. Collaboration Space. NIST. URL: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space (date of access: 24.05.2024).

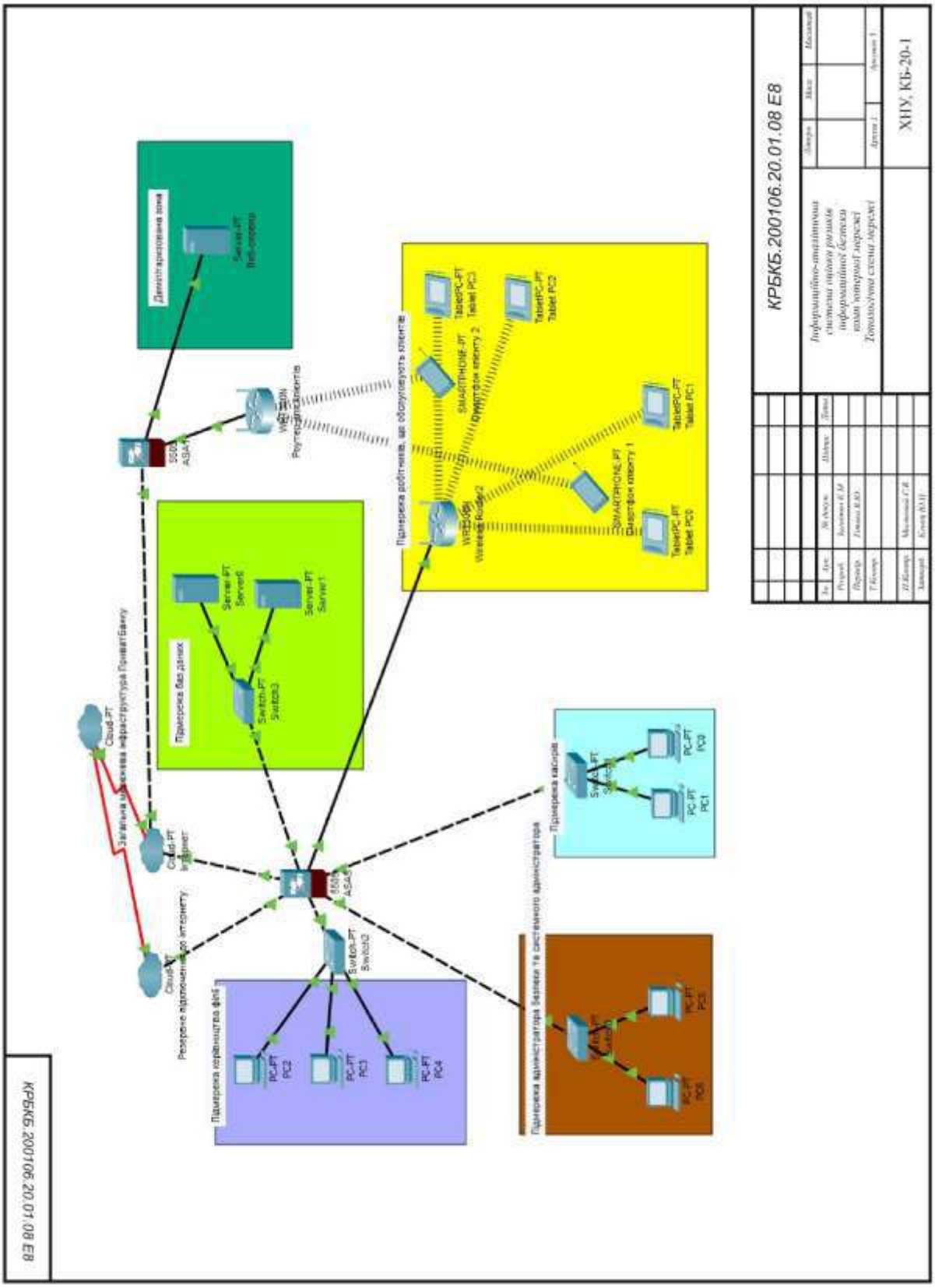
46. Calderon P. Nmap Network Exploration and Security Auditing Cookbook - Third Edition: Network Discovery and Security Scanning at Your Fingertips. Packt Publishing, Limited, 2021. 436 p.

47. Chapter 15. Nmap Reference Guide | Nmap Network Scanning. Nmap: the Network Mapper - Free Security Scanner. URL: https://nmap.org/book/man.html (date of access: 25.05.2024).

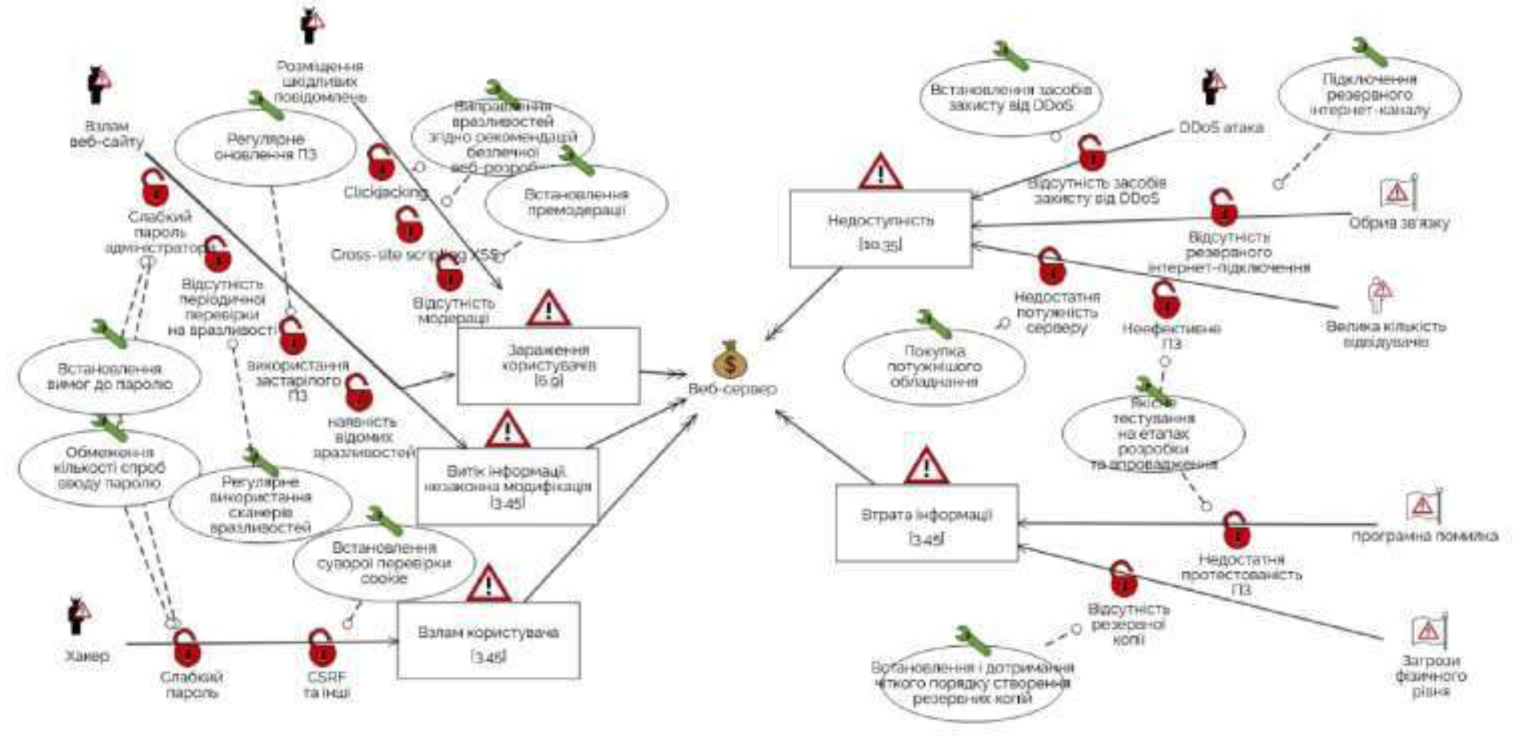
ДОДАТОК А

(обов’язковий)

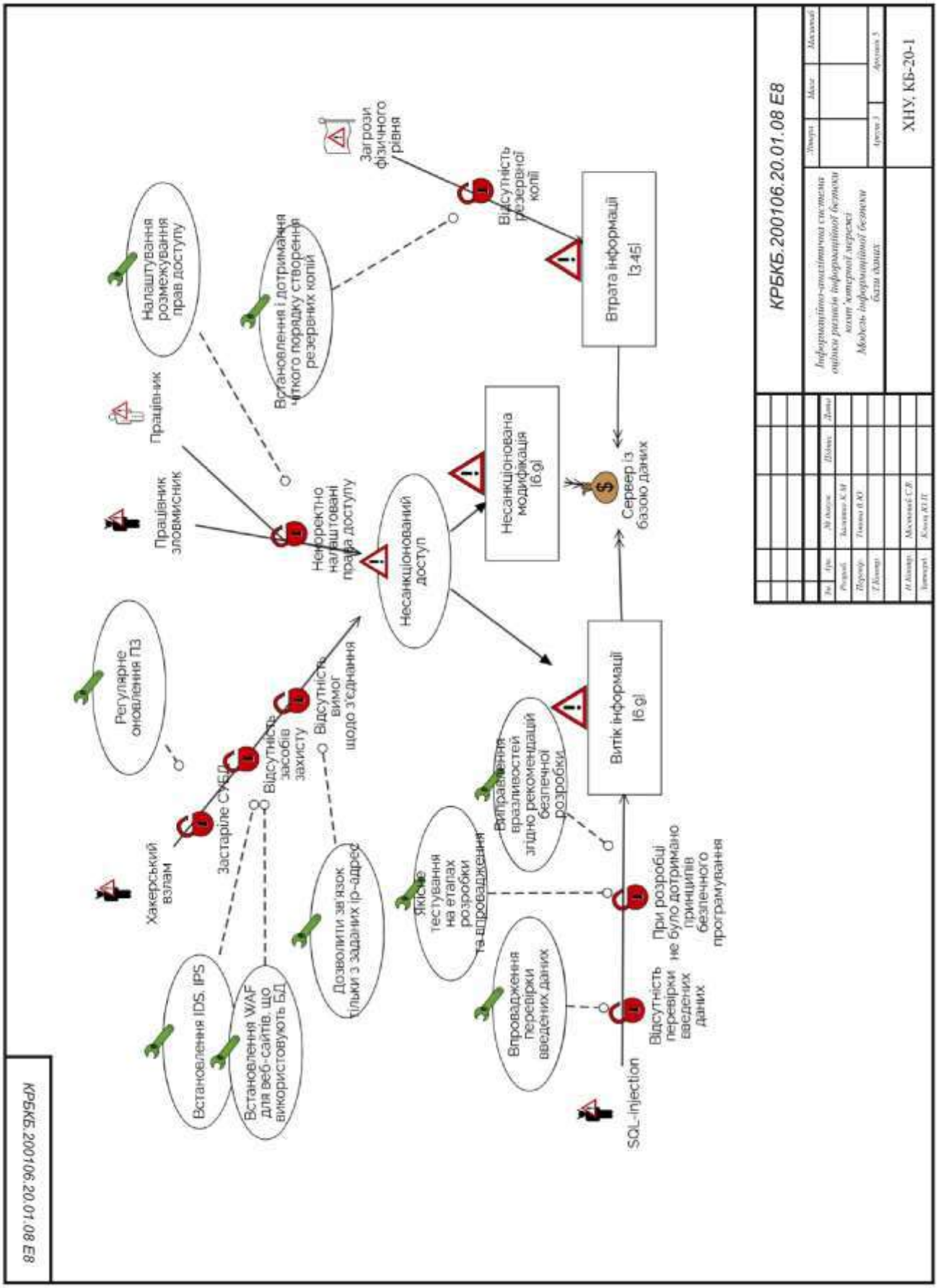
Копії графічної частини

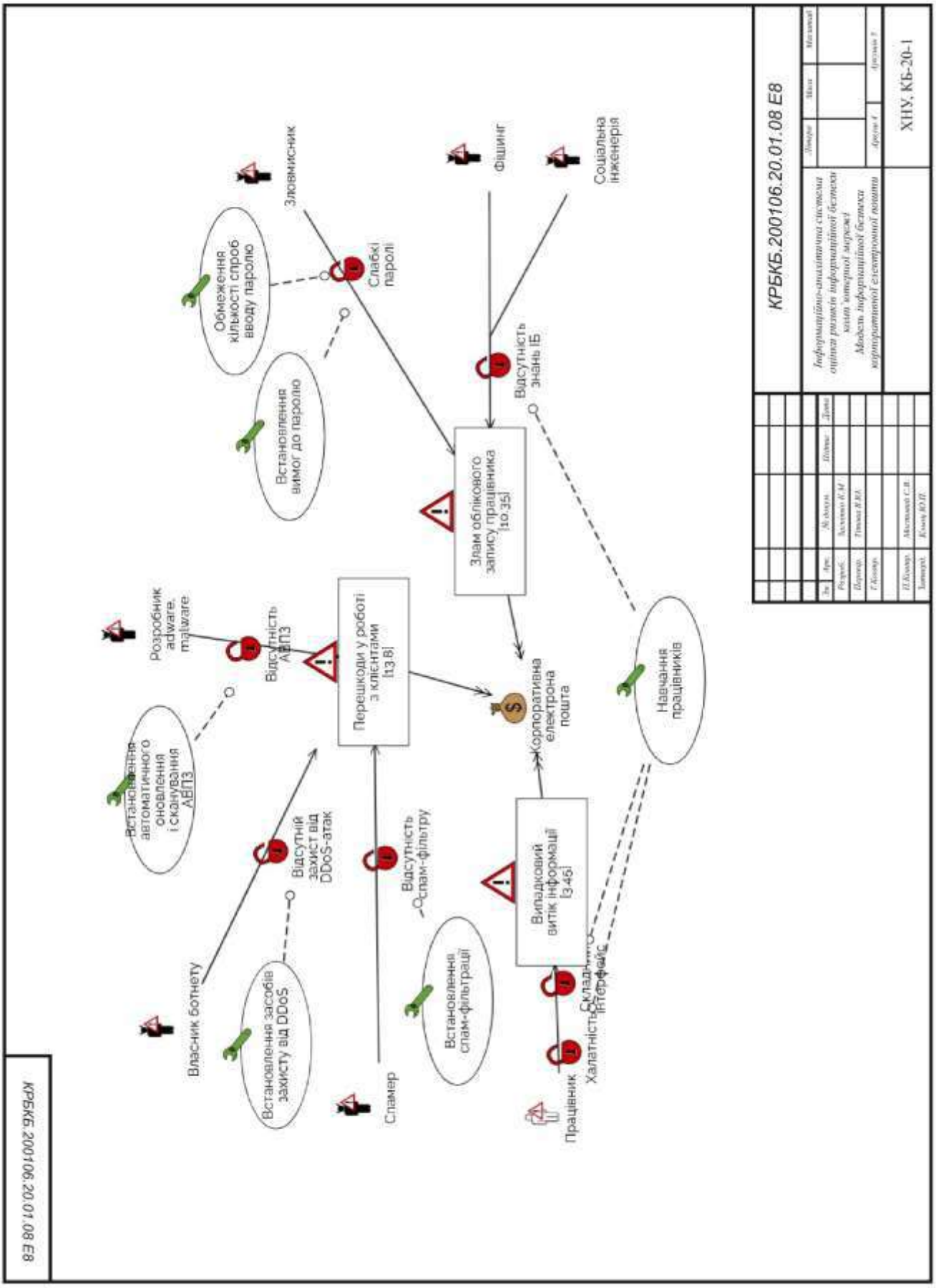


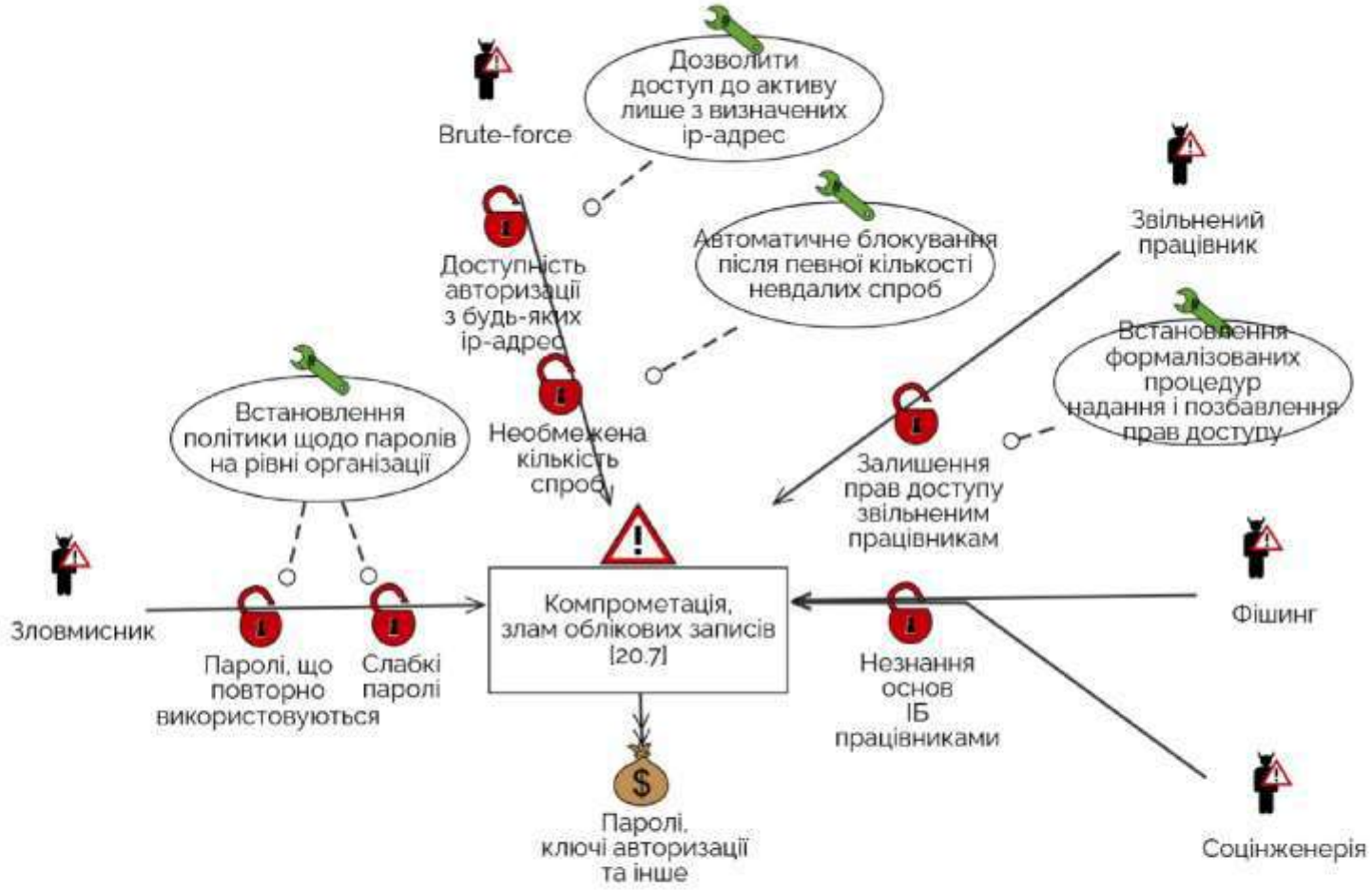
КРБКБ.200106.20.01.08 Е8



				КРБКБ.200106.20.01.08 Е8			
Зм.	Арк.	№ докум.	Підпис	Дата	Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі. Модель інформаційної безпеки веб-серверу	Літера / Маса / Масштаб	
Розроб.	Заплатні К.Н					Аркуш 2	Аркушів 3
Перевір.	Тітова В.Ю.						
Т.Контр.							
Н.Контр.	Мостовий С.В.					ХНУ, КБ-20-1	
Затверд.	Кліць Ю.П.						


КРБКБ.200106.20.01.08 Е8
Інформаційно-аналітична система оцінки рівнів інформаційної безпеки коли контент зберігається Модель інформаційної безпеки бази даних
ХНУ, КБ-20-1
Втрата інформації [3,4,5]
Несанкціонований доступ
Несанкціонована модифікація [6,g]
Витік інформації [6,g]
Сервер із базою даних
Працівник
Працівник зловмисник
Хакерський взлам
SQL-injection
Загрози фізичного рівня
Налаштування розмежування прав доступу
Встановлення і дотримання чіткого порядку створення резервних копій
Відсутність резервної копії
Некоректно налаштовані права доступу
Регулярне оновлення ПЗ
Застаріле ПЗ
Відсутність засобів захисту
Відсутність вимог щодо з'єднання
Встановлення IDS, IPS
Встановлення WAF для веб-сайтів, що використовують БД
Дозволити зв'язок тільки з заданих ip-адрес
Якісне тестування на етапах розробки та впровадження
Впровадження вразливостей згідно рекомендацій безпечної розробки
Впровадження перевірки введених даних
Відсутність перевірки введених даних
При розробці не було дотримано принципів безпечного програмування
КРБКБ.200106.20.01.08 Е8


КРБКБ.200106.20.01.08 Е8
Інформаційно-аналітична система оцінки рівнів інформаційної безпеки банківської установи
Модель інформаційної безпеки корпоративної електронної пошти
ХНУ, КБ-20-1
Зловмисник
Фішинг
Соціальна інженерія
Обмеження кількості спроб вводу паролю
Слабкі паролі
Встановлення вимог до паролю
Відсутність знань ІБ
Злам облікового запису працівника [10;35]
Розробник adware, malware
Відсутність АВПЗ
Перешкоди у роботі з клієнтами [13;8]
Корпоративна електронна пошта
Встановлення автоматичного оновлення і сканування АВПЗ
Відсутній захист від DDoS-атак
Відсутність спам-фільтру
Навчання працівників
Власник ботнету
Випадковий витік інформації [3;45]
Встановлення засобів захисту від DDoS
Спамер
Встановлення спам-фільтрації
Працівник
Халатність
КРБКБ.200106.20.01.08 Е8



						КРБКБ.200106.20.01.08 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Тютюнюк К.М.			Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі. Модель інформаційної безпеки облікових записів	Літера	Маса	Масштаб
Перевір.		Тютюнюк В.Ю.						
Т.Контр.						Аркуш 5	Аркушів 5	
Н.Контр.		Московський С.В.				ХНУ, КБ-20-1		
Затвердив		Клюєв Ю.Л.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Загнітка Костянтина Миколайовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

08 червня 2024 р.
дата

Загнітко
підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016347108

Дата перевірки:
11.06.2024 12:32:53 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
11.06.2024 22:33:25 EEST

ID користувача:
100008300

Назва документа: **Загнітко_плагіат**

Кількість сторінок: 67 **Кількість слів:** 10031 **Кількість символів:** 82156 **Розмір файлу:** 2.91 MB **ID файлу:** 1016148837

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

0.77%
Схожість

Найбільша схожість: 0.41% з джерелом з Бібліотеки (ID файлу: 1016148839)

0.47% Джерела з Інтернету	108	Сторінка 69
0.59% Джерела з Бібліотеки	35	Сторінка 69

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	5
Підозріле форматування	20 сторінок

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 6%**

	Документ		Сумарний збіг по Базі Даних	
ID: 129630 Назва: Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі Додано в БД: 2024-06-11 Автора: Загнітко К.М, Керівники: Тітова В.Ю. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	67905	1051	396 (1%)	5 (0%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Назва: Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі

Автор: Загнітко Костянтин Миколайович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 99,23%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Загнітко Костянтин Миколайович
Тема: «Інформаційно-аналітична система оцінки ризиків інформаційної безпеки комп'ютерної мережі»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3 ; кількість сторінок записки 76;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань, пов'язаних з розробкою інформаційно-аналітичної системи для оцінки ризиків комп'ютерної мережі. Для досягнення поставленої мети було досліджено предметну область, зібрано та проаналізовано теоретичну інформацію про існуючі методи оцінки ризиків у сфері інформаційних технологій. Робота має на меті покращити управління інформаційною безпекою для організацій.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було розглянуто існуючі методи та алгоритми оцінювання ризиків інформаційної безпеки, проведено їх порівняльний аналіз, що для постановки задачі кваліфікаційної роботи. У другому розділі було проаналізовано методи та засоби виявлення інформаційних загроз в комп'ютерних мережах, розроблено моделі інформаційної безпеки в комп'ютерній мережі, обґрунтовано вибір методу оцінювання ризиків інформаційної безпеки в комп'ютерних мережах. У третьому розділі наведено реалізацію інформаційно-аналітичної системи оцінювання ризиків інформаційної безпеки комп'ютерної мережі, проведено оцінювання її ефективності.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, у процесі реалізації системи було створено набір методів та засобів для виявлення загроз, розроблено моделі інформаційної безпеки, на основі яких було створено інформаційно-аналітичну систему оцінки ризиків. Створену систему було апробовано і оцінено ефективність реалізованої методики.

5. Негативні сторони кваліфікаційної роботи: -

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «відмінно/ А (4,75)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 10 » червня 2024 . (підпис)