Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента Нікіперовича Олександра Олексійовича

академічної групи 125м-22з-2

спеціальності 125 Кібербезпека

спеціалізації[1]

за освітньо-професійною програмою Кібербезпека

на тему: Дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web-сайту

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н., доц. Герасіна О.В.			
економічний	к.т.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро

2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____д.т.н., проф. Корнієнко В.І.
«__»_____ 20__ р.

З А В Д А Н Н Я
на кваліфікаційну роботу ступеня магістра

студенту Нікіперович Олександр Олексійович **академічної групи** 125м-22з-2

спеціальності 125 Кібербезпека

спеціалізації[1] _____

за освітньо-професійною програмою Кібербезпека

на тему: Дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web-сайту

Затверджену наказом ректора НТУ «Дніпровська політехніка»
від 09.10.23 № 1228-с

Розділ	Зміст	Термін виконання
Розділ 1	Літературний огляд за темою дослідження	01.12.2023
Розділ 2	Практичні аспекти захисту інформації Web-сайту	15.12.2023
Розділ 3	Економічна частина	30.12.2023

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Нікіперович О.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79 с., 10 рис., 8 табл., 39 джерел.

Об'єкт дослідження: новітні технології систем безпеки інформації Web-сайту.

Мета роботи: дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web-сайту.

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділу було розкрито основні положення теорії захисту інформації; запропоновано класифікацію заходів забезпечення безпеки Web-сайту; досліджено основні методи і засоби захисту інформації Web-сайту.

У спеціальній частині було виділено методи і засоби захисту інформації Web-сайту; висвітлено загальні аспекти побудови аналітичної системи захисту Web-сайту.

В економічному розділі визначено економічну доцільність розробки та впровадження методики для захисту інформації Web-сайту. Проведено розрахунок капітальних (фіксованих) витрат, поточних (експлуатаційних) витрат, загального збитку від атаки на Web-сайт та загального ефекту від впровадження рекомендацій.

Наукова новизна роботи полягає у комплексному рішенні по всіх рівнях захисту, щодо Web-сайту.

Практичне значення роботи полягає у впровадження засобів інформаційної безпеки по етапах розвитку Web-сайту.

ІНФОРМАЦІЙНА БЕЗПЕКА, WEB-САЙТ, ІНФОРМАЦІЯ, ІНЦИДЕНТ, КІБЕРБЕЗПЕКА, АТАКА, МЕТОДИКА, ЗАСОБИ.

ABSTRACT

Explanatory note: 79 p., 10 figures, 8 tables, 39 sources.

Research object: the latest technologies of information security systems of the Web site.

The purpose of the work: research of ways and development of recommendations for the protection of information on the Web site.

Development methods: observation, comparison, analysis, description.

In the first chapter, the main provisions of the theory of information protection were revealed; classification of website security measures is proposed; the main methods and means of protecting the information of the Web site were studied.

In a special part, the methods and means of protecting the information of the Web site were highlighted; the general aspects of building an analytical system for the protection of the Web site are covered.

In the economic section, the economic feasibility of the development and implementation of the methodology for the protection of information on the Web site is determined. The calculation of capital (fixed) costs, current (operating) costs, total damage from an attack on the Web site, and the total effect from the implementation of the recommendations was carried out.

The scientific novelty of the work consists in a comprehensive solution for all levels of protection for the Web site.

The practical significance of the work lies in the implementation of information security tools at the stages of Web site development.

INFORMATION SECURITY, WEBSITE, INFORMATION, INCIDENT, CYBER SECURITY, ATTACK, METHODOLOGY, TOOLS.

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ

ЕОМ	електронно-лбчислювальна машина
ІР	інформаційний ресурс
ІТС	інформаційно-телекомунікаційна система
ККА	канонічний кореляційний аналіз
КРМ	Кваліфікаційна робота ступеня магістра
ЛСА	латентний семантичний аналіз
ПІБ	підсистема інформаційної безпеки
РІТС	розподілена інформаційно-телекомунікаційна система
DER	Diarization Error Rate
JFA	Joint Factor Analysis
LAN	Local-Area Networks
LFCC	Linear Frequency Cepstral Coefficients
MFCC	Mel Frequency Cepstral Coefficients
MIMD	Multiple Instruction Multiple
OGSA	Open Grid Services Architecture
SIMD	Single Instruction Multiple
SVM	Support Vector Machine
UBM	Universal Background Model
VAD	Voice Activity Detector
WAN	Wide Area – Wide-Area Networks
WSRF	Web Services Resource Framework

ЗМІСТ

ВСТУП

Актуальність дослідження. Становлення інформаційного суспільства пов'язано з широким розповсюдженням персональних комп'ютерів, побудовою глобальної інформаційної мережі та підключення до неї великого числа користувачів. Ці досягнення повинні докорінно змінити життя суспільства, висунувши на передній план діяльність, пов'язану з виробництвом, споживанням, трансляцією і збереженням інформації.

Однією з найбільш серйозних проблем, що ускладнюють застосування інформаційних технологій, є забезпечення інформаційної безпеки.

Інформаційна безпека – такий стан розглянутої системи, при якому вона, з одного боку, здатна протистояти дестабілізуючому впливу зовнішніх і внутрішніх загроз, а з іншого – її функціонування не створює інформаційних загроз для елементів самої системи і зовнішнього середовища.

Загроза безпеці інформації – сукупність умов та факторів, що створюють потенційну або реально існуючу небезпеку, пов'язану з витоком інформації або несанкціонованими і ненавмисними діями на неї.

Комп'ютерна революція допомогла інформації стати центром уваги основоположних поглядів. Визнання інформації основою життя навряд чи зводиться до внутрішніх мотивацій. Соціальні, економічні та політичні науки в спробах усвідомлення змін, що відбуваються звертають пильну увагу на комп'ютерну інформацію, як на новий фактор глобального впливу.

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку української інформаційної інфраструктури, для реалізації конституційних прав і свобод людини і громадянина в області отримання інформації і користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності України, політичної, економічної та соціальної стабільності, в безумовному забезпеченні законності і правопорядку, розвитку рівноправного і взаємовигідного міжнародного співробітництва.

Захист інформації – це діяльність, спрямована на запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається.

Враховуючи вищевикладене тема кваліфікаційної роботи «Дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web-сайту» є актуальною.

Метою даної роботи є дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web-сайту. Для досягнення поставленої мети у роботі необхідно виконати наступні ***завдання***:

- розкрити методологію захисту інформації Web-сайту;
- навести практичні рекомендації захисту інформації Web-сайту;
- виконати верифікацію результатів;
- запропонувати розрахунок капітальний витрат на придбання і налагодження складових систем інформаційної безпеки та річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;
- навести визначення річного економічного ефекту від впровадження об'єкта проектування та аналіз показників економічної ефективності запропонованого проектного рішення;
- представити висновок про економічну доцільність проектного рішення.

Об'єкт та предмет дослідження. Об'єктом роботи виступають новітні технології систем безпеки інформації Web-сайту.

Предметом є процес дослідження методів та засобів захисту інформації Web-сайту.

Наукова новизна та практична значущість результатів роботи полягає в наступному:

- уперше запропоновано комплексне рішення по всіх рівнях захисту, щодо Web-сайту;

– наведено методи аналізу середовища Web-сайту: формування хронологічної послідовності типових впливів базових факторів середовища для їх подальшого аналізу й прогнозу;

– дістало подальшого розвитку вивчення та розробка методів впровадження універсальних засобів інформаційної безпеки у межах Web-сайту.

Отримані результати можуть бути використані у межах організацій для впровадження засобів інформаційної безпеки по етапах.

***Основними результатами роботи є*:**

– розкриття основних положень теорії захисту інформації;

– проведення класифікації заходів забезпечення безпеки Web-сайту;

– дослідження основних методів і засобів захисту інформації Web-сайту;

– виділення методів і засобів захисту інформації Web-сайту.

– висвітленні загальних аспектів побудови аналітичної системи захисту Web-сайту.

Структуру роботу складають вступ, три розділи, висновки, список використаної літератури яка була використана, додатки.

РОЗДІЛ 1
ЛІТЕРАТУРНИЙ ОГЛЯД ЗА ТЕМОЮ ДОСЛІДЖЕННЯ

1.1 Поняття Web-сайту, структура, сутність

WEB-розробка (web development) – це процес професійного програмування сайту, який регулює всі наступні етапи, пов'язані з формуванням HTML-коду, додаванням різних функціональних компонентів та скриптів, що впливають на показники юзабіліті та технічної стабільності.

Завданням розробника є створення інфраструктури для реалізації оптимального функціоналу сайту, на який у майбутньому кріпляться візуальні компоненти, що забезпечують інтерактивні можливості.

Якщо сказати іншими словами, більш доступною мовою, то WEB-розробка – це процедура створення WEB-програми або WEB-сайту.

Попереднє визначення етапів роботи над унікальним проектом дозволяє вирішити більшість проблем у процесі взаємодії між клієнтською стороною та виконавцем, оскільки чіткий план дій показує замовнику, які основні дії необхідні для створення повноцінного робочого ресурсу, відповідно до його вимог.

Спочатку передбачається визначити призначення сайту, які завдання він повинен вирішити. Цей етап можна позначити як визначення цілі веб-сайту. Цілі проекту визначаються результатами відповіді замовника на питання «яку проблему проект повинен вирішити?». У випадку, якщо цей замовник затрудняється, відповісти на питання, велика ймовірність, що робота виконавця буде незадоволена, а тимчасові та грошові витрати на розробку проекту будуть невиправдані.

Не менш важливим етапом є визначення цільової аудиторії веб-ресурсу. Цільова аудиторія представляє собою коло осіб із подібними визнаннями, на задоволення потреб яких і буде спрямовано вміст веб-ресурсу. Визначення портрета цільової аудиторії впливає не тільки на

контент ресурсу, але і на те, яким чином буде представлена інформація: стилістика написання текстів, дизайн сайту.

Перед тим як перейти до проектування ресурсу, необхідно провести підготовчу роботу, а саме – аналіз подібних ресурсів-конкурентів. Необхідно проаналізувати переваги, недоліки даних сайтів, оцінити їх функціональність, особливості. У подальшому це допоможе при визначенні основних розділів ресурсу, способів залучення та утримання цільової аудиторії.

Наступним етапом є визначення ключових фраз – пошукових запитів, за якими цільова аудиторія може знайти майбутній ресурс у пошукових системах. Інакше цей процес можна назвати складанням семантичного ядра [1]. Очевидно, що ресурс замовника користувачі мережі Інтернет будуть шукати за тими же, або схожими ключовим фразам, що і ресурси конкурентів. Також варто проаналізувати, які питання частіше всього виникають у потенційних клієнтів замовника при зверненні в організацію.

Далі слід перейти до розробки важливого документа, в якому виражені всі вимоги до створюваного ресурсу, умови та порядок виконання робіт виконавцем. Таким документом є технічне завдання. В ньому слід відобразити ціль, завдання проекту, описати цільову аудиторію. Також описати структуру сайту, кількість розділів, сторінки в кожному з розділів, динамічні та статичні елементи. Немало важливим є відображення побажань замовника щодо дизайну сайту, його наповнення. Крім того, необхідно описати, які технології будуть використані при проектуванні та розробці ресурсу. Значно спростить процес взаємодії із замовником визначення порядку надання інформації для наповнення сайту.

Технічне завдання – основа для виконання всіх наступних етапів робіт. Тому слід віднестись до написання документа досить відповідально. Важливо зрозуміти, що це завдання не розробника або замовника, зокрема, а спільна робота. Замовник визначає цілий сайт, цільову аудиторію, надає

побажання щодо функціонування та виконання, а виконавець у свою чергу описує те, яким чином буде функціонувати проектований ресурс.

Після узгодження ТЗ із замовником слід перейти до визначення зовнішнього виду майбутнього сайту. Спочатку бажано створити прототипи ресурсу. Прототипування передбачає створення чорного макету, що відображає базову функціональність сайту. Прототип показує, яким чином буде розміщено контент на сторінках.

Погодження із замовником прототипу сайту перед тим, як приступити до розробки дизайну, дозволяє уникнути більшої кількості правок на вже готовий дизайн-макет.

Далі на основі узгодженого прототипу дизайнер приступає до розробки дизайн-макету сайту. Дизайн-макет відображає повноцінний зовнішній вигляд сторінки сайту з урахуванням усіх графічних і текстових елементів. Обов'язковою умовою є відповідність дизайн-макету вимогам до зовнішнього виду сайту, описаним у ТЗ.

Після того, як дизайн сайту підтверджено замовником, проводиться робота по верстці веб-сторінки. Верстка передбачає розміщення графічних, текстових та інших елементів веб-сторінки відповідно до дизайн-макету. У цьому етапі важлива участь, яким чином будуть відображатися елементи в різних браузерах, на різних дозволах екрана.

Після приведення елементів веб-сторінки до коректно-відображуваного виду починається процес програмування сайту. Визначається порядок роботи динамічних елементів, розставляються гіперсилки, розробляється логіка обробки дій користувача на сайті, інтерфейс адміністрування ресурсу та ін.

Далі коректно відповідаючий на запити користувача сайт наповнюється контентом, наданим замовником. Строк наповнення інформації ресурсу залежить не тільки від кількості сторінок сайту, але й від того, в якому вигляді та наскільки якісна інформація була надана виконавцю.

Після того, як файли сайту розміщені на хостингу в мережі Інтернет, проводиться тестування сайту [2]. Це передбачає виявлення недоліків і

помилок, допущених на стадіях верстки, програмування сайту. Строк тестування так само залежить від обсягу і складності виготовлених робіт, зазвичай займає 2-4 неділі.

У результаті аналізу інформації з розробки сайтів були виявлені основні етапи цього процесу. У залежності від особливостей проекту порядок етапів може змінюватися, можливо паралельне виконання процесів. Описаний план дій дозволяє не тільки спростити процес роботи із замовником, але й процес взаємодії команди розробників з іншим.

В якості примітки слід зазначити, що WEB-дизайн сайту, що розробляється, неодмінно зобов'язаний привабливо виглядати при використанні користувачами різних браузерів, особливо це стосується таких браузерів, як Chrome, Internet Explorer, Firefox і Opera.

Front-end розробка стосується управління клієнтським аспектом або зовнішнім інтерфейсом веб-сайтів. Це охоплює все, що бачить користувач, від тексту та зображень до меню та панелей навігації. За це відповідають фронтенд-розробники.

Інтерфейсний розробник читає файл дизайну і складає план перетворення цього дизайну на допустимий код HTML, CSS і JavaScript. Потім веб-браузер відображає цей код, коли користувач здійснює перехід на веб-сайт. HTML, CSS та JavaScript – це три основні мови програмування, які використовуються для створення зовнішнього інтерфейсу веб-сайту.

Основний обов'язок фронтенд-розробника – створити функціональний інтерфейс користувача. Користувачі повинні мати можливість легко переміщатися сайтом і отримувати відповіді, які вони шукали до того, як клацнути на сайт. Користувачі не повинні стикатися з помилками чи невідповідностями у процесі.

Існують різні області веб-розробки, і розробники, що працюють у кожній із них, мають унікальні обов'язки.

Веб-розробників серверної частини більше цікавить частина веб-сайту, яку користувач не бачить. Коди, які вони пишуть, можуть бути використані

для обробки платежів на сайті або визначення контенту, який користувач бачить при відкритті сторінки. Для цього вони використовують мови програмування, такі як Python, Ruby та PHP, для створення програми.

Розробники повного стеку – мають досвід і знання з обох сторін веб-сайту.

Веб-розробники повного стеку мають вирішальне значення для будь-якого веб-проекту. Вони допомагають подолати розрив між клієнтською та серверною частиною веб-сайту. Це тягне за собою забезпечення функціональності та естетичності сайту. Звичайно, вони володіють як клієнтськими інструментами, такими як JavaScript, і серверними технологіями, такими як PHP і Ruby.

Терміни «інтерфейсний інженер» та «інтерфейсний розробник» часто використовуються як синоніми. Хоча їхні обов'язки схожі, між цими кодувальниками є кілька тонких відмінностей.

Інтерфейсні інженери більше залучені до створення зовнішнього інтерфейсу сайту. Більшість часу вони проводять за аналізом архітектури сайту. За допомогою інших розробників та дизайнерів вони з'ясовують, як продати сайт.

З іншого боку, розробники зовнішнього інтерфейсу відповідають за написання коду зовнішнього інтерфейсу. Їхній код повинен бути підтримуваним і добре працювати в масштабі.

Хоча розуміння принципів дизайну, що лежать в основі сайту, є частиною обов'язків фронтенд-розробників, вони не витрачають багато часу на їх аналіз. Натомість вони приділяють більше уваги перетворенню макетів дизайну на код.

Розробникам зовнішнього інтерфейсу необов'язково бути експертами з веб-дизайну. Веб-дизайн – це окрема область. З урахуванням сказаного ключовим моментом є глибоке знання веб-дизайну. Дві основні частини веб-дизайну – це дизайн інтерфейсу користувача (UI) і (UX) "користувацький

досвід". Простими словами, це те, як користувач взаємодіє з інтерфейсом і наскільки сайт або додаток для нього зрозумілі і зручні.

Дизайн інтерфейсу користувача відноситься до створення зовнішнього вигляду веб-сторінки. Дизайнер інтерфейсу користувача вирішить, де на веб-сайті будуть відображатися такі елементи, як кнопки, текст і зображення.

UX-дизайн стосується іншого досвіду користувача на веб-сайті. Дизайнери інтерфейсу користувача аналізують і досліджують продукт, щоб визначити будь-які моменти, які можуть збентежити користувачів. Потім вони з'ясовують, як вирішити ці проблеми, щоб користувачі могли без проблем використовувати веб-сайт.

Люди використовують мобільні телефони, планшети та монітори з екранами різного розміру. Саме тут на допомогу приходить адаптивний дизайн. Адаптивний дизайн пов'язаний із створенням веб-сайту, який ефективно відображається на різних пристроях.

Це включає розуміння різних типів пристроїв, на яких користувач може переглядати сайт. Розробники зовнішнього інтерфейсу повинні мати можливість розробляти унікальні можливості для користувачів цих пристроїв.

Інтерфейси прикладного програмування (API) використовуються у різних контекстах веб-розробки. Часто серверні розробники створюють API-інтерфейси, які підтримують логіку сайту, таку як автентифікація користувачів та платежі. Потім розробники зовнішнього інтерфейсу повинні запитати ці API, щоб вони могли взаємодіяти з ними.

API також дозволяють взаємодіяти із зовнішніми службами. Наприклад, Google Sheets API дозволяє отримувати дані з Google Sheets, які можна використовувати на своєму веб-сайті. Це означає, що є можливість створювати інтеграцію поверх існуючого веб-сайту.

Тим часом робота з дизайнерами має вирішальне значення для розуміння того, як має виглядати сторінка. Не кажучи вже про всіх інших

людей, з якими потрібно взаємодіяти, від менеджерів проектів та інженерів із забезпечення якості до клієнтів.

1.2 Інциденти мережі

Світовий досвід створення різних захисних систем незмінно показує: як тільки людство відкриває нові засоби захисту, тут ж знаходяться джерела протидії і руйнування [1]. Вік інформатизації не став винятком. Від розробників новітніх технологій, не відстають зловмисники, які прагнуть знайти уразливості, створюючи засоби загроз і атак. Сучасне підприємство вже не може існувати без захищеної, належним чином, інформаційної системи. На сьогоднішній день інформація стає найбільш цінним ресурсом будь-якої компанії: витік важливих даних про клієнтів або фінансових відомостей може завдати непоправної шкоди репутації і подальшої комерційної діяльності організації [2-4].

Однак при всій значущості захисних систем, залишаються нерозв'язаними багато проблем. Серед них, насамперед, варто зазначити проблему витоку корпоративної інформації, і її подальше незаконне використання третіми особами. Загроза може виходити як від неуважного співробітника, так і від партнерів по бізнесу, клієнтів або підрядників. Для того щоб оптимізувати захист інформаційного середовища та знизити число неминуче виникаючих інцидентів (інцидент – від лат. incidens – випадок, пригода, подія (зазвичай неприємна); зіткнення), необхідно звернутися до методологічної бази управління інцидентами, як існуючої в Україні, так і з урахуванням зарубіжного досвіду [5].

Інцидент, згідно вимог IT Infrastructure Library (ITIL), – будь-яка подія, яка не є частиною нормальної роботи послуги і провідна чи здатна призвести до зупинки або втрати рівня якості цієї послуги [6].

Згідно ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016) «інцидент інформаційної безпеки (information security incident): одна або серія

небажаних або несподіваних подій інформаційної безпеки, які мають значну ймовірність компрометації бізнес-операції і загрожують інформаційній безпеці» [39]. Модель інциденту інформаційної безпеки наведена на рис. 1.1.

Рисунок 1.1 – Модель інциденту інформаційної безпеки [7, 8]

Міжнародний стандарт ISO 27001:2013 звертає особливу увагу на «необхідність створення процедури управління інцидентами інформаційної безпеки – очевидно, що без своєчасної реакції на інциденти безпеки та усунення їх наслідків неможливе ефективне функціонування системи управління інформаційною безпекою». На жаль, в процесі аудиту різних інформаційних систем доводиться стикатися з безліччю проблем реєстрації та розслідування інцидентів, які свідчать про те, що стандартам на підприємствах приділяється дуже мало уваги [9-16]. Наприклад, у корпоративній мережі однієї з компаній з'явився новий обліковий запис користувача з привілейованими повноваженнями. У процесі розслідування з'ясувалося, що пароль від єдиного адміністративного облікового запису знають кілька адміністраторів, а на контролері домену не ведуться журнали реєстрації подій, тому дізнатися, хто створив обліковий запис, і розслідувати даний інцидент виявилося неможливо. При цьому користувач, який буде заходити під новим привілейованим обліковим записом, може виконувати в системі будь-які дії, переглядати, змінювати або видаляти інформацію, зупиняти або модифікувати роботу сервісів.

Виділяють 2 типи мережевих атак:

Зовнішні атаки: виконується групою хакерів або індивідуалами, які володіють технікою для виконання атаки. Виконується атака шляхом сканування системи та збором інформації. Для запобігання атакам можна виконувати трасування портів на комутаторах, до яких приєднані чужі пристрої та блокування даних портів;

Внутрішні атаки: виконуються колишніми або чинними співробітниками компанії. Один із способів захисту є розгортання системи виявлення вторгнень (IDS) та конфігурування її для сканування системи на предмет як зовнішніх, так і внутрішніх атак.

Ніхто «в лоб» зламувати систему не буде. Насамперед хакер намагається зібрати якомога більше інформації про мережу, далі він створює карту мережі для виявлення відкритих портів, типу операційних пристроїв і так далі. Хакер здійснює збір інформації про компанію по доменному імені, що використовується IP адресою, тестування хостів у блоці IP адрес, використовує такий інструмент як Nmap, які дозволяє визначити, які операційні системи використовуються. Далі зломщик здійснює сканування портів з метою знайти відкриті. Це може зробити за допомогою стробування: коли атакуючий намагається приєднатися до діапазону портів, які відкриті на хостах з операційними системами Linux, Windows. Для сканування портів використовується такий метод як розгортка, тобто величезний набір IP-адрес сканується з метою знайти хоча б один відкритий порт. Також трафік може копіюватися повністю, а потім аналізуватися для пошуку відкритих портів. Використовується такий метод, як перебір. Атакуючий намагається зламати користувацькі облікові записи, як правило, це облікові записи «за замовчуванням», які не мають паролів, і проводить збір інформації по додатках на мережі. Для отримання доступу до системи програми типу Троян або спеціальні програми для зламування пароля (Wi-Lomster). Існує такий тип атак, як ескалація привілеїв, тобто зломщик із мінімальними правами намагається піднятися до привілеїв адміністратора, для контролю над

системою. Це можна зробити за допомогою документів з інформацій про адміністративні права, паролі та ключі для реєстрації паролів.

Порушення роботи бездротової мережі може викликати атаку типу Відмова в Обслуговуванні, основне завдання якої не дати нормально користуватися ресурсом. Ця атака може відправляти в мережу велику кількість некоректних даних, запитів, внаслідок чого мережа стає перевантаженою, фізично ушкоджуватиме мережу.

Розглянемо варіанти, які допоможуть захистити бездротову мережу від хакінгу:

1. SSID Cloaking – приховування імені мережі. Доступ дозволяється лише клієнтам, які знають це ім'я.

2. MAC Filtering – фільтрація за MAC адресами. Доступ дозволяється лише клієнтам, адреси мережевих адаптерів яких записані у точці доступу.

Ці два методи допоможуть обмежити доступ до мережі, тобто, але навіть якщо всі ці засоби включені на точці доступу, зловмисник зможе, увімкнувши свій бездротовий адаптер у «monitor mode», слухати ефір і виловлювати всю інформацію, що передається. Наступні методи криптографічно захищають дані:

1. WEP – статистично найвикористаніший метод захисту бездротової мережі. Надає шифрування всіх даних, що передаються по мережі. Аутентифікації як такої не має – якщо користувач не знаєте ключа, він не зможе розшифрувати дані. Мінуси методу дуже слабкий алгоритм, ключ зламується дуже швидко.

2. WPA та WPA2 Pre-Shared Key – сильна система аутентифікації та шифрування даних. Доступ здійснюється через загальний ключ. Рівень захисту дорівнює складності загального ключа, оскільки система схильна до brute force атак.

3. WPA та WPA2 Enterprise – варіант попередньої системи, але для підтвердження особистості використовується зовнішній автентифікатор 802.1x EAP, що дозволяє використовувати сертифікати, смарт-карти тощо.

Існують атаки з використанням сніфферів (Sniffer attacks): атаки сніфінгу – це процес, коли атакуючий використовує спеціальні програми для перехоплення та аналізу мережевого трафіку. Сніфери перехоплюють, копіюють мережну інформацію, як, наприклад, паролі та відкриті дані користувача. Якщо хтось має фізичний доступ до мережі, він може легко встановити аналізатор протоколів у мережу та копіювати трафік. Можна виділити такі сніфери, які часто використовуються атакуючими:

- Dsniff
- Ethereal
- Sniffit
- Snort
- Windump.

Для захисту від сніфера використовують шифрування трафіку, наприклад, за допомогою IPSec (Internet Protocol Security). В даному випадку ніякий перехоплений пакет не може бути інтерпретований доступною формою.

Атаки на паролі (Password attacks): найчастіше засновані на доборі паролів для системи поки що не буде визначено вірний. Одне з основних слабких місць у безпеці, пов'язаних з контролем доступу за паролями, - те, що підхід заснований на корпоративному ідентифікаторі користувача (user ID) та на будь-якому паролі. Деякі старі програми не захищають паролі, що передаються. У такому разі паролі просто відправляються як звичайний текст (не використовується жодна форма шифрування). Величезна небезпека, коли користувач використовує одні й ті ж логін та пароль до всіх систем. Тоді атакуючий відразу отримує доступ до цілої низки систем.

Отже, важливо захищати не тільки системи користувача, але й сховища з резервними копіями, оскільки при зломі можлива переустановка систем безпеки. Крім того, важливо визначити систему визначення вторгнень для збору даних, що постраждали і хто за цим стоїть. Для захисту цілісності даних, що передаються по мережі, можна використовувати цифрові підписи,

для збереження даних та їх достовірності, постійне резервне копіювання інформації, встановлення антивірусного програмного забезпечення, використовувати довгі паролі, конфігурування фільтрів на маршрутизаторах.

1.3 Методологічні основи захисту

Методи захисту від атак на VoIP доцільно розглядати як спеціалізовані та загальні.

Спеціалізовані методи захисту від атак складаються з чотирьох, отриманих на основі аналізу Best Practices.

ЗС_1. Відмова від підключення до загальнодоступного Wi-Fi

Метод призначений для захисту даних та з'єднань за рахунок обмеження свободи підключення користувача до загальнодоступних мереж Wi-Fi. Метод може бути реалізований як на рівні безпекових політик, так і програмними засобами. Метод дозволяє запобігти таким атакам, як SPIT, MITM, Dos і підбір ключів, оскільки знизить для зловмисника можливість отримати нелегітимний доступ.

ЗС_2. Розділення мережі даних та мережі телефонії

Метод спрямований на розмежування складових корпоративної мережі на VoIP та IP мережі як для виключення сторонніх загроз та спрощення їх пошуку, так і для розвантаження мережі VoIP від непотрібних широкомовних запитів QoS або VLAN. Метод дозволить запобігти поширенню вірусів або стороннього доступу з IP до мережі VoIP.

ЗС_3. Об'єднання підрозділів компанії у загальну VPN мережу

Суть методу полягає в підключенні користувачів VoIP через VPN, що призводить до того, що абоненти отримують доступ до віртуального та шифрованого VoIP каналу всередині мережі. Найчастіше VoIP-сервер розташований у хмарі і, отже, зловмисники можуть реалізовувати перехоплення даних, DDoS-атаки та несанкціонований доступ до корпоративної мережі. Застосування методу знизить подібні атаки.

ЗС_4. Використання спеціалізованого програмного забезпечення для протидії перебору паролів

Метод заснований на використанні такого ПЗ, як Fail2Ban та SSHGuard, які блокують IP-адреси користувачів при перевищенні розвішеної кількості спроб доступу. Даний метод запобігає атакам типу «грубою сили», що не дає зловмиснику здійснити підбір пароля до VoIP-серверу. Використання такого ПЗ є досить поширеною практикою для мережевих адміністраторів.

Загальні методи захисту від атак складаються з наступних десяти, одержаних на основі аналізу наукових статей [10, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23].

ЗО_1. Забезпечення комп'ютерної грамотності користувачів

Метод передбачає навчання користувачів базовим навичкам безпечної роботи з інформацією, таким як застосування надійних паролів, робота в сучасній ОС з оновленнями (тобто мають актуальні виправлення вразливостей), використання антивірусного ПЗ, захист від соціальних атак і т. п. Метод здатний виключити безліч атак, як на VoIP, так і на IP мережі на початкових етапах проведення та підвищити загальну безпеку корпоративної мережі.

ЗО_2. Керування доступом та перевірка на відповідність приладдя мережі

Метод полягає у розмежуванні прав доступу та перевірці на відповідність належності пристрою даної локальної мережі; поділ мереж Wi-Fi на гостьову та внутрішню, виділення прав доступу користувачів, безпечна (багатофакторна) автентифікація, комутована передача даних та номерний план. Метод забезпечує можливість попередження несанкціонованого доступу, що потенційно веде до тріади загроз інформаційній безпеці – порушення конфіденційності, цілісності та доступності [24, 25].

ЗО_3. Застосування планів маршрутизації та дзвінків

Аналогічно плану маршрутизації в IP мережах, у VoIP є так званий номерний план (перев. на англ. dialplan), за допомогою якого система має

порядок дій за певного сценарію дзвінків: передавати їх далі, зберігати, відповідати самостійно, блокувати та ін. Це дозволяє виключити з небажаного трафіку, заблокувати заборонені напрями викликів та запобігти таким атакам, як спам, DDos та фармінг. Застосування методу дозволить здійснювати своєчасний захист у разі злому сервера, або принаймні мінімізувати шкоду.

ЗО_4. Захист BYOD/мобільних пристроїв

Використання одного пристрою для особистих та робочих цілей призводить до перемішування корпоративної та персональної інформації співробітника, що ускладнює контроль над даними. Як результат, можливі ризики у вигляді підключення до незахищеної мережі Wi-Fi, скачування та встановлення шкідливого ПЗ, крадіжки або втрата пристрою з даними і т.п. хмарі, а не на власному пристрої.

ЗО_5. Впровадження криптосистем та протоколів шифрування

Метод полягає у шифруванні трафіку (IP або VoIP) при його передачі в мережі, що, очевидно, суттєво ускладнює його компрометацію під час перехоплення (наприклад, у процесі атаки MITM). Найчастіше застосовуваними цього протоколами є SSH, TLS, SMTP, IPSEC і SRTP.

ЗО_6. Застосування програмних та апаратних міжмережевих екранів

Суть методу полягає в налаштуванні мережного екрану таким чином, щоб він обслуговував лише свідомо довірені пакети та напрямки їх передачі. Можливою реалізацією методу є застосування спеціально налаштованих ланцюжків правил. Так, наприклад, типовим захистом АТС на базі Asterisk є використання правил фільтрації та перенаправлення пакетів за допомогою утиліти iptables. Так, щоб до сервера Asterisk могли підключатися IP-телефони з внутрішньої мережі, то необхідна наявність відповідного правила. Коректне та повне налаштування правил зведе практично на нуль ймовірність отримання доступу зловмисника до VoIP-сервера

ЗО_7. Моніторинг підозрілої активності та впровадження системи виявлення та запобігання вторгненням

Метод ґрунтується на постійному моніторингу підозрілої активності робочих пристроїв мережі (наприклад, за допомогою SIEM-систем). Також, метод включає виявлення і запобігання вторгнень (наприклад, за допомогою IPS/IDS систем) в результаті проведення атак зловмисником [26]. Даний метод здатний виключити безліч атак, що використовуються у своїй схемі маніпуляції зі службовим трафіком і даними (наприклад, атаки типу грубої сили, DoS, використання вразливостей і шкідливого ПЗ, неавторизований доступ і підвищення привілеїв користувача, і т. п.).

ЗО_8. Резервне копіювання та відновлення конфігурацій системи

Метод полягає у відновленні системи, що перестала працювати, для чого, зокрема, потрібне її резервне копіювання. Наприклад, якщо АТС не функціонує через збій після DoS-атаки, її коректна конфігурація може бути відновлена з резервної копії.

ЗО_9. Використання інструментів віртуалізації

Застосування методу дозволяє розділити фізичний сервер за допомогою гіпервізора на кілька ізольованих віртуальних серверів, які є незалежними один від одного [27]. Як результат, збій на одній з них не вплине на працездатність інших. Метод особливо ефективний для захисту від атак типу «грубої сили» та DoS.

ЗО_10. Застосування антивірусного програмного забезпечення

Виходячи з актуальної проблеми наявності вразливостей у ПЗ, що призводять до критичних наслідків для будь-якої системи [28, 29], в рамках даного методу використовується актуальне антивірусне ПЗ (як на стороні клієнта, так і сервері). Крім класичних та добре відомих антивірусних продуктів для клієнтської сторони, для серверів існують спеціалізовані рішення, такі як Dr.Web Server Security Suite, Avast Essential Business Security, Microsoft Windows Defender, McAfee Server Security та ін.

1.4 Проблематика та постановка завдань інформації Web-сайту

Без урахування світового досвіду з розробки методологічної бази управління інцидентами в сфері захисту інформаційних систем, неможливо організувати належні заходи безпеки, необхідність яких визначається сучасним розвитком технічних засобів та глобалізацією інформаційного простору.

Міжнародні стандарти управління інформаційною безпекою можуть сприяти зниженню кількості інцидентів, а їх дотримання допомагає перейти на новий рівень управління інформаційної безпекою.

Для автоматизації захисту інформаційних систем оптимально використовувати систему Snort, яка є вільною мережевою системою запобігання вторгнень (IPS) і мережевою системою виявлення вторгнень (IDS).

Метою даної роботи є дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web-сайту. Для досягнення поставленої мети у роботі необхідно:

- розкрити методологію захисту інформації Web-сайту;
- навести практичні рекомендації захисту інформації Web-сайту;
- виконати верифікацію результатів;
- запропонувати розрахунок капітальний витрат на придбання і налагодження складових систем інформаційної безпеки та річних експлуатаційних витрат на утримання і обслуговування об’єкта проектування;
- навести визначення річного економічного ефекту від впровадження об’єкта проектування та аналіз показників економічної ефективності запропонованого проектного рішення;
- представити висновок про економічну доцільність проектного рішення.

Висновки до розділу

У рамках першого розділу описано поняття ат сутність веб-сайту, розкрито інциденти мережі та методологічні основи захисту. Окреслено проблематику та здійснено постановку завдань.

РОЗДІЛ 2
ПРАКТИЧНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ WEB-САЙТУ

2.1 Методологія захисту інформації Web-сайту

Інцидент інформаційної безпеки може помітити користувач або адміністратор системи. Але часто цього буває недостатньо, тому необхідно звертатися до автоматизованих систем. Найбільш ефективною для цих цілей представляється система Snort.

«Snort є вільною мережевою системою запобігання вторгнень (IPS) і мережевою системою виявлення вторгнень (IDS) з відкритим вихідним кодом, здатною виконувати реєстрацію пакетів в реальному часі здійснювати аналіз трафіку в IP мережах» [21].

«Snort виконує протоколювання, аналіз, пошук по вмісту, а також широко використовується для активного блокування або пасивного виявлення низки нападів і зондувань, таких як переповнення буфера, стелс-сканування портів, атаки на веб-додатки, SMB-зондування і спроби визначення операційної системи. Програмне забезпечення в основному використовується для запобігання проникнення, блокування атак, якщо вони мають місце» [21].

А.О. Корченко, В.В. Волянська та А.І. Гізун наводять наступне визначення «Система виявлення вторгнень (СВВ) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до комп'ютерної системи або мережі або несанкціонованого управління ними в основному через Інтернет. Відповідний англійський термін – Intrusion Detection System (IDS). Системи виявлення вторгнень забезпечують додатковий рівень захисту інформаційних систем» [21].

Автори також зазначають, що «Системи виявлення вторгнень використовуються для виявлення деяких типів шкідливої активності, яка може порушити безпеку комп'ютерної системи. До такої активності

відносяться мережеві атаки проти вразливих сервісів, атаки, спрямовані на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків)» [21].

У роботі [21] підкреслено, що «Система запобігання вторгнень (англ. Intrusion Prevention System) – програмна або апаратна система мережевої та комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки та автоматично захищає від них» [21].

У свою чергу, потрібно розумути, що «системи IPS можна розглядати як розширення Систем виявлення вторгнень (IDS), враховуючи той факт, що завдання відстеження атак залишається однаковим в умовах їх виникнення. Проте, варто зазначити, що вони відрізняються в тому, що IPS повинна відслідковувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак. Можливі заходи – блокування потоків трафіку в мережі, скидання сполук, видача сигналів оператору» [21].

Також IPS можуть виконувати дефрагментацію пакетів, зміна пакетів TCP для захисту від пакетів зі зміненими SEQ і ACK номерами.

Після виявлення інциденту, настає важливий етап реагування на інцидент. Вся формальна модель процесу реагування на інциденти визначаться документом: ISO/IEC 27035-1:2016 Information security incident management. Цілями слідування цій моделі є впевненість у тому, що: «події та інциденти інформаційної безпеки виявляються і обробляються ефективним чином, особливо в частині класифікації подій; виявлені інциденти інформаційної безпеки в організації враховуються й обробляються найбільш ефективним і підходящим чином; наслідки інцидентів інформаційної безпеки можуть бути мінімізовані у процесі реагування на інциденти, можливо із залученням процесів відновлення після збоїв і аварій (DRP/BCP); за рахунок аналізу інцидентів і подій підвищується ймовірність запобігання майбутніх інцидентів, поліпшуються механізми і процеси забезпечення інформаційної безпеки» [ISO/IEC 27035-1:2016].

Процес реагування на інциденти складається з декількох етапів. У ці етапи в обов'язковому порядку входять наступні елементи.

1. Планування і підготовка. На даному етапі розробляється схема реагування на інциденти, готуються і затверджуються ряд організаційно-регламентуючих документів, виділяються людські і матеріальні ресурси, проводиться необхідне навчання та апробація обраної схеми реагування на інциденти.

2. Експлуатація. Власне виявлення інциденту інформаційної безпеки, його ідентифікація, попередній аналіз та початкове реагування.

3. Аналіз. Проводиться поглиблений аналіз інциденту, на його основі робляться висновки та складаються рекомендації щодо поліпшення процесу забезпечення інформаційної безпеки та реагування на інциденти. Формується звіт про інцидент.

4. Поліпшення. На даному етапі реалізуються рекомендації, вироблені на етапі аналізу.

У результаті, уся система захисту інформаційних систем набуває завершений цілісний вигляд. Подібна методологічна база, побудована на основі провідних світових стандартів захисту інформації та з використанням спеціалізованого програмного забезпечення, здатна якщо не повністю запобігти, то значно зменшити кількість інцидентів і мінімізувати викликані ними наслідки.

2.2 Практичні рекомендації захисту інформації Web-сайту

Сайт, або веб-сайт – одна або кілька логічно пов'язаних між собою веб-сторінок, а також місце розташування контенту сервера [2]. Захист сайтів від можливих загроз інформаційної безпеці – важливе завдання для його власника, оскільки можливі такі наслідки, як, наприклад, витік персональних даних, неотримання від потенційних клієнтів прибутку через недоступність

сайту, зниження позиції сайту в результатах пошуку, падіння репутації організації тощо. [3].

Веб-сайтам притаманні такі типи загроз [4]:

– зміна контенту веб-сайту – тобто розміщення на сайті зловмисником будь-якої інформації;

– видалення даних зловмисником, у тому числі інформації про паролі, бази даних клієнтів;

– впровадження шкідливих програм, які можуть здійснювати шкідливі дії (наприклад, крадіжка персональних даних користувача, переадресація на шахрайський сайт або зараження відвідувачів веб-сайту вірусними програмами);

– розсилання спаму веб-додатком сайту – загроза, що призводить до включення веб-сайту до спам-листів та неможливості в подальшому відправляти санкціоновані повідомлення;

– DDoS-атака – загроза, що ускладнює або припиняє доступ легальних користувачів до сайту.

До засобів захисту веб-сайтів належать такі [4]:

– міжмережевий екран веб-застосунків (Web application firewall, WAF);

– засоби аналізу веб-сайтів на наявність вірусів;

– балансувальники навантаження на веб-додатки;

– засоби захисту від DDoS-атак;

– сканери захищеності веб-додатків.

Розглянемо кожен засіб окремо. Принцип роботи міжмережевого екрану веб-застосунків заснований на використанні його основного компонента захисту – машинного навчання, за допомогою якого формується «білий» список допустимих ідентифікаторів доступу (на даний момент у веб-додатках використовуються три типи ідентифікатора доступу: HTTP-параметри, ідентифікатор ресурсу, ідентифікатор сесії, він також cookie). Завдання міжмережевого екрану веб-застосунків, реалізованого як фізичний

або віртуальний пристрій, полягає у виявленні допустимих значень ідентифікаторів для веб-додатка (реалізація у вигляді агента на веб-сервері не рекомендована до використання). Класичний спосіб розміщення WAF в мережі – в режимі зворотного проксі-сервера, перед веб-серверами, що захищаються – показаний на рисунку 2.1 [5]. Файрволи веб-застосунків можуть захистити від таких атак, як зміна та видалення даних веб-сайту, впровадження шкідливих програм, розсилання спаму [6].

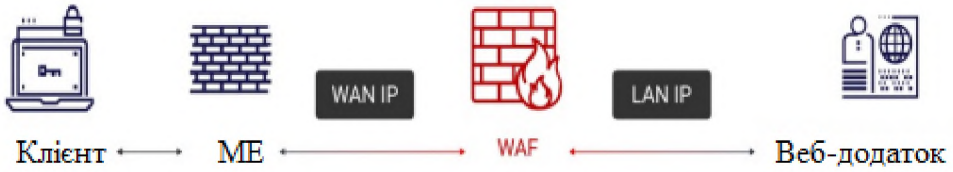

Рисунок 2.1 – Розміщення міжмережевого екрану веб-програм у мережі в режимі зворотного проксі-сервера

Засоби аналізу веб-сайтів на наявність вірусів дозволяють виявляти зловмисне програмне забезпечення (ПЗ) у файлах сайту або його коді. Серед засобів перевірки веб-сайту на наявність шкідливих програм можна виділити такі: онлайн-сервіси (що виконують статичний та динамічний аналіз коду веб-сторінки), антивірусні програми (скануючі файли на локальному веб-сервері, а також комп'ютери адміністраторів сайту) [7].

Балансування навантаження на веб-застосунки дозволяє розподілити навантаження між кількома мережевими пристроями, такими як сервери, маршрутизатори, міжмережеві екрани [8]. Ця операція може бути реалізована у вигляді додаткового заходу або на окремому сервері [9]. На рисунку 2.2 зображено схему, на якій балансувальник розподіляє навантаження між серверами [10]. Балансування навантаження дозволяє уникнути надмірної завантаженості сервера та, як наслідок, труднощів із доступом клієнтів до сайту [11].

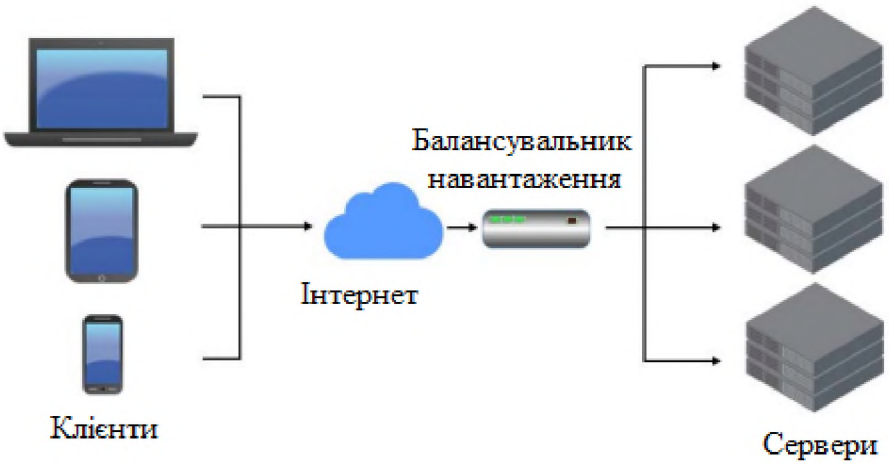

Рисунок 2.2 – Схема доступу клієнтів до ресурсів сервера у вигляді балансування навантаження

Для захисту від DDoS-атак застосовуються два підходи – створення програмно-апаратного комплексу в інфраструктурі організації-власника сайту або вибір спеціального стороннього сервісу. У роботі буде розглянуто підхід з допомогою сторонніх спеціальних сервісів [12]. На рисунку 2.3 показано схему захисту від DDoS-атак стороннім сервісом. При спробі користувача зайти на сайт, запит від нього відправляється в хмару компанії, що надає сервіс. У цій хмарі відбувається перевірка та фільтрація трафіку. Якщо трафік визнано атакуючим, він блокується. Решта відправляється на веб-сервер, на якому зберігається потрібний користувачеві сайт [3].

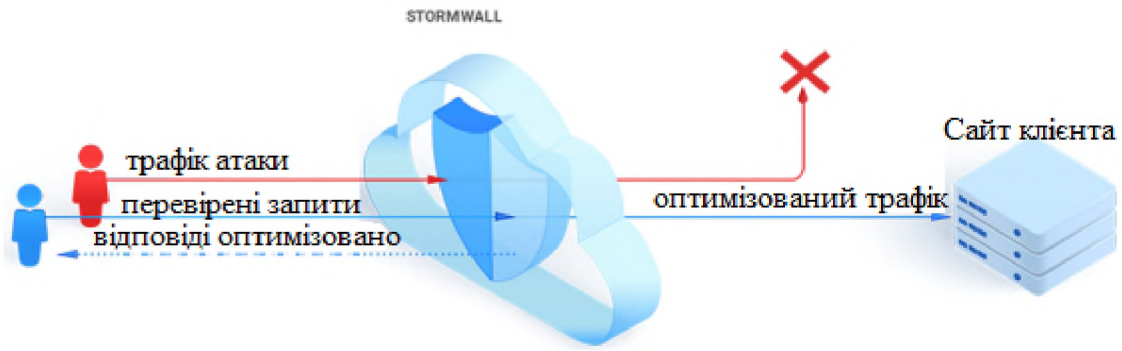

Рисунок 2.3 – Схема захисту від DDoS-атак за допомогою стороннього сервісу

Сканери захищеності веб-застосунків як засіб захисту веб-сайтів призначені для пошуку вразливостей у веб-додатках [13].

Для захисту сайтів зараз використовуються різні засоби та сервіси від іноземних виробників. Так, як міжмережевий екран веб-додатків популярне рішення американської компанії Imperva, призначене для забезпечення безпеки критичних веб-додатків, - Imperva SecureSphere Web Application Firewall [14]. Для його заміщення можна знайти багато інших варіантів програмного забезпечення зазначеного призначення, що забезпечує послуги в галузі кібербезпеки та гарантує захист корпоративних даних. Одним із вітчизняних міжмережевих екранів веб-додатків є Solid Wall WAF [15]. Так це рішення може бути реалізовано у вигляді ПЗ, віртуального пристрою, програмно-апаратного комплексу або у якості хмарного сервісу [16]. Перевага Solid Wall WAF перед Imperva SecureSphere Web Application Firewall в тому, що він є в єдиному реєстрі програм для електронних обчислювальних машин та баз даних [17].

У категорії імпортних антивірусних засобів для захисту веб-сайтів можна назвати програмне забезпечення Trend Micro Web Security від японської компанії Trend Micro, яка вважається світовим лідером серед розробників програмного забезпечення для кібербезпеки [20].

У яеості балансувальника навантаження на веб-додатки використовується модуль Local Traffic Manager, розроблений американською транснаціональною корпорацією F5 Networks, Inc., що спеціалізується на послугах, пов'язаних з Інтернет-сайтами та додатками [30]. Модуль, що входить до комплексу BIG-IP, може поставлятися як апаратне забезпечення, віртуальний пристрій або хмарний сервіс [30].

Серед зарубіжних сервісів захисту від DDoS-атак популярний Cloudflare DDoS protection, розроблений в американській компанії Cloudflare [35].

Для сканування веб-застосунків можна використовувати фреймворк з відкритим вихідним кодом Metasploit, створений в американській компанії

Rapid7 [37]. За допомогою цього найпотужнішого інструменту, що є в розпорядженні як кіберзлочинців, так і «білих хакерів» і фахівців з проникнення, можна дослідити вразливості в мережах і на серверах, застосовуючи готовий або створюючи код користувача і вводячи його в мережу для пошуку слабких місць.

2.3 Верифікація результатів

Метод аудиту будується на принципі рівно значимості та рівно вагомості компонентів системи забезпечення управління інцидентами інформаційної безпеки від всіх способів реалізації можливих загроз порушення ІБ [32]. Це означає, що оцінка ризику порушення ІБ дорівнює величині максимального ризику порушення ІБ серед системи забезпечення управління інцидентами інформаційної безпеки цього сегмента, тобто оцінка проводиться по найбільш уразливому компоненту.

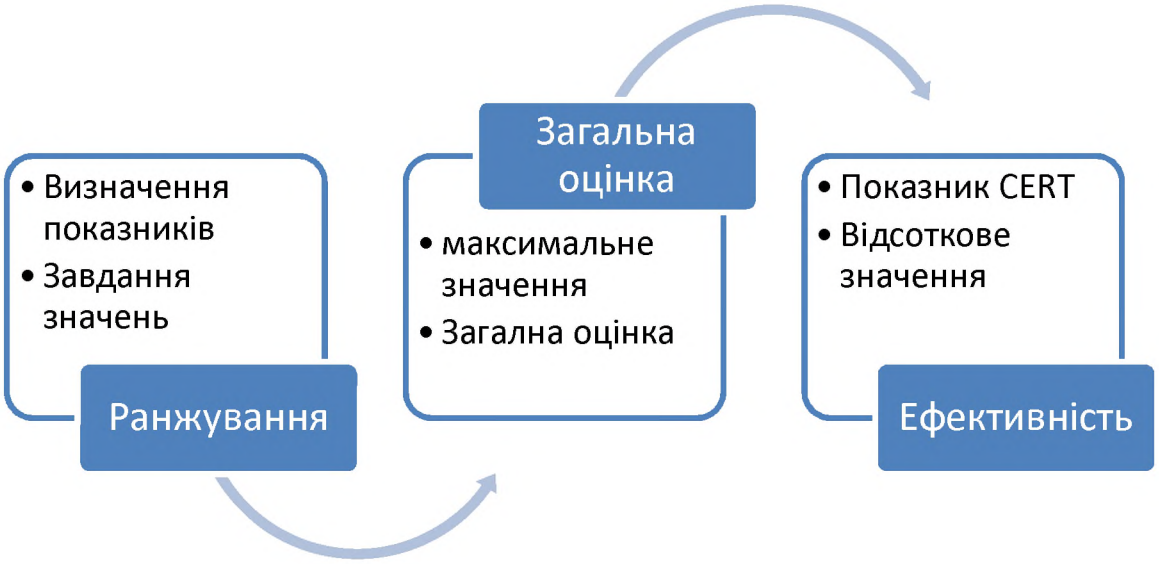

Рисунок 2.4 – Основні етапи аудиту

За словами В.В. Волянської, А.І. Гізуна та В.О. Гнатюка «Аудит являє собою незалежну експертизу окремих областей функціонування організації.

Розрізняють зовнішній і внутрішній аудит. Зовнішній аудит - це, як правило, разовий захід, що проводиться за ініціативою керівництва організації або акціонерів. Рекомендується проводити зовнішній аудит регулярно, а, наприклад, для багатьох фінансових організацій і акціонерних товариств це є обов'язковою вимогою. Внутрішній аудит являє собою безперервну діяльність, яка здійснюється на підставі "Положення про внутрішній аудиті "І відповідно до плану, підготовка якого здійснюється підрозділом внутрішнього аудиту і затверджується керівництвом організації. Аудит безпеки інформаційних систем є однією зі складових IT аудиту» [15]. Цілями проведення аудиту безпеки є:

– аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів веб-сайту;

– оцінка поточного рівня захищеності веб-сайту;

– локалізація вузьких місць в системі захисту веб-сайту;

– оцінка відповідності веб-сайту існуючим стандартам в області інформаційної безпеки;

– вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки веб-сайту.

У число додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

– розробка політик безпеки та інших організаційно-розпорядчих документів щодо захисту інформації та участь в їх впровадженні в роботу організації;

– постановка завдань для IT персоналу, що стосуються забезпечення захисту інформації;

– участь в навчанні користувачів і обслуговуючого персоналу ІС питань забезпечення інформаційної безпеки;

– участь в розборі інцидентів, пов'язаних з порушенням інформаційної безпеки;

– та інші.

Також авторами наголошується, що «Необхідно відзначити, що всі перераховані вище "додаткові" завдання, які стоять перед внутрішнім аудитором, за винятком участі в навчанні, по суті аудитом не являються. Аудитор за визначенням повинен здійснювати незалежну експертизу реалізації механізмів безпеки в організації, що є одним з основних принципів аудиторської діяльності. Якщо аудитор бере діяльну участь в реалізації механізмів безпеки, то незалежність аудитора втрачається, а разом з нею втрачається і об'єктивність його суджень, тому що аудитор не може здійснювати незалежний і об'єктивний контроль своєї власної діяльності. Однак, на практиці, внутрішній аудитор, часом, будучи найбільш компетентним фахівцем в організації в питань із забезпечення інформаційної безпеки, не може залишатися осторонь від реалізації механізмів захисту. До того ж майже завжди існує дефіцит кваліфікованих кадрів саме в цій області» [15].

Роботи по аудиту безпеки веб-сайту включають в себе ряд послідовних етапів, які в цілому відповідають етапам проведення комплексного IT аудиту АС, який включає в себе наступне:

- формування принципів аудиту
- акумулювання інформаційної складової аудиту
- формалізація даних аудиту
- окреслення рекомендацій направлених на реалізацію аудиту
- розробка аудиторського звіту
- ініціювання процедури аудиту.

Низка авторів наголошують, що «Аудит проводиться не з ініціативи аудитора, а з ініціативи керівництва компанії, яке в даному питанні є основною зацікавленою стороною. Підтримка керівництва компанії є необхідною умовою для проведення аудиту» [16].

У [18] зазначається, що «Аудит являє собою комплекс заходів, в яких крім самого аудитора, виявляються задіяними представники більшості структурних підрозділів компанії. Дії всіх учасників цього процесу повинні

бути скоординовані». Тому на етапі ініціювання процедури аудиту повинні бути вирішені наступні організаційні питання:

- права і обов'язки аудитора повинні бути чітко визначені і документально закріплені в його посадових інструкціях, а також в положенні про внутрішній (зовнішньому) аудиті;
- аудитором повинен бути підготовлений і узгоджений з керівництвом план проведення аудиту;
- в положенні про внутрішній аудиті має бути закріплено, зокрема, що співробітники компанії зобов'язані сприяти аудитору і надавати всю необхідну для проведення аудиту інформацію.

«На етапі ініціювання процедури аудиту повинні бути визначені межі проведення обстеження. Одні інформаційні підсистеми компанії не є достатньо критичними і їх можна виключити з меж проведення обстеження. Інші підсистеми можуть виявитися недоступними для аудиту з міркувань конфіденційності» [15].

Етап збору інформації аудиту, є найбільш складним і тривалим. Це пов'язано з відсутністю необхідної документації на інформаційну систему і з необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації.

«Компетентні висновки щодо стану справ в компанії з інформаційною безпекою можуть бути зроблені аудитором тільки за умови наявності всіх необхідних вихідних даних для аналізу. Отримання інформації про організацію, функціонування і поточний стан ІС здійснюється аудитором в ході спеціально організованих інтерв'ю з відповідальними особами компанії. Шляхом вивчення технічної і організаційно-розпорядчої документації, а також дослідження веб-сайту з використанням спеціалізованого програмного інструментарію» [18].

Використовувані аудиторами методи аналізу даних визначаються вибраними підходами до проведення аудиту, які можуть істотно різнитися.

Етап планування аудиту – перша стадія проведення всього аудиторського завдання. Тут аудитор розробляє стратегію та заходи аудиту залежно від сфери діяльності конкретного клієнта.

На цьому етапі аудитор зобов'язаний так спланувати аудит, щоб оптимально використані трудові ресурси аудиторського підприємства, час і можливість зведення до гранично низького рівня ризику не виявлення суттєвих помилок.

При складанні плану аудиту важливо врахувати:

1. Матеріально-технічну базу аудиторської організації;

2. Ефективну стратегію аудитора після оцінки ризику;

3. Кількість перевірок можливих замовників;

4. Підбір висококваліфікованих аудиторів, які здійснюватимуть сформовані замовлення;

5. Запас часу на лікарняні, відрядження, відпустки та щорічне підвищення кваліфікації аудиторів.

Існує кілька основних вимог щодо процесу планування:

– придбання знань про облік та про стан внутрішнього контролю;

– вироблення очікуваного рівня довіри до внутрішнього контролю замовника;

– визначення та прогнозування змісту, часу проведення та обсягу аудиторських процедур;

– системна робота аудиторів та експертів.

Планування в аудиті варто розглядати у двох аспектах: планування аудиторської перевірки та планування аудиторської діяльності. Аудиторські компанії розробляють та складають стратегічні плани аудиторської роботи, які розраховані на кілька років, бізнес-плани на поточний рік та план програми конкретної аудиторської перевірки.

Виконання аудиторського завдання є складним процесом, що потребує великої кількості часу, повноти інформації, знань спеціаліста, а також має

обмеження у часі за умовами укладеного договору між аудитором та замовником.

На думку вчених, як А.А. Аренс та Дж.К. Лоббекк планування аудиту ділиться на попереднє та безпосереднє (пряме) [11]:

Безпосереднє планування

- оцінка аудиторського ризику та рівня суттєвості
- складання загального плану та програми аудиту.

Попереднє планування полягає в отриманні аудитором якомога точнішої інформації про потенційного клієнта.

Кінцевим результатом може бути рішення про можливість проведення подальшої перевірки, так і про відмову від проведення аудиторської перевірки.

Попереднє планування

- знайомство зі специфікою
- вивчення стану
- оцінка системи внутрішнього контролю.

За згодою аудитора у проведенні аудиторської перевірки переходять до безпосереднього планування. Від того наскільки ефективно, надійно та грамотно виконане попереднє планування залежатиме якість стадії прямого планування. У цьому етапі аудитор розробляє стратегію аудиторської перевірки [6].

У процесі планування аудиторської перевірки аудиторським фірмам рекомендується дотримуватися чотирьох основних принципів.

Комплексність передбачає взаємозв'язок усіх стадій роботи від попереднього планування до складання плану та програми аудиту. Безперервність встановлює взаємозв'язок стратегічного та тактичного планування аудиту. Оптимальність забезпечує розробку різних варіантів плану та вибір найбільш оптимального. Мобілізація допомагає найефективніше використовувати час фахівців. Сукупність даних принципів

дозволяє підвищити якість планування аудиторської перевірки та результативність її проведення.

При побудові загального плану та програми аудиторської перевірки необхідно взяти до уваги показник аудиторського ризику та припустимої помилки.

У процесі складання загального плану аудитор має врахувати сферу діяльності клієнта, систему контролю, рівень ризику, обсяг роботи та часові рамки [8].

Основним етапом планування аудиторської перевірки є створення програми аудиту, який виступає фундаментом для формування загального плану.

У програмі аудиту відображаються методи, обсяг, процедури перевірки та термін їх реалізації. Тому реалізація аудиторського завдання зводиться до виконання його програми з перевірки достовірності показників кожного розділу звітності.

На завершальному етапі у загальному плані відображаються результати від проведеної процедури перевірки та складається аудиторський висновок. Складовою загального плану на заключній стадії аудиту є положення, що передбачають здійснення внутрішнього контролю за проведенням аудиторської перевірки [9].

Таким чином, план аудиту включає перелік етапів аудиту та напрямки перевірки. Програма аудиту є розвитком та вдосконаленням плану, тому має бути смисловий зв'язок між цими документами [4].

Показники $P_1, P_2, P_3 \dots P_n$ основними показниками дієвості системи, важливість кожного показника задається коефіцієнтом важливості КВ та пріоритетом кожного показника КП. Значення КВ варіюються у межах одиниці, тобто $КВ = 1$, а пріоритет задається значенням від 0 до 1 та у подальшому підсумовуються.

Розвиток системи ґрунтується на послідовних етапах:

1) ранжування:

Показники	Р4	Р1	Р6	...	Pn	Р1
$\sum$ КВ = 1	0,01	0,05	0,1	...	0,22	0,3

2) Загальна оцінка:

$$\text{Заг. оцінка} = \sum KB_i P_i$$

$$\text{Заг. оцінка}_{\text{КВ}} = \sum KB_i P_{i\,max} = max$$

$$\text{Заг. оцінка}_{\text{пот}} = \sum KB_i P_{i\,\text{пот}} = \text{Оцінка}$$

KB_i - коефіцієнт важливості;

КP_i - коефіцієнт пріоритету.

3) Показник ефективності CERT:

$$E = {}^{\text{Оцінка}}/_{max} \cdot 100\%$$

Загальна архітектура експертної системи наведена на рис. 2.5

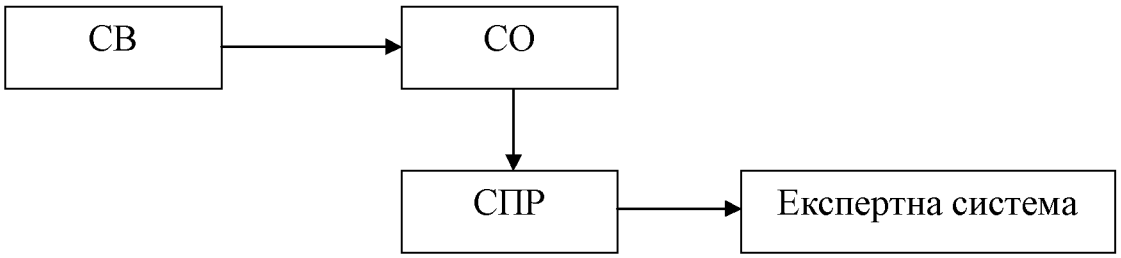

Рисунок 2.5 – Загальна архітектура експертної системи виявлення інцидентів веб-сайту

СВ – система виявлення вторгнень

СО – система обробки вторгнень

СПР – система прийняття рішень

У [20] наводиться наступне визначення «Система виявлення вторгнень виявляє факти несанкціонованого доступу в комп'ютерну систему або

несанкціонованого управління ними в основному через Інтернет та забезпечує додатковий рівень захисту комп'ютерних систем. При виявленні шкідливої активності до якої відносяться мережеві атаки проти вразливих сервісів, атаки, спрямовані на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків) СВ надає інформацію системі обробки вторгнень, яка обробляє сигнал, що надійшов та проводе аудит знайдених вторгнень, після чого до системи прийняття рішень, надходять результати проведеного аудиту, на основі чого СПР приймає рішення, щодо рівня загрози та можливих наслідків відносно впливів загрози, окреслені дані передаються експертній системі, яка виносить рішення, щодо потреби у захисті, того, чи іншого об’єкту».

Деталізована згадана система пропонується на рис. 2.6.

Технологія запобігання атак на мережевому рівні може бути реалізована тільки за допомогою спеціалізованих мережевих датчиків, структура та алгоритм роботи яких описуються нижче. Мережеві датчики в цьому випадку виконуються у вигляді окремих апаратних блоків, які встановлюються в канали зв'язку таким чином, щоб через них проходив весь мережевий трафік. Для цього датчик оснащується двома мережевими адаптерами, які функціонують у "змішаному" режимі (promiscuous mode) і через які передбачається проходження всієї інформації, що передається в сегменті веб-сайту. Структура такого датчика показана на рис.2.7.

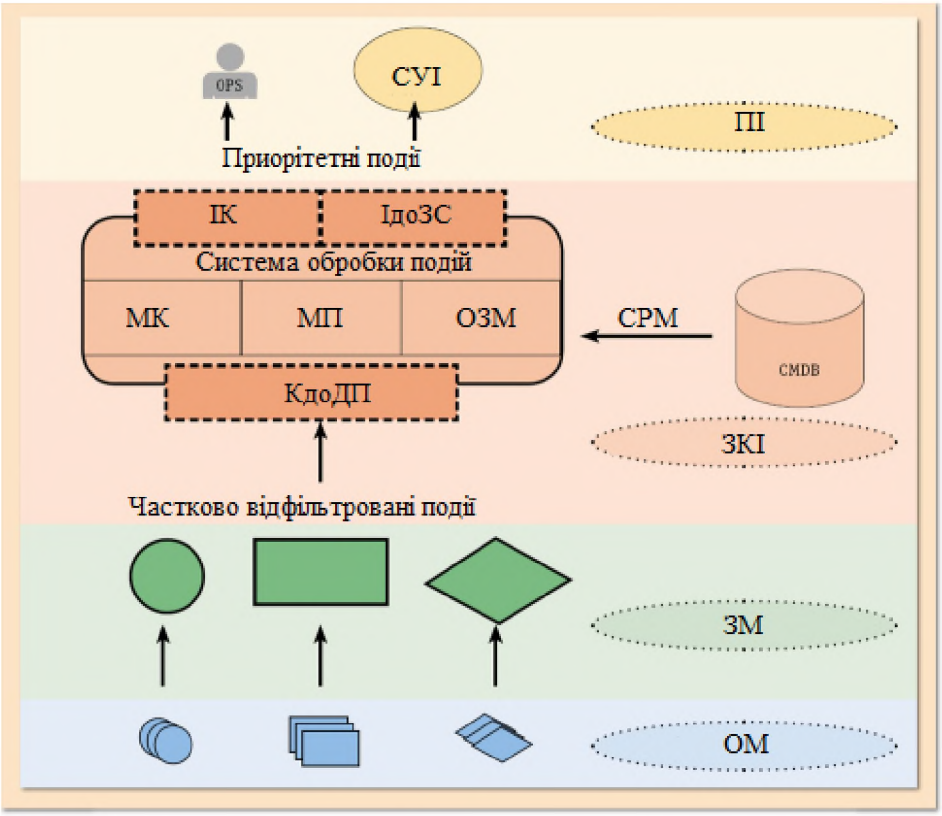

Рисунок 2.6 – Деталізована архітектура експертної системи виявлення інцидентів

СУІ – система управління інцидентами

ПІ – представлення інформації

ІК – інтерфейс користувача

ІдоЗС – інтерфейси до зовнішніх систем

МК – модуль кореляції

МП – модель пріоритизації

ОЗМ – оперативне зберігання моделей

СРМ – сервісно-ресурсні моделі

КдоДП – коннектори до джерел подій

ЗКІ – засоби консолідації інформації

ЗМ – засоби моніторингу

ОМ – об’єкти моніторингу

«Принцип роботи компонентів мережевого датчика полягає в наступному. Пакети даних поступають на вхід одного з двох адаптерів, встановлених в мережевому датчику. Далі вони записуються в буферну пам'ять датчика, звідки зчитуються МВА. МВА дані аналізуються з метою виявлення інформаційних атак порушника. При необхідності можуть бути задіяні наявні в МВА механізми IP-дефрагментації і складання TCP-сесій. В процесі проведення аналізу пакетів даних модуль звертається до бази даних сигнатур атак і профілів. У разі виявлення атаки інформація про це направляється в модуль реагування, який і визначає оптимальний метод реакції СОА. Крім описаних вище стандартних методів реагування модуль може прийняти рішення і про видалення тих пакетів, за допомогою яких реалізується атака. Така операція дозволяє мережному датчику блокувати виявлену інформаційну атаку» [3]. У разі ж якщо пакети даних, що проходять через датчик, не представляють небезпеки для веб-сайту, вони передаються далі по заданому маршруту.

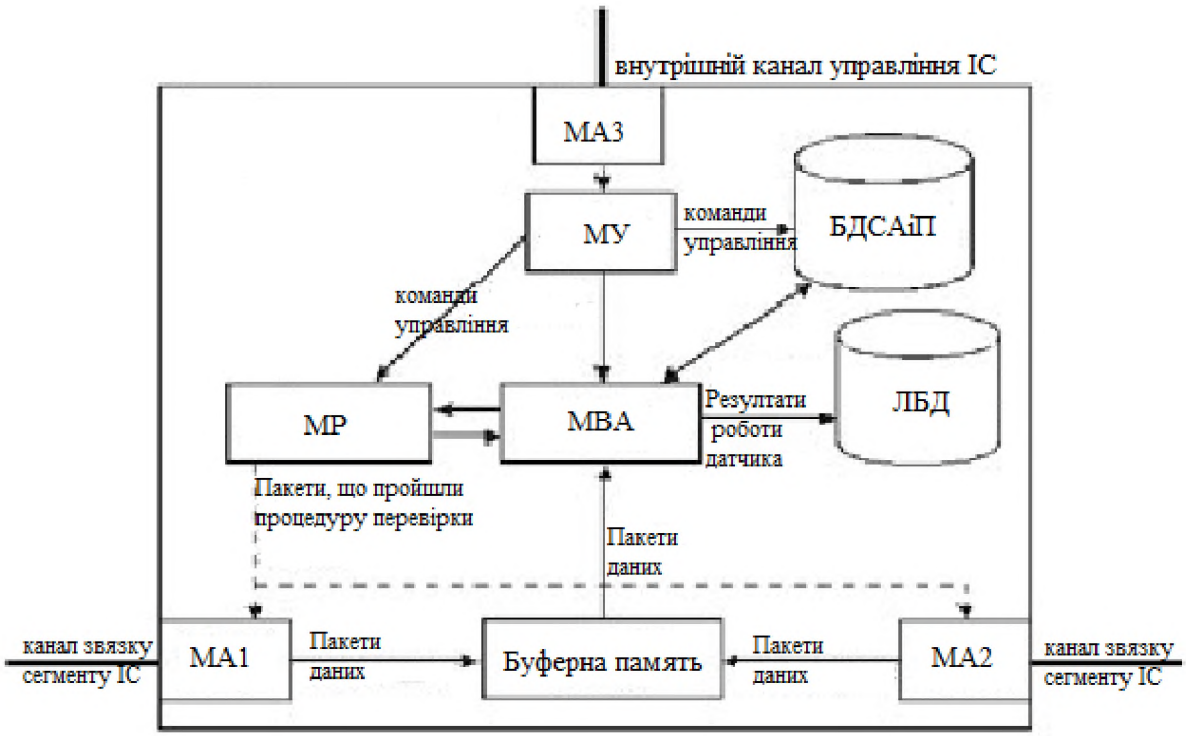

Рисунок 2.7 – Структура мережевого датчику

Дуже важливо сказати і про те, що алгоритм функціонування МВА мережевого датчика дозволяє використовувати два методи виявлення інформаційних атак – сигнатурний та профільний. Зміст сигнатурного методу аналізу полягає у виявленні атак на основі відомих шаблонів, або сигнатур, які зберігаються у відповідній базі даних датчика. «Профільний метод виявлення призначений для виявлення аномального мережевого трафіку, параметри якої не відповідають параметрам профілю ІС, також зберігається в базі даних датчика. Будь-який аномальний трафік, виявлений у веб-сайті, розцінюється датчиком як спроба реалізації атаки і підлягає блокуванню. Профільний метод виявлення атак відноситься до групи поведінкових методів аналізу. Технологічно передбачається, що мережевий датчик для кожного з хостів ІС зобов'язаний зберігати окремий профіль трафіку, який може отримувати або відправляти хост. Завдання полягає в тому, щоб трафік, параметри якого не відповідають значенням параметрам профілю, видалявся із загального інформаційного потоку» [20]. В якості прикладу можна навести параметри профілю HTTP-трафіку, який може вступати в веб-сервер ІВ (табл.2.2).

Таблиця 2.2 – Приклад профілю трафіку веб-сервера, що зберігається в базі даних мережевого датчика

Найменування параметра профілю	Опис параметра профілю
IP-адреси відправника HTTP-трафіку	Діапазон IP-адрес хостів, від яких можуть надходити HTTP-запити до веб-сервера
Номери TCP-портів веб-сервера	Допустимі номери TCP-портів, з яких до веб-вервера можуть надходити HTTP-запити
Методи формування HTTP-запитів	Дозволені методи формування HTTP-запитів до веб-сервера
Інформаційні ресурси веб-сервера	Допустимі інформаційні ресурси, доступ до яких може бути отриманий за допомогою HTTP запитів
Параметри HTTP-запиту	Допустимі значення параметрів, які можуть міститися в HTTP-запитах до ресурсів веб-серверу

Аналогічні профілі задаються і по відношенню до інших типів мережевого трафіку, циркулюючого у веб-сайті.

Перевага профільного методу в тому, що він створює можливість для запобігання не тільки відомих в даний час інформаційних атак, але і великої кількості несанкціонованих впливів порушників, які ще не вивчені в достатній мірі та реалізація яких пов'язана з порушенням параметрів, закладених у профілі. Так, наприклад, введення обмеження на допустимі значення параметрів HTTP-запитів дозволяє блокувати такі атаки, як Code Red, Code Red II, Nimbda [4], а також всі їх подальші модифікації. Крім того, профільний метод не зберігає сигнатури конкретних мережевих атак і, отже, не вимагає постійного оновлення сигнатурной бази.

Керування компонентами мережевого датчика проводиться за допомогою окремого модуля управління, у функції якого закладена здатність змінювати параметри роботи кожного з компонентів. Реалізуються ці функції по командам, формованим у центральному модулі управління і переказуються мережному датчику по виділеному каналу зв'язку через окремий мережний адаптер.

Результати роботи мережевого датчика протоколюються в локальній базі даних, доступ до вмісту якої адміністратор безпеки веб-сайту може отримати з використанням модуля управління мережевого датчика.

Запобігання атак на системному рівні веб-сайту. Технологія запобігання інформаційних атак на системному рівні реалізується на рівні хостів веб-сайту з використанням хостових датчиків. Цей підхід дозволяє запобігти два типи інформаційних атак:

– мережеві атаки, які реалізуються порушником віддалено шляхом посилки об'єкту нападу серії пакетів даних з метою порушити інформаційну безпеку хоста;

– системні атаки, які реалізуються порушником локально за допомогою несанкціонованого запуску програм, також з метою порушити інформаційну безпеку хоста. Прикладами таких програм є інформаційні

віруси, програми типу "троянський кінь", програми, спрямовані на несанкціоноване підвищення прав доступу та ін.

Захист від атак цього типу забезпечується мережевими та системними компонентами хостовых датчиків. Алгоритм функціонування мережевого компонента в чомусь повторює алгоритм роботи мережевого датчика. Мережевий компонент перехоплює всі пакети даних, що надходять на хост веб-сайту, аналізує їх і відфільтровує ті, які можуть представляти небезпеку для хоста. Аналіз проводиться на основі сигнатур, або на основі профілю трафіку хоста. Мережевий компонент, на відміну від датчика, перехоплює і аналізує пакети даних на різних рівнях моделі взаємодії відкритих систем. Це дає можливість запобігати атакам, які реалізуються за криптозахищеним IPSec і SSL/TLS-з'єднанням. Мережевий компонент датчика може складатися з декількох окремих програмних модулів, що запускаються на хості. Так, наприклад, для перехоплення і аналізу HTTP-трафіку, що надходить в веб-сервер MS Internet Information Services, мережевий компонент може включати окремий модуль, виконаний у вигляді ISAPI-фільтру, який дозволяє перехоплювати весь вхідний HTTP-трафік на прикладному рівні і видаляти ті HTTP-запити, які не відповідають заданим профілем.

Важливо підкреслити, що системний компонент хостового датчика дозволяє перехоплювати і аналізувати системні виклики всіх додатків, запущених на сайті. Аналіз проводиться на основі сигнатур або на основі профілю хоста веб-сайту У кожному з перехоплених системних викликів аналізуються наступні параметри:

– ім'я процесу/додатка, який ініціював системний виклик;

– обліковий запис користувача, від імені якого виконується системний виклик;

– ідентифікатор ресурсу, до якого спрямований системний виклик;

– параметри системного виклику та ін.

У разі встановлення факту порушення системним викликом інформаційної безпеки хоста, цей виклик блокується. Такий механізм аналізу

та обробки системних викликів дозволяє запобігти системні атаки порушників.

Параметри функціонування додатків, які можна контролювати з використанням системного компонента, та їх опис наведені в табл. 2.3.

Таблиця 2.3 – Параметри функціонування додатків, які можна контролювати з використанням системного компонента, та їх опис

Найменування параметра	Опис
Доступ додатків до файлової системи хоста	Параметр контролює доступ додатків до файлової системи хоста. З використанням цього параметра компонент може запобігти несанкціонований доступ до файлів користувачів з боку деяких додатків
Доступ додатків до системних конфігураційних файлів операційної системи (ОС) хоста	Параметр дозволяє контролювати доступ додатків до реєстру, системних бібліотек та інших конфігураційних файлів ОС. За допомогою цього параметра компонент може заборонити внесення змін у ці системні файли, що дозволить забезпечити захист від програм типу "троянський кінь", а також програм, спрямованих на несанкціоноване отримання адміністраторських прав
Параметри виклику системних функцій з програми	Параметр дозволяє блокувати ті системні виклики, значення параметрів яких не відповідають заданим обмеженням. Це дозволяє запобігти системні атаки, спрямовані на переповнення буфера програм (buffer overflow attacks), які призводять до несанкціонованого виконання коду на хості
Середовище виконання програми	Параметр системного компонента блокує запити програми на запис в ту область пам'яті, яка не належить цьому додатку. Це дозволяє забезпечити захист від інформаційних вірусів, а також програм, спрямованих на несанкціоноване отримання адміністраторських прав

Велика частина наведених вище параметрів аналізується системним компонентом за допомогою профільного методу. При цьому для кожної програми або групи програм визначається свій власний профіль роботи. Так, наприклад, профіль HTTP-сервера повинен дозволяти доступ до веб-додатків

тільки до веб-ресурсів, що включає HTML-документи, ASP-сценарії CGI-модулі та ін. Доступ до всіх інших інформаційних ресурсів хоста, включаючи системні конфігураційні файли ОС, повинен бути заборонений.

«Сигнатурний аналіз системних викликів дозволяє виявляти відомі системні атаки, такі як GetAdmin і SecHole, які реалізуються шляхом запуску на локальній машині спеціальних програм, що дозволяють несанкціоновано отримати адміністраторські права доступу до хосту» [19].

Оскільки нове покоління СУІ здатне не тільки виявляти, а й запобігати інформаційні атаки, до тестування систем цього класу пред'являються інші вимоги. В першу чергу це пов'язано з тим, що тестуватися повинні не тільки функції виявлення атак, але функції їх блокування. Для тестування СУІ, що реалізують технологію запобігання атак на мережевому рівні, можуть використовуватися спеціалізовані системи аналізу захищеності, що дозволяють змоделювати задану безліч мережевих атак порушника. В цьому випадку ефективність СУІ буде визначатися кількістю допущених помилок першого і другого роду. Під помилкою першого роду розуміється блокування СУІ легального мережевого запиту, не є атакою. Помилка другого роду виникає в тому випадку, якщо СУІ не змогла блокувати реальну мережну атаку.

Тестування СУІ, що реалізують технологію запобігання атак на системному рівні, реалізується способом, аналогічним тому, який застосовується на мережевому рівні ІС.Єдина відмінність полягає в тому, що тут, крім всього іншого, необхідно проводити моделювання системних атак порушника. Іншими словами, потрібно провести установку програм типу "троянський кінь", активізувати інформаційний вірус, несанкціоновано змінити системні файли ОС хоста та ін. Ефективність СУІ цього типу оцінюється шляхом підрахунку кількості помилок першого і другого роду, допущених системою в процесі функціонування.

На сьогоднішній день, одним з головних напрямків ефективної реалізації будь-якої методики є експериментальне дослідження тобто виявлення якостей досліджуваних об’єктів, перевірка достовірності гіпотез, а також широке та глибоке вивчення досліджуваної наукової тематики. У рамках сучасної науки існує багато різних класифікацій експериментів в залежності від галузі науки, мети дослідження, структури об’єктів та явищ, організаційних заходів, характеру взаємодії об’єкту та засобів дослідження тощо.

Провідним місцем у досконалому проведенні експерименту, займає правильна розробка методики експерименту – визначена послідовність процесів, у результаті якої досягається мета дослідження.

Першочерговим етапом проведення експериментального дослідження є план програми дослідження, який складається за умови проведення дослідження, де визначається:

– гіпотеза;

– мета та задачі;

– вхідні і вихідні параметри, область їх визначення та крок дискредитації;

– порядок проведення власне експерименту;

– зазначаються необхідні засоби проведення дослідження, моделювання, обробки результатів;

– порядок і вимоги щодо оформлення результатів.

Далі, слідує етап визначення об’єму експериментальних досліджень та необхідних програмних та апаратних засобів тощо.

Останнім кроком є безпосередньо експеримент, який проводиться з регламентацією всіх кроків, та обробка і систематизація експериментальних і усіх числових даних, перевірка зведення до єдиної системи одиниць, побудова графіків залежностей, таблиць, діаграм тощо.

Гіпотеза

Експеримент базується на припущені, що запропонована методика захисту інформації Web-сайту адекватно реагує на зміну ідентифікуючих та оціночних параметрів при різних умовах контрольованого середовища.

Мета та задачі експерименту

Метою експерименту є перевірка адекватності запропонованої методики захисту інформації Web-сайту, а саме:

– дослідження запропонованої методики захисту інформації Web-сайту на основі експертних методів та нечіткої логіки стосовно ефективності її роботи;

– дослідження запропонованої методики захисту інформації Web-сайту на основі експертних методів та нечіткої логіки стосовно ефективності її роботи, а саме коректності оцінювання критичності ситуації, що склалася під впливом ІПКС, та встановлені факту переходу небажаних подій з класу «інциденти інформаційної безпеки» до класу «кризова ситуація».

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– обробка і верифікація отриманих результатів;

– проведення виявлення ІПКС та оцінки критичності ситуацій в контрольованому середовищі при зміні ідентифікуючих та оціночних параметрів

– визначення можливості використання системи управління інцидентами інформаційної безпеки для забезпечення процесів КУББ.

Вибір вхідних та вихідних параметрів

Для методики захисту інформації Web-сайту

вхідні параметри – значення параметру, КВ1, Пар23, КВ2, ..., Пар Н, КВ Н, а також порівняльні судження експертів, щодо важливості оціночних е -го та е'-го параметрів між собою відповідно до методу кількісного парного порівняння з визначенням квадратного кореня;

– вихідні параметри – показник рівня критичності ситуації, спричиненої впливом ІПКС, відображений індикатором критичності.

Вибір кроку зміни вхідних параметрів. Значення параметрів КВ1, ПР2,3, КВ2, ..., ПР Н, КВ Н для обробки в системі захисту інформації Web-сайту параметри ПР1, ПР2, ..., ПР Н приймають значення від 0 до 1, попередньо нормуючись. Максимальні значення параметрів встановлюються експертом в залежності від галузі застосування, контрольованого середовища і виду інциденту, що є причиною поточної ситуації.

Крім того ідентифікуючі та оціночні параметри можуть бути описані у вигляді лінгвістичних змінних, наприклад, «низький» (Н), «середній» (С), «великий» (В) тощо.

Послідовність дій в експериментальному досліджені

Для дослідження системи захисту інформації Web-сайту виконуються в повній відповідності до етапів методу оцінки критичності ситуації та режиму роботи системи – задається множина оціночних параметрів; визначаються КВ важливості кожного параметра; проводиться фазифікація їх поточних значень; обчислюється показник рівня критичності ситуації; отриманий показник порівнюється з оціночним еталоном, на основі чого приймається рішення щодо критичності ситуації; проводиться дефазифікації значень оціночних параметрів та рівня критичності і на основі отриманих даних створюється індикатор критичності.

Засоби проведення експерименту

Для дослідження, створення необхідного програмного забезпечення, імітаційного модулювання, обробки результатів та представлення їх в табличному та графічному вигляді використовувалося середовище Microsoft Excel 2007.

Аналіз результатів

Результати представлені в табличній формі та у вигляді графіків і діаграм.

Розроблена методика захисту інформації Web-сайту складається з таких етапів: визначення показників функціонування системи, визначення

ключових показників ефективності роботи системи, побудова панелі індикаторів та візуалізація залежності KPI та E.

Етап 1 – Визначення показників функціонування системи захисту інформації Web-сайту. При функціонуванні система захисту інформації Web-сайту здійснюється запис до бази даних (БД) інформації про кіберінциденти.

Відповідно до розробленої методики було проведено експериментальні дослідження системи захисту інформації Web-сайту. Далі опишемо хід проведення експерименту, а також обробку та аналіз його результатів.

Етап 2 – Визначення ключових показників ефективності роботи системи захисту інформації Web-сайту. Щоб визначити з множини показників функціонування системи захисту інформації Web-сайту PI ключові показники ефективності KPI використаємо процедуру множинного кореляційно-регресійного аналізу [9], яка включає наступні кроки:

Крок 1. Вибір всіх можливих чинників (обираються чинники, які впливають на показник (або процес), що досліджується, якщо деякі чинники неможливо кількісно чи якісно визначити або для них недоступна статистика, то їх вилучають з подальшого розгляду).

Крок 2. Вибір вигляду регресійної чи багаточинникової моделі (знаходження аналітичного виразу, який найкраще відображував би зв'язок чинникових ознак з результативною).

Крок 3. Перевірка адекватності отриманої моделі (розрахунок: розбіжності між спостереженими та розрахунковими значеннями; відносної похибки між спостереженими та розрахунковими значеннями; середньоквадратичної помилки дисперсії збурень; коефіцієнта множинної кореляції).

За допомогою системи захисту інформації Web-сайту була проведена оцінка критичності різних ситуацій, спричинених впливом ІПКС. В процесі дослідження на основі розроблених еталонів множини оціночних параметрів з врахування їх КВ та проведення фазифікації поточних значень отримана оцінка критичності ситуації та сформований індикатор критичності. Так,

було оцінено критичність збоїв роботи почтового сервера внаслідок проведення DDOS-атаки і ситуація в зоні надзвичайної ситуації в моменти виникнення ситуації, в процесі розвитку та після застосування контрзаходів. Отриманий результат підтвердив адекватність розроблених еталонів і коректність вибору множини оціночних параметрів.

Використовуючи БД з показниками функціонування системи управління інцидентами інформаційної безпеки (за II квартал 2022 року) сформуємо табл. 2.4.

Таблиця 2.4 – Значення показників діяльності системи захисту інформації Web-сайту за II квартал 2022 р.

Параметр	Значення									
$ПР_1$	1	0	1	1	0	1	1	1	0	1
$ПР_2$	1	0	1	1	0	0	0	1	0	1
$ПР_3$	1	1	1	1	1	1	1	1	1	1
$ПР_4$	1	1	0	0	0	1	0	1	1	0
$КВ_1$	1	2	3	1	3	2	4	1	3	2
$КВ_2$	3	2	4	1	3	2	2	3	4	4
$КВ_3$	2	5	8	8	2	1	5	2	3	5
$КВ_4$	1	2	3	1	3	2	4	1	3	2
$КВ_5$	2	5	8	8	2	5	8	8	7	7
ЗО	9	9	10	10	8	10	8	10	10	9

Відповідно до наведених даних здійснюємо аналіз отриманих даних. Розраховуємо середньоквадратичне відхилення та дисперсію, отримані результати наводимо у таблиці 2.5.

Таблиця 2.5 – Результати математичного аналізу

Параметр	Значення										Середнє відхилення	Дисперсія
$ПР_1$	1	0	1	1	0	1	1	1	0	1	0,42	0,21
$ПР_2$	1	0	1	1	0	0	0	1	0	1	0,5	0,25

$ПР_3$	1	1	1	1	1	1	1	1	1	1	0	0
$ПР_4$	1	1	0	0	0	1	0	1	1	0	0,5	0,25
$КВ_1$	1	2	3	1	3	2	4	1	3	2	0,84	0,96
$КВ_2$	3	2	4	1	3	2	2	3	4	4	0,84	0,96
$КВ_3$	2	5	8	8	2	1	5	2	3	5	2,1	5,69
$КВ_4$	1	2	3	1	3	2	4	1	3	2	0,84	0,96
$КВ_5$	2	5	8	8	2	5	8	8	7	7	2	5,2
ЗО	13	18	29	22	14	15	25	19	22	23	4,2	23,8

Наступним кроком є кореляційний аналіз. Результати у таблиці 2.6.

Таблиця 2.6 – Кореляційний аналіз отриманих результатів

	$ПР_1$	$ПР_2$	$ПР_3$	$ПР_4$	$КВ_1$	$КВ_2$	$КВ_3$	$КВ_4$	$КВ_5$	ЗО
$ПР_1$	1									
$ПР_2$	0,846564	1								
$ПР_3$	0,721958	0,949874	1							
$ПР_4$	0,696756	0,930106	0,953304	1						
$КВ_1$	0,888679	0,845974	0,749418	0,626177	1					
$КВ_2$	0,908195	0,883933	0,770116	0,74774	0,87989	1				
$КВ_3$	0,612761	0,89553	0,927541	0,869699	0,743616	0,80344	1			
$КВ_4$	0,825308	0,872774	0,831848	0,83447	0,730714	0,936313	0,824554	1		
$КВ_5$	0,835144	0,930264	0,886976	0,806971	0,881455	0,943425	0,904059	0,937171	1	
ЗО	0,805695	0,945124	0,972585	0,924287	0,789531	0,860236	0,907963	0,92644	0,94391	1

Аналізуючи дані з табл. 2.6 та використовуючи шкалу Чеддока, можна зробити висновок, що найбільш впливають на ефективність такі чинники:

- $ПР_2$,
- $КВ_1$
- $КВ_2$
- $КВ_4$
- $КВ_5$
- ЗО

На виході цього етапу, згідно до формули:

$$KPI = \left\{ \bigcup_{w=1}^{v} KPI_w \right\} = \{KPI_1, KPI_2, \dots, KPI_v\}$$

де

$$KPI_w \subseteq KPI, (w = \overline{1, v})$$

v – кількість ключових показників ефективності.

при w = 6 отримуємо множину ключових показників ефективності KPI :

$$KPI = \{ПР2, КВ1, КВ2, КВ4, КВ5, ЗО\}$$

Розрахуємо загальну ефективність системи. Показник ефективності CERT:

$$E = {Оцінка}/{max} \cdot 100\%$$

Для цього сформуємо таблицю максимальних показників (табл.2.7)

Таблиця 2.7 – Максимальні значення показників

Параметр	Значення
$ПР_1$	1
$ПР_2$	1
$ПР_3$	1
$ПР_4$	1
$КВ_1$	5
$КВ_2$	5
$КВ_3$	10
$КВ_4$	5
$КВ_5$	10
ЗО	39

Наступним кроком розрахуємо ефективності системи та результати зведемо до таблиці 2.8.

Таблиця 2.8 – Результати розрахунку ефективності

Параметр	Максимальне значення	Оцінка	Ефективність
$ПР_1$	1	0,7	70
$ПР_2$	1	0,5	50
$ПР_3$	1	1	100
$ПР_4$	1	0,5	50
$КВ_1$	5	2,2	44
$КВ_2$	5	2,8	56
$КВ_3$	10	4,1	41
$КВ_4$	5	2,2	44
$КВ_5$	10	6	60
ЗО	39	20	51,28205

Наведемо графічно результати розрахунку:

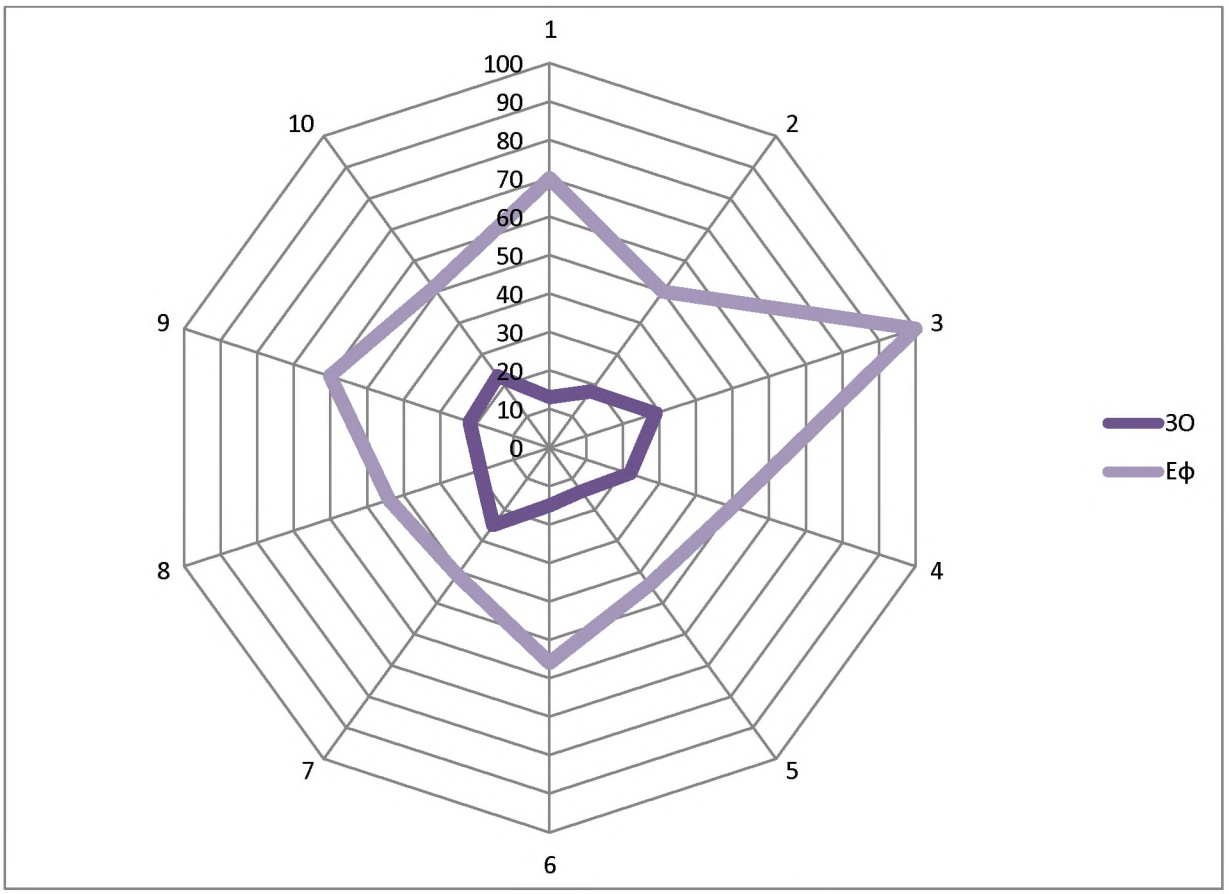

Рисунок 2.8– Графік залежності ефективності від Загальної оцінки

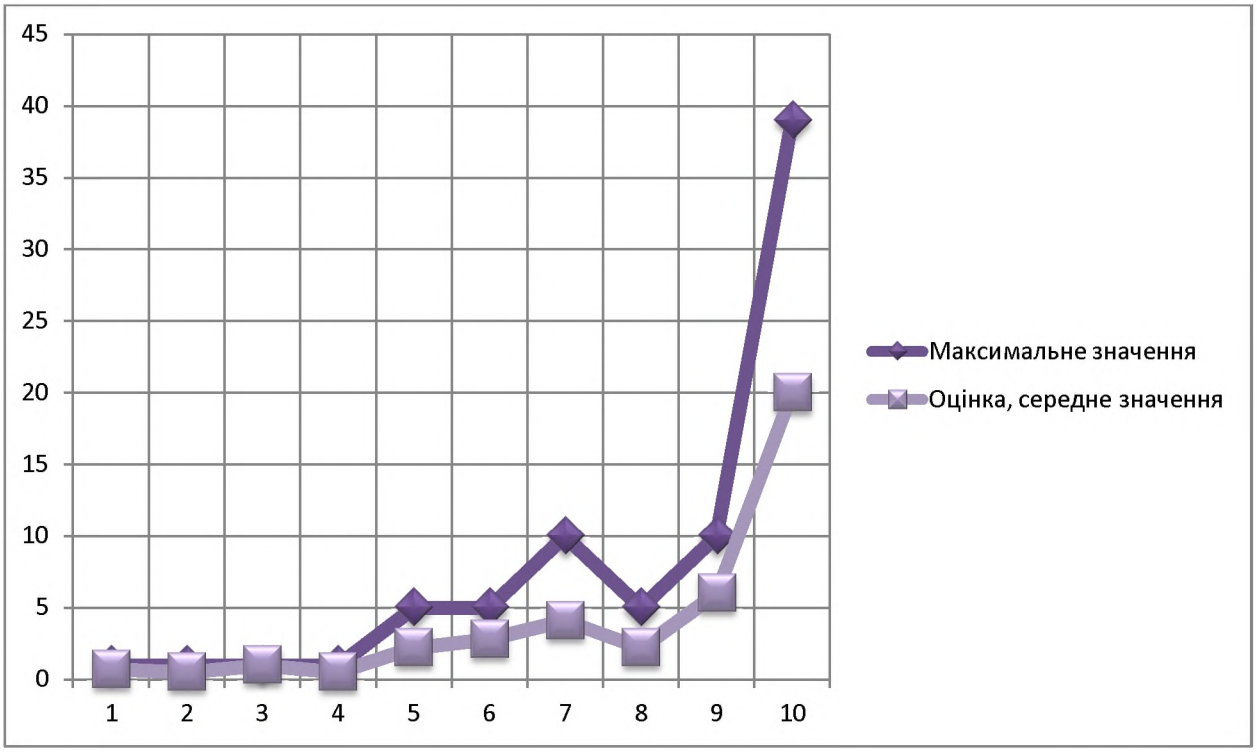

Рисунок 2.9 – Графік залежності ефективності від середньої оцінки

Провівши аналіз отриманих результатів (рис. 2.8 та 2.9), можна зробити висновок про залежність ефективності від кожного із визначених показників.

Висновки до розділу

У рамках другого розділу представлено методологію захисту інформації Web-сайту та запропоновано практичні рекомендації захисту інформації Web-сайту. На основі проведеного дослідження здійснено верифікацію результатів.

РОЗДІЛ 3
ЕКОНОМІЧНА ЧАСТИНА

Представлена кваліфікаційна робота розглядає розробку системи захисту інформації Web-сайту. Ціль економічної частини проекту полягає у визначенні економічної ефективності отриманих результатів, їх оцінки, а також трудомісткості роботи. Цей розділ присвячений розрахункам визначення економічної вигоди.

Отже, задля визначення собівартості розробки та терміну окупності необхідно визначити і розрахувати всі витрати, пов'язані з проведенням цієї роботи.

3.1 Розрахунок капітальних витрат на придбання і налагодження складових систем інформаційної безпеки

Трудомісткість розробки і налагодження складових систем інформаційної безпеки визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання і закінчуючи оформленням документації:

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}}, \text{годин}$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку і налагодження складових систем інформаційної безпеки;

$t_{\text{в}}$ – тривалість розробки концепції систем інформаційної безпеки;

$t_{\text{а}}$ – тривалість процесу аналізу ризиків;

$t_{\text{вз}}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{\text{озб}}$ – тривалість вибору основних рішень із забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування систем інформаційної безпеки;

$t_д$ – тривалість документального оформлення політики безпеки.

$$t = 20 + 45 + 60 + 8 + 6 + 22 + 6 = 167 \text{ годин}$$

Витрати на розробку і налагодження складових систем інформаційної безпеки $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з програмування $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки і налагодження складових систем інформаційної безпеки $З_{мч}$:

$$К_{рп} = З_{зп} + З_{мч}$$

$$К_{рп} = 25050 + 859265 = 884315 \text{ грн}$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби та визначається за формулою:

$$З_{зп} = t \cdot З_{іб}, \text{грн}$$

де t – загальна тривалість розробки і налагодження складових систем інформаційної безпеки, годин;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з програмування з нарахуваннями, грн./годину.

$$З_{зп} = 167 \cdot 150 = 25050 \text{ грн}$$

Вартість машинного часу для розробки і налагодження складових систем інформаційної безпеки на ПК визначається за формулою:

$$З_{мч} = t \cdot С_{мч}, грн$$

де t – трудомісткість розробки і налагодження складових систем інформаційної безпеки на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

$$З_{мч} = 167 \cdot 5145{,}3 = 859265 \text{ грн}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р},$$

де P – встановлена потужність ПК, кВт;

$C_е$ – тариф на електричну енергію, грн./кВт година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн..;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн..;

$F_р$ – річний фонд робочого часу.

$$C_{мч} = 450 \cdot 6 \cdot 1{,}90 + \frac{15000 \cdot 1{,}50}{1920} + \frac{5500 \cdot 1{,}25}{1920} = 5130 + 11{,}72 + 3{,}58$$
$$= 5145{,}3 \text{ грн}$$

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первістю та зносом за час використання.

Визначено таким чином вартість розробки і налагодження складових систем інформаційної безпеки $К_{рп}$ є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури систем.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта систем інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн..;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн..;

$К_{рп}$ – вартість розробки і налагодження складових систем інформаційної безпеки, тис. грн..;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн..;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн..;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

$$К = 800 + 50 + 884{,}315 + 25 + 20 + 10 = 1789{,}315 \text{ тис. грн}$$

3.2 Розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування

Річні поточні витрати на функціонування складових систем інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{тис. грн}$$

де $С_в$ – витрати на відновлення та модернізацію системи інформаційної безпеки, тис. грн.;

$С_к$ – витрати на керування системою в цілому, тис. грн.;

$С_{ак}$ – витрати викликані активністю користувачів системи інформаційної безпеки, тис. грн.;

$$С_к = С_н + С_а + С_з + С_е + С_{ел} + С_о + С_{тос}, грн$$

де $С_н$ – навчання персоналу;

$С_а$ – амортизаційні відрахування;

$С_з$ – річний фонд заробітної плати;

$$С_з = З_{осн} + З_{дод}, грн$$

$$С_з = 264000 + 24000 = 288000 грн$$

$С_{ел}$ – вартість електроенергії;

$$С_{ел} = Р \cdot F_р \cdot Ц_е$$

$$С_{ел} = 450 \cdot 1920 \cdot 1{,}9 = 1641600 грн$$

$С_о$ – витрати на залучення;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс.

$$С_к = С_н + С_а + С_з + С_е + С_{ел} + С_о + С_{тос}, грн$$

$$С_к = 25000 + 9000 + 288000 + 1{,}90 + 1641600 + 15000 + 26000 = 2004601{,}9 грн$$

$С_н$ = 25 тис. грн;

$С_а$ = 9 тис. грн;

$С_з$ = 288 тис. грн.;

$С_е$ = 1,9 тис. грн.;

$С_{ел}$ = 1641,6 тис. грн.;

$С_о$ = 15 тис. грн..;

$С_{тос}$ = 26 тис. грн..

$$C = 17{,}8 + 2004{,}602 + 10 = 2032{,}4 \text{ тис. грн}$$

$С_в$ = 17,8 тис. грн

$С_к$ = 2004601,9 грн

$С_{ак}$ = 10 тис. грн..

3.3 Визначення річного економічного ефекту від впровадження об'єкта проектування

Упущена вигода від простою становить:

$$U = П_п + П_в + V$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників, грн..;

$П_в$ – вартість відновлення роботи, грн.;

V – втрати від зниження обсягу продажів, грн.

$$П_п = \frac{\sum З_с}{F} \cdot t_п$$

$$П_п = \frac{46000}{176} \cdot 3 = 784 \text{ грн}$$

$$П_в = П_{ви} + П_{вп} + П_{зч}$$

$$П_в = 2500 + 3600 + 10000 = 16100 \text{ грн}$$

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{12000}{2080} \cdot (3 + 45 + 8) = 323 \text{ грн}$$

$$U = 784 + 16100 + 323 = 17207 \text{ грн}$$

3.4 Визначення на аналіз показників економічної ефективності запропонованого проектного рішення

Загальний ефект від впровадження складових систем інформаційної безпеки становить:

$$E = B \cdot R - C$$

де C – щорічні витрати на експлуатацію системи інформаційної безпеки, C = 10 тис. грн.;

B – загальний збиток від атаки на вузол або сегмент мережі, тис. грн.;

R – очікувана імовірність атаки на вузол або сегмент мережі, тис. грн..

$$E = 17{,}207 \cdot 0.75 - 10 = 2.9 \text{ тис. грн}$$

Щодо ефективності говорять не про прибуток, а про запобігання можливих втрат, отже:

$$ROSI = \frac{E}{K}$$

$$ROSI = \frac{2.9}{2} = 1.45$$

проект є економічно вигідним.

Термін окупності:

$$T_o = \frac{1}{ROSI} = \frac{1}{1,45} = 0,69 \text{ років}$$

3.5 Висновок про економічну доцільність проектного рішення

Таким чином економічні розрахунки показують ефективність впровадження комплексу систем інформаційної безпеки. Відповідно до проведених розрахунків, окупність комплексу систем інформаційної відбудеться ще в першому кварталі їх використання термін окупності складає 0,69 року. Що для підприємства є дуже мінімальним фінансовим навантаженням. Коефіцієнт повернення інвестицій складає 1.45, даний показник показує скільки додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи здійснено дослідження шляхів та вироблення рекомендацій щодо захисту інформації Web-сайту. На основі вищевикладеного варто зробити наступний висновок:

Сайт, або веб-сайт – одна або кілька логічно пов'язаних між собою веб-сторінок, а також місце розташування контенту сервера. Захист сайтів від можливих загроз інформаційної безпеці – важливе завдання для його власника, оскільки можливі такі наслідки, як, наприклад, витік персональних даних, неотримання від потенційних клієнтів прибутку через недоступність сайту, зниження позиції сайту в результатах пошуку, падіння репутації організації тощо.

Світовий досвід створення різних захисних систем незмінно показує: як тільки людство відкриває нові засоби захисту, тут ж знаходяться джерела протидії і руйнування. Вік інформатизації не став винятком. Від розробників новітніх технологій, не відстають зловмисники, які прагнуть знайти уразливості, створюючи засоби загроз і атак. Сучасне підприємство вже не може існувати без захищеної, належним чином, інформаційної системи. На сьогоднішній день інформація стає найбільш цінним ресурсом будь-якої компанії: витік важливих даних про клієнтів або фінансових відомостей може завдати непоправної шкоди репутації і подальшої комерційної діяльності організації.

Міжнародні стандарти управління інформаційною безпекою можуть сприяти зниженню кількості інцидентів, а їх дотримання допомагає перейти на новий рівень управління інформаційної безпекою.

Для автоматизації захисту інформаційних систем оптимально використовувати систему Snort, яка є вільною мережевою системою запобігання вторгнень (IPS) і мережевою системою виявлення вторгнень (IDS).

Інцидент інформаційної безпеки може помітити користувач або адміністратор системи. Але часто цього буває недостатньо, тому необхідно звертатися до автоматизованих систем. Найбільш ефективною для цих цілей представляється система Snort.

Оцінка ризику порушення ІБ дорівнює величині максимального ризику порушення ІБ серед системи забезпечення управління інцидентами інформаційної безпеки цього сегмента, тобто оцінка проводиться по найбільш уразливому компоненту.

Завдання управління ризиками полягає у виборі обгрунтованого набору контрзаходів, що дозволяють знизити рівні ризиків до прийнятної величини. Вартість реалізації контрзаходів повинна бути менше величини можливого збитку. Різниця між вартістю реалізації контрзаходів і величиною можливого збитку повинна бути обернено пропорційна ймовірності заподіяння шкоди.

Технологія запобігання атак на мережевому рівні може бути реалізована тільки за допомогою спеціалізованих мережевих датчиків, структура та алгоритм роботи яких описуються нижче. Мережеві датчики в цьому випадку виконуються у вигляді окремих апаратних блоків, які встановлюються в канали зв'язку таким чином, щоб через них проходив весь мережевий трафік. Для цього датчик оснащується двома мережевими адаптерами, які функціонують у "змішаному" режимі (promiscuous mode) і через які передбачається проходження всієї інформації, що передається в сегменті ІС.

Економічні розрахунки показують ефективність впровадження комплексу систем інформаційної безпеки. Відповідно до проведених розрахунків, окупність комплексу систем інформаційної відбудеться ще в першому кварталі їх використання. Що для підприємства є дуже мінімальним фінансовим навантаженням.

СПИСОК ДЖЕРЕЛ

1. Bahuguna, A., Bisht, R.K., & Pande, J. Country-1eve1 cybersecurity posture assessment: Study and ana1ysis of practices. Information Security Journa1. 2020. № 29 (5). P. 250-266.

2. ISO / IEC 27035:2011, Information techno1ogy – Security techniques – Information security incident management. 2011. 78 p.

3. Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі // В.О. Гнатюк / Безпека інформації. №3 (19). 2020. С. 175-180.

4. Computer Emergency Response Team of Ukraine [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/?page_id=207. (04.12.23)

5. Кінзерявий В.М. Базові показники ефективності роботи команд реагування на кіберінциденти / В.М. Кінзерявий, В.О. Гнатюк // Безпека інформації. Том 20, №2. 2020. С. 193-196.

6. Vinogradov M., Ivanchenko Ye., Gnatyuk V. Method for efficiency assessment of cyberincidents processing by CSIRT // Ukrainian Scientific Journa1 of Information Security, 2017, vo1. 23, issue 1, p. 56-62.

7. Гізун А.І. Аналіз сучасних систем управління кри-зовими ситуаціями / А.І. Гізун, А.О. Корченко, С.О. Скворцов // Безпека інформації. 2015. Т.21. №1. С. 87-101.

8. Корченко А.О. Система виявлення та ідентифікації порушника в інформаційно–комунікаційних мережах // А.О. Корченко, В.В. Волянська, А.І. Гізун / Безпека інформації. 2013. Т.19. №3. С. 158-162.

9. Іванченко Є.В. Базова архітектура експертної системи прогнозування та попередження кризових ситуацій / Є.В. Іванченко, О.В. Гавриленко, А.І. Гізун // Захист інформації. 2012. № 3. С. 94-104.

10. Карпінський М.П. Метод виявлення інцидентів/потенційних кризових ситуацій / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Захист інфо-рмації. 2015. Т.17. №2. С. 124-130.

11. Gizun A. Approaches to Improve the Activity of Computer Incident Response Teams / A. Gizun, V. Gnatyuk, N. Ba1yk, P. Fa1at // Proceedings of the 2015 IEEE 8th Internationa1 Conference on “Inte11igent Data Acquisition and Advanced Computing Systems: Techno1ogy and App1ications” (IDAACS’2015), Warsaw, Po1and, September 24-26, 2015: Vo1. 1. – Pp. 442-447.

12. Карпінський М.П. Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих парамет-рів / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. В.1 (29). С. 76 - 85.

13. Параметры прогнозирования и идентификации вторгнень в информационно-коммуникационных системах / В. Азарсков, А. Гизун, А. Грехов, С. Скворцов // Захист інформації. 2014. 16, № 1. С. 89-95.

14. Gizun A.I. Base parameters of forecasting and identification of computer attacks in information and communication systems / A.I. Gizun, S.I. Topcheev, M.O. Ryabyy // Proceedings the sixth wor1d congress «Aviation in the XXI-st century». «Safety in Aviation and Space Techno1ogies». Vo1. 1. K.: NAU, 2014. P. 1.11.40-1.11.44.

15. Волянська В.В. Моделі еталонів лінгвістичних змінних для систем виявлення та ідентифікації порушника інформаційної безпеки // В.В. Волянська, А.І. Гізун, В.О. Гнатюк / Безпека інформа-ції. №1 (19). 2013. С. 13-21.

16. Mohanty, Suneeta & Sharma, Sourav & Pattnaik, Prasant & Ho1, Ana. (2023). A Comprehensive Review on Cyber Security and On1ine Banking Security Frameworks. 10.4018/978-1-6684-9317-5.ch001.

17. Bang, Kee-Chun. (2014). A Study of Information Security Maturity Measurement Methodo1ogy for Banking System based on Cyber -based Transaction Processing Architecture Diagnosis. Journa1 of Digita1 Contents Society. 15. 10.9728/dcs.2014.15.1.121.

18. Kour, Manjit & Sharma, Nee1am. (2023). Security Issues in e-Banking.

1291-1294. 10.1109/ICAAIC56838.2023.10140397.

19. 1imna, Pongsakorn & Kraiwanit, Tanpat & Siripipattanaku1, Sutithep. (2022). The Re1ationship between Cyber Security Awareness, Know1edge, and Behaviora1 Choice Protection among Mobi1e Banking Users in Thai1and. Internationa1 Journa1 of Computing Sciences Research. 6. 1-19. 10.25147/ijcsr.2017.001.1.123.

20. U11ah, Inam & A1i, Farhad & Nazir, Shah & Khan, Habib & Anwar, M. & Choi, Chang. (2023). Educating Banking Emp1oyees to Ensure Security in the Cyberwor1d. 10.1201/9781003369042-4.

21. Кузнєцов П. В. Сутність проблеми інформаційної безпеки [Електронний ресурс] / П. В. Кузнєцов, С. О. Гринь, Д. М. Дейнека // Topical issues of the development of modern science : abstr. of 4th Intern. Sci. and Practic. Conf., 11-13 December 2019 / ed. M. L. Komarytskyy. – Electron. text data. Sofia, 2019. P. 270-276. – URL: https://sci-conf.com.ua/wp-content/uploads/2019/12/topical-issues-of-the-development-of-modern-science_11-13.12.2019.pdf

22. Karpukhin, E.O. & Gazov, A.I. Application of parametric optimization of linear network code for overload prediction in telecommunication systems. Telecommunications. 2022. P. 34-40. 10.31044/1684-2588-2022-0-9-34-40.

23. Огнєвий О.В., Хмельницький Ю.В. Методи захисту інформаційних ресурсів в телекомунікаційних системах. Хмельницький національний університет: Вісник ХНУ: Економічні науки, 2021. №5 (301). С. 27-31.

24. Afolalu, Adeniran & Ikumapayi, Omolayo & Abdulkareem, Ademola & Emetere, Moses & Adejumo, Olaoluwa. A short review on queuing theory as a deterministic tool in sustainable telecommunication system. Materials Today: Proceedings. 2021. P.44. 10.1016/j.matpr.2021.01.092.

25. Хмельницький Ю., Чешун В., Джулій А., Чорненький В. Використання інформаційних технологій для підвищення якості роботи та

безпеки телекомунікаційних мереж. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. 2022. № 1. С. 36-42.

26. Nenadovich, D. & Markin, I. Methodology for the Formation of Assessment Values of Expert Performance Indicators for Perspective Automated Digital Telecommunication Systems. Vestnik Tambovskogo gosudarstvennogo tehnicheskogo universiteta. 2021. № 27. P.368-379. 10.17277/vestnik.2021.03.pp.368-379.

27. Alvarez, Stephanie & Juan, Angel & Armas, Jésica & Silva, Daniel & Riera, Daniel. (2018). Metaheuristics in Telecommunication Systems: Network Design, Routing, and Allocation Problems. IEEE Systems Journal. PP. 1-10. 10.1109/JSYST.2017.2788053.

28. Гуменюк І. В., Басараба М. С., Некрилов О. В. Методика забезпечення кібербезпеки критичних компонентів інформаційно-телекомунікаційної системи. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2020. С. 101-110. 10.46972/2076-1546.2020.18.10.

29. Ryapukhin, Anatoly & Karpukhin, Evgeny & Zhuikov, Ivan. Method of Forming Various Configurations of Telecommunication System Using Moving Target Defense. Inventions.2022. P. 7. 83. 10.3390/inventions7030083.

30. Казмірчук С., Корченко А., Паращук Т. Аналіз систем виявлення вторгнень // Захист інформації, 2018. Т. 20, № 4. С. 259–276.

31. Пількевич І. А., Бойченко О. С., Гуменюк І. В. Метод децентралізованого управління мережевими ресурсами інформаційно-комунікаційних мереж // Технічна інженерія. Житомир : ДУ “Житомирська політехніка”, 2019. № 2 (84). С. 100–109.

32. Yakymchuk, Natalia & Selepyna, Yosyp & Mykola, Yevsiuk & Prystupa, Stanislav & Moroz, Serhii. MONITORING OF LINK-LEVEL CONGESTION IN TELECOMMUNICATION SYSTEMS USING INFORMATION CRITERIA. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2022. №12. P. 26-30. 10.35784/iapgos.3076.

33. Zuiev, P., Zhyvotovskyi, R., Zvieriev, O., Hatsenko, S., Kuprii, V., Nakonechnyi, O. Development of complex methodology of processing heterogeneous data in intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 2020. № 4 (9 (106)). P. 14–23. doi: http://doi.org/10.15587/1729- 4061.2020.208554

34. Sova, Oleg. Analysis of conditions and factors affecting cyber security in the special purpose information and telecommunication system. Technology audit and production reserves. 2022. №4. P. 25-28. 10.15587/2706-5448.2022.261874.

35. Гуменюк І. В., Басараба М. С., Некрилов О. В. Методика захисту інформації важливих компонентів мережі інформаційно-телекомунікаційної системи // III Всеукр. наук.-техн. конф. “Комп’ютерні технології: інновації, проблеми, рішення” : тези доповідей. Житомир : Житомирська політехніка, 2020. С. 27–28.

36. Yakymchuk, N.M. & Toroshanko, A.I. METHODS OF IDENTIFICATION AND COMPREHENSIVE DIAGNOSIS OF TELECOMMUNICATION SYSTEMS. Collection of scientific works of the Military Institute of Kyiv National Taras Shevchenko University. 2020. P. 58-65. 10.17721/2519-481X/2020/69-06.

37. Naoumov, Valery & Gaidamaka, Yuliya & Yarkina, Natalia & Samouylov, Konstantin. Modeling and Performance Analysis of Telecommunication Systems. 2022. 10.1007/978-3-030-83132-5_1.

38. Shevchenko, D. G. The set of indicators of the cyber security system in information and telecommunication networks of the armed forces of Ukraine. Suchasni informatciini tekhnologii u sferi bezpeki ta oboroni, 2020. № 38 (2). P. 57–62. doi: https://doi.org/ 10.33099/2311-7249/2020-38-2-57-62

39. ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT)

Додаток А. Відомості матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листків	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	3	
5	А4	Літературний огляд за темою дослідження	17	
6	А4	Практичні аспекти захисту інформації WEB-сайту	34	
7	А4	Економічна частина	8	
8	А4	Висновки	2	
9	А4	Список джерел	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

Додаток Б. Перелік документів на оптичному носії

Нікіперович_ОО_125м_22з_2_МР.docx

Додаток В. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку « ».

Керівник розділу, Пілова Д.П.

к.т.н. доц.

Додаток Г

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22з-2 Нікіперовича О.О. на тему: «Дослідження шляхів та вироблення рекомендацій щодо захисту інформації веб-сайту»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 64 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на дослідження шляхів, а також вироблення рекомендацій щодо захисту інформації Web-сайту.

При виконанні кваліфікаційної роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу основних положень теорії захисту інформації, класифікації заходів забезпечення безпеки Web-сайту, а також основних методів і засобів захисту інформації Web-сайту в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було виділено методи і засоби захисту інформації Web-сайту, а також висвітлено загальні аспекти побудови аналітичної системи захисту Web-сайту.

Наукова новизна результатів полягає у дослідженні системи захисту інформації Web-сайту, що виконується у повній відповідності до етапів методу оцінки критичності ситуації та режиму роботи систем.

Практична цінність роботи полягає у тому, що запропоновані рішення можуть бути використані на етапах розвитку Web-сайту.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Нікіперович Олександр Олексійович заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,

к.т.н., доцент **О.В. Герасіна**