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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Високос Максима Андрійовича*

академічної групи *125м-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз реалізацій систем запобігання вторгнень в інформаційних системах вищих навчальних закладів*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доцент Флоров С.В			
розділів:				
спеціальний	ст. викладач Святошенко В.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

ЗАТВЕРДЖЕНО:

завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Високос Максиму Андрійовичу* **академічної групи** *125м-20-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Аналіз реалізацій систем запобігання вторгнень в інформаційних системах вищих навчальних закладів***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 № 1036-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Описати загальну структуру інформаційних систем вищих навчальних закладів, їх сервіси, середовище користувачів, апаратне забезпечення. Виконати модель загроз для загальних інформаційних систем вищих навчальних закладів.	01.10.2021
Розділ 2	Обґрунтувати вибір рішень, що до захисту інформаційної системи. Описати критерії класифікації систем запобігання вторгнень. Зробити аналітичний огляд програмних продуктів систем запобігання вторгнень представлених на ринку. Обрати та обґрунтувати вибір програмних продуктів для захисту інформаційних продуктів Навести приклад реалізацій обраних програмних продуктів в інформаційній системі вищого навчального закладу.	01.11.2021

Розділ 3	Розрахувати капітальні витрати на розробку і впровадження системи запобігання вторгнень. Розрахувати річні експлуатаційні витрати на утримання і обслуговування системи запобігання вторгнень. Оцінити можливі збитки від атаки на сегмент інформаційної системи. Визначити та проаналізувати показники економічної ефективності впровадження системи запобігання вторгнень.	01.12.2021

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

Дата видачі: 01.09.2021р.

Дата подання до екзаменаційної комісії: 18.01.2022р.

Прийнято до виконання _____

_____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 7 рис., 11 табл., 5 додатка, 13 джерел.

Об’єкт дослідження: інформаційні системи вищих навчальних закладів.

Мета роботи: забезпечення безпеки сервісів інформаційних систем вищих навчальних закладів.

Методи розробки: спостереження, аналіз, порівняння, опис.

У першому розділі було проведено аналіз загальної структури інформаційних систем вищих навчальних закладів та її компоненті. Були описані сервіси, середовище користувачів та апаратне забезпечення інформаційних систем. Була розроблена модель загроз інформаційних систем вищих навчальних закладів. Визначено перелік актуальних загроз для інформаційних систем вищих навчальних закладів.

В спеціальній частині кваліфікаційної роботи було виконано обґрунтування доцільності використання систем запобігання вторгнень для забезпечення безпеки інформаційних систем вищих навчальних закладів. Було виконано аналіз програмних продуктів систем запобігання вторгнень представлених на ринку. Було обрано перелік програмних продуктів, що відповідають вимогам інформаційних систем вищих навчальних закладів. Було наведено приклад реалізації систем запобігання вторгнень в інформаційній системі вищого навчального закладу.

В економічному розділі було економічно обґрунтовано доцільність використання обраних програмних продуктів, а також визначено їх економічну ефективність.

Практичне значення роботи полягає в підвищені рівня захисту інформаційних систем вищих навчальних закладів за рахунок впровадження описаних в кваліфікаційній роботі засобів.

Наукова новизна полягає визначені та обґрунтуванні необхідності використання систем запобігання вторгнень в інформаційних системах вищих навчальних закладів. ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, СИСТЕМИ ЗАПОБІГАННЯ ВТОРГНЕНЬ, БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ.

ABSTRACT

Explanatory note: _75 p., 7 fig., 11 tab., 5 additions, 13 sources.

Object of research: information systems of higher educational institutions.

Purpose: ensuring security of information systems services of higher educational institutions.

Development methods: observation, analysis, comparison, description.

In the first part were analyzed the general structure of information systems of higher education institutions and its components. Services, user environment and information systems hardware were described. A model of threats for information systems of higher education institutions was developed. A list of current threats for information systems of higher education institutions has been identified.

In the special part of the qualification work, the substantiation of the expediency of using intrusion prevention systems to ensure the security of information systems of higher education institutions was performed. The analysis of software products of intrusion prevention systems presented on the market was performed. A list of software products that meet the requirements of information systems of higher education institutions was selected. An example of the implementation of intrusion prevention systems in the information system of a higher education institution was given.

In the economic part, the expediency of using the selected software products was economically substantiated, as well as their economic efficiency was determined.

The practical significance of the work is to increase the level of protection of information systems of higher education institutions through the introduction of the tools described in the qualification work.

The scientific novelty is to identify and justify the need to use intrusion prevention systems in the information systems of higher education institutions.

INFORMATIONAL SECURITY, CYBER SECURITY, INVASION PREVENTION SYSTEMS, INFORMATION SYSTEMS SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВНЗ – вищий навчальний заклад;

НД ТЗІ – нормативний документ технічного захисту інформації

IPS (англ. intrusion prevention system) – система запобігання вторгнень

IDS (англ. intrusion detection system) – система виявлення вторгнень

NIPS (англ. network-based intrusion prevention system) – мережева система запобігання вторгнень

HIPS (англ. host-based intrusion prevention system) – система запобігання вторгнень на базі хоста

WIPS (англ. wireless intrusion prevention system) – система запобігання вторгнень для бездротових мереж

NBA (англ. network behavior analysis) – аналізатор поведінки мережі

SIEM (англ. security information and event management) – управління інформаційною безпекою та подіями безпеки

ЗМІСТ

ВСТУП

На сьогоднішній день кількість та різноманіття атак, що здійснюються на інформаційні системи значно збільшилась. Деякі з них стало важко виявити та запобігти. З розвитком штучного інтелекту та програм-ботів, вони почали активно використовуватись в проведенні атак. Для запобігання цих атак вже недостатньо лише людського ресурсу, оскільки швидкість їх проведення значно перевищує швидкість можливої реакції людини. А отже для протидії атакам на інформаційні системи доцільно використовувати автоматизовані системи запобігання вторгнень на боці захисту цих систем. Саме для цих цілей були розробленні системи виявлення вторгнень та системи запобігання вторгнень. Вони здатні виявляти та запобігати вторгнення без попередньої участі людини, а отже і швидкість протидії атакам є значно більшою. На ринку представлено багато варіантів систем запобігання вторгнень з різною функціональністю, та у різних цінових категоріях.

Проте інформаційні системи вищих навчальних закладів не є типовими, вони використовують різні технології для реалізації своїх сервісів. Завданням спеціаліста з інформаційної безпеки є аналіз часткових готових рішень представлених на ринку, вибір необхідних, та доопрацювання їх відповідно до потреб системи, що захищається.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1Короткі відомості про об’єкт, що аналізується

Об’єкт аналізу: загальна інформаційна система вищих навчальних закладів.

Інформаційна система вищих навчальних закладів – це сукупність програмних та технічних ресурсів, що використовуються для збереження, пошуку та обробки інформації з метою можливості виконання закладом вищої освіти своєї діяльності.

Відповідно до Закону України «Про вищу освіту» діяльність вищих навчальних закладів описується наступним переліком:

- наукова та дослідницька діяльність;
- підготовка та атестація наукових та науково-педагогічних кадрів;
- культурно-освітня діяльність;
- методична діяльність;
- здійснення зовнішніх зв’язків;
- видавнича діяльність;
- фінансово-господарська діяльність[2].

Оскільки інформаційні системи вищих навчальних закладів відрізняються за технологіями побудови та наявністю певних сервісів, у цій частині розглянуто їх загальні характеристики спільні для кожної з таких систем.

1.2 Структура інформаційних систем вищих навчальних закладів

Структура інформаційної системи вищих навчальних закладів складається з таких компонентів як:

- сервіси інформаційної системи;
- користувачі інформаційної системи;
- апаратне забезпечення інформаційної системи;

Класифікація та детальний опис сервісів, що надаються інформаційними системами ВНЗ наведено у розділі 1.2.1.

Класифікація та опис користувачів інформаційних систем ВНЗ наведено у розділі 1.2.2.

Перелік та опис апаратного забезпечення інформаційних систем наведено у розділі 1.2.3.

Загальне представлення структури інформаційної системи вищих навчальних закладів надано на рисунку 1.1.

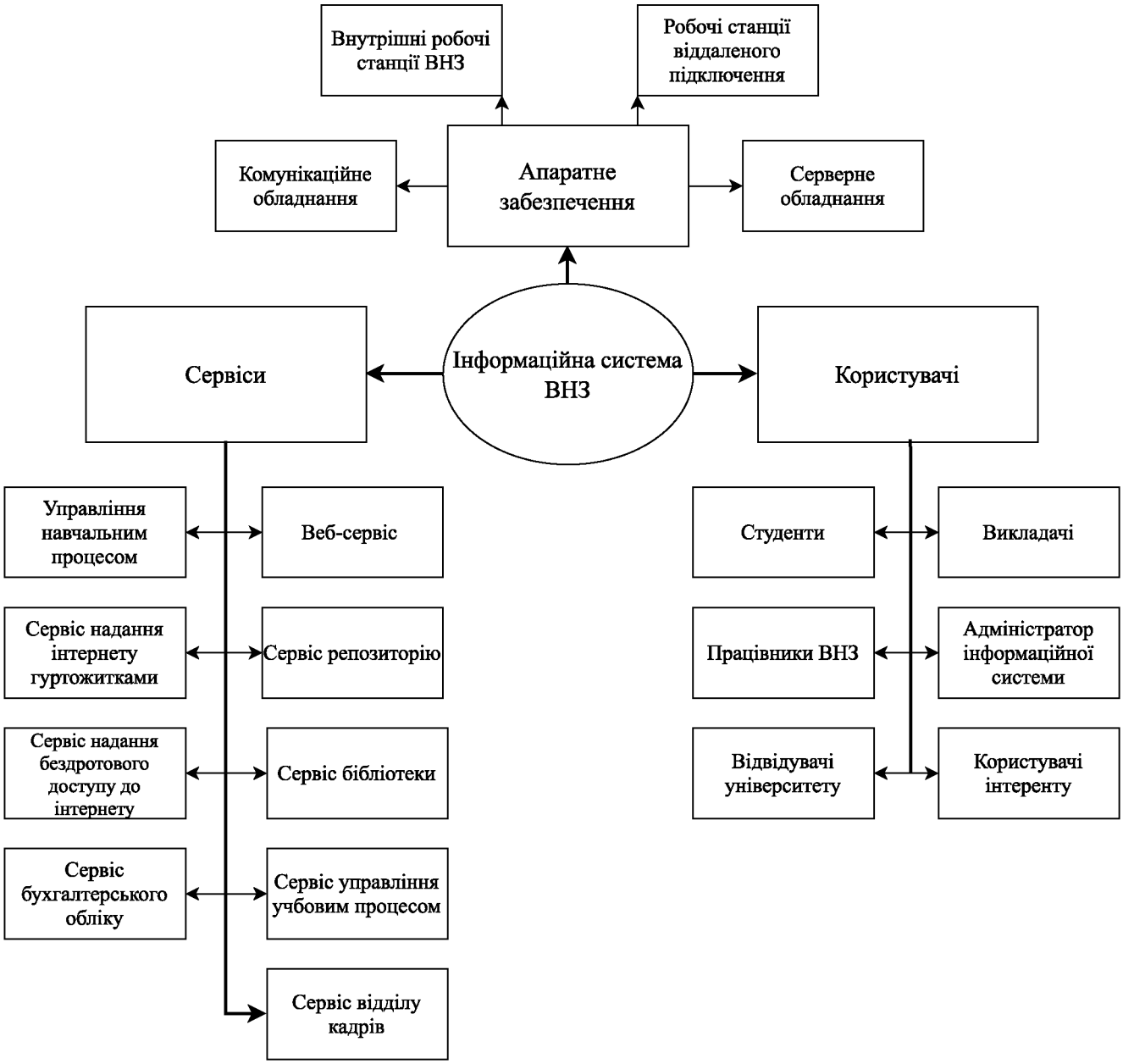

Рисунок 1.1 – Загальна структура інформаційної системи ВНЗ

1.2.1 Класифікація сервісів, що надаються інформаційними системами ВНЗ

Основною задачею будь якої інформаційної системи є обробка, передача та зберігання інформації, а також надання певних сервісів своїм користувачам. Сервіси інформаційних систем ВНЗ поділяють на публічні та внутрішні. Під публічними сервісами розуміють публічні послуги, що можуть отримати будь які

користувачі інтернету. Під внутрішніми сервісами розуміють послуги, що можуть отримати лише обмежений круг користувачів внутрішньої мережі, що мають доступ до цього сервісу.

До публічних сервісів інформаційної системи належать:

- система управління навчанням;
- доступ до веб-ресурсів вищого навчального закладу та його підрозділів;
- сервіс надання інтернету мешканцям гуртожитків вищих навчальних закладів;
- репозиторію документів створених співробітниками та студентами;
- сервіс надання бездротового доступу до інтернету в приміщеннях на території вищого навчального закладу;
- електронного каталогу та інші сервіси бібліотеки.

До внутрішніх сервісів інформаційної системи належать:

- автоматизована система бухгалтерського обліку;
- автоматизована система управління навчальним процесом;
- автоматизована система відділу кадрів.

1.2.1.1 Опис системи навчального процесу

Відповідно до наказу Міністерства освіти та науки України №446 від 25.04.2013 «Про затвердження Положення про дистанційне навчання» вищі навчальні заклади зобов'язані здійснювати організаційне та науково-технічне забезпечення дистанційного навчання [3]. З цією метою в інформаційній системах вищих навчальних закладів існує система управління навчанням. Цей сервіс надає послугу доступу до начальних ресурсів для студентів вищих навчальних закладів. Сервіс є публічним оскільки він надає вільний доступ до переліку курсів ВНЗ для всіх охочих. Однак доступ до змісту матеріалів курсів зазвичай надається лише для авторизованих користувачів.

1.2.1.2 Опис сервісу доступу до веб-ресурсів

Відповідно частини першої статті 79 Закону України «Про вищу освіту», інформація про процедури та результати прийняття рішень і провадження

діяльності у сфері вищої освіти підлягає обов'язковому оприлюдненню на офіційних веб-сайтах та у засобах масової інформації, на інформаційних стендах та в будь-який інший спосіб.[2] З цією метою в інформаційних системах вищих навчальних закладів використовується сервіс доступу до веб-ресурсів. Основною послугою сервісу доступу до веб-ресурсів є надання доступу до веб-сайтів вищих навчальних закладів, а також їх підрозділів. На веб-сайтах ВНЗ зазвичай розміщується інформація для абітурієнтів, студентів, співробітників, а також загальні новини про діяльність університету.

1.2.1.3 Опис сервісу надання інтернету мешканцям гуртожитків вищих навчальних закладів

В нинішніх умовах використання інтернету для навчання є однією з основних потреб. А отже вищим навчальним закладам необхідно забезпечувати доступ до інтернету для мешканців їх гуртожитків. З цією метою в інформаційних системах ВНЗ використовується сервіс надання інтернету мешканцям гуртожитків. Цей сервіс дозволяє відключати та підключати певних абонентів провайдеру, а також надає можливість продивлятися данні про оплату за інтернет та тарифи цим абонентам. Хоча сервіс є публічним зазвичай, доступ до інформації про оплату за інтернет надається лише для авторизованих користувачів.

1.2.1.4 Опис сервісу репозиторію документів створених співробітниками та студентами

Відповідно до частини другої статті 16 Закону України «Про вищу освіту» вищі навчальні заклади зобов'язані здійснювати щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників закладу вищої освіти та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті закладу вищої освіти, на інформаційних стендах та в будь-який інший спосіб.[2] З цією метою в інформаційних системах ВНЗ існує сервіс репозиторію. Цей сервіс використовується для надання послуг зберігання да публічного представлення кваліфікаційних та наукових робіт студентів та співробітників

університету. Сервіс дозволяє продивлятися ці данні без необхідності попередньої авторизації.

1.2.1.5 Опис сервісу надання бездротового доступу до інтернету в приміщеннях та на території ВНЗ

Зручною практикою останніх часів є наявність бездротової мережі на території ВНЗ. Студенти, викладачі, працівники та відвідувачі вищих навчальних закладів мають можливість підключення до цієї мережі с подальшою можливістю виходу в зовнішній інтернет для своїх потреб. З цією метою в інформаційній системі використовується сервіс надання доступу до бездротового інтернету на територій вищого навчального закладу. Зазвичай бездротова мережа поширюється по всій території університету та надає безкоштовний відкритий доступ до інтернету. Для цих цілей по всій території університету розміщена певна кількість точок доступу підключених до спільних комутаторів або маршрутизаторів.

1.2.1.6 Опис сервісу електронного каталогу та інших сервісів бібліотеки

В кожному вищому навчальному закладі існує науково-технічна бібліотека, що надає студентам можливість використання своїх ресурсів для навчання. Сервіс електронного каталогу та інші сервіси бібліотеки ВНЗ використовується для надання каталогу архіву документів та книг, представлених у бібліотеці цього закладу та загального представлення інформації о цих документах та книгах.

1.2.1.7 Опис автоматизованої системи бухгалтерського обліку

Як було описано вище фінансово-господарська діяльність є однією з основних для вищих навчальних закладів. Для контролю та управління цією діяльністю в кожному ВНЗ існує бухгалтерській відділ. Автоматизована система бухгалтерського обліку забезпечує управління бухгалтерською звітністю вищих навчальних закладів. Цей сервіс зазвичай являє собою відокремлену від іншої інформаційної системи локальну мережу з обмеженим доступом.

1.2.1.8 Опис автоматизованої системи управління навчальним процесом

Однією з функцій вищих навчальних закладів є освітня діяльність. Основним аспектом освітньої діяльності є можливість оцінювання здобувачів вищої освіти. Автоматизована система управління навчальним процесом надає послуги обліку успішності навчання студентів ВНЗ. Деякі викладачі вищих навчальних закладів мають можливість внесення і редагування інформації про оцінювання студентів. На основі цих даних є можливість створення звітів для окремих груп та студентів.

1.2.1.9 Опис автоматизованої системи відділу кадрів

Автоматизована система відділу кадрів надає можливість обліку працівників та студентів ВНЗ. Цей сервіс використовується співробітниками відповідного відділу вищого навчального закладу.

1.2.2 Опис середовища користувачів інформаційних систем ВНЗ

Користувачі інформаційної системи вищого навчального закладу поділяються на:

- внутрішніх;
- зовнішніх.

До внутрішніх користувачів належать:

- студенти;
- викладачі;
- працівники ВНЗ;
- адміністратори інформаційних систем.

До зовнішніх користувачів належать:

- відвідувачі ВНЗ;
- користувачі інтернету.

Студенти та викладачі це користувачі, що використовують інформаційну систему ВНЗ задля здійснення освітньої діяльності. Під працівниками вищого навчального закладу мають на увазі співробітників певного відділу ВНЗ, що в своїй роботі користуються певними сервісами інформаційної системи. Прикладами можуть бути працівники відділу кадрів або відділу бухгалтерії, що в своїй роботі

використовують відповідно автоматизовану систему відділу кадрів та автоматизовану систему бухгалтерського обліку. Адміністратори інформаційної системи це працівники ВНЗ, що мають повноваження управління, редагування та оновлення сервісів та апаратного обладнання інформаційної системи. Вони відповідають за коректну роботу програмних та апаратних засобів інформаційної системи. Відвідувачі ВНЗ це люди, що мають можливість знаходження на території вищого навчального закладу, проте які не є його штатом. Користувачі інтернету це будь які люди, що мають можливість доступу до публічних ресурсів інформаційної системи ВНЗ за допомогою інтернету.

Оскільки система управління навчанням, сервіс доступу до веб-ресурсів, сервіс надання інтернету мешканцям гуртожитків ВНЗ, сервіс репозиторію, сервіс надання бездротового доступу до інтернету на території ВНЗ та сервіс бібліотеки є публічними сервісами, доступ до них є у всіх користувачів інформаційної системи ВНЗ.

Автоматизована система бухгалтерського обліку, автоматизована система управління навчальним процесом, та автоматизована система відділу кадрів є закритими сервісами, доступ до цих сервісів є у обмеженого числа користувачів інформаційної системи ВНЗ.

Зіставлення користувачів інформаційної системи ВНЗ та відповідних сервісів, до яких вони мають доступ представлено в таблиці 1.1.

Таблиця 1.1 – Доступ користувачів інформаційної системи до її сервісів

Користувачі	1	2	3	4	5	6	7	8	9
Студенти	+	+	+	+	+	+	–	–	–
Викладачі	+	+	+	+	+	+	–	+	–
Працівники ВНЗ	+	+	+	+	+	+	+	+	+
Адміністратор інформаційної системи	+	+	+	+	+	+	+	+	+
Відвідувачі ВНЗ	+	+	+	+	+	+	–	–	–

Користувачі інтернету	+	+	+	+	+	+	–	–	–

Перелік умовних позначень:

- 1 – система управління навчанням;
- 2 – сервіс доступу до веб-ресурсів вищого навчального закладу та його підрозділів;
- 3 – сервіс надання інтернету мешканцям гуртожитків ВНЗ;
- 4 – сервіс репозиторію;
- 5 – сервіс надання бездротового доступу до інтернету на території ВНЗ;
- 6 – сервіс електронного каталогу та інші сервіси бібліотеки;
- 7 – автоматизована система бухгалтерського обліку;
- 8 – автоматизована система управління навчальним процесом;
- 9 – автоматизована система відділу кадрів.

1.2.3 Опис апаратного забезпечення інформаційної системи вищих навчальних закладів

До апаратного забезпечення інформаційних систем ВНЗ належать:

- комунікаційне обладнання;
- внутрішні робочі станції вищих навчальних закладів;
- робочі станції віддаленого підключення;
- серверне обладнання.

До комунікаційного обладнання належать маршрутизатори, комутатори та точки доступу, що використовуються для побудування внутрішньої фізичної мережі ВНЗ. Комунікаційне обладнання зазвичай встановлюється в контрольованих приміщеннях.

До внутрішньої мережі підключаються внутрішні робочі станції ВНЗ, що являють собою комп'ютери розташовані в кабінетах та аудиторіях вищого навчального закладу. В загальному випадку доступ до робочих станцій надається лише для авторизованих в мережі користувачів.

Робочі станцій віддаленого підключення це власні пристрої користувачів інформаційної системи з яких вони мають можливість підключитися до інформаційної системи ВНЗ. З загальному випадку підключення відбувається до внутрішньої мережі ВНЗ за допомогою сервісу надання бездротового доступу до інтернету, або до публічних сервісів інформаційної системи за допомогою інтернету. Прикладами можуть бути мобільні пристрої та ноутбуки підключені до бездротової мережі ВНЗ та стаціонарні комп'ютери, що знаходяться за межами ВНЗ та використовують інтернет для підключення до веб-сервісу.

Серверне обладнання використовується для розміщення на ньому певної кількості сервісів інформаційної системи. В загальному випадку це обладнання встановлюється в контрольованому приміщені, з обмеженим доступом сторонніх осіб.

1.3 Розробка моделі загроз інформаційних систем вищих навчальних закладів

Відповідно до НД ТЗІ 1.1-003-99, модель загроз – це абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз. [4]

Розробка моделі загроз відбувається завдяки виявленню та аналізу таких критеріїв як:

- джерела загроз;
- вразливості інформаційної системи.

Для кожного критерію визначається найбільші показники, що визначають перелік найбільш актуальних джерел загроз та вразливостей інформаційних систем. Наступним кроком відбувається їх зіставлення результатом якого є перелік найбільш актуальних загроз інформаційних систем.

Аналіз джерел загроз представлений у розділі 1.3.1.

Аналіз вразливостей інформаційних систем надано у розділ 1.3.2.

Виявлення та аналіз загроз інформаційної системи надано у розділ 1.3.3.

1.3.1 Аналіз джерел загроз інформаційних систем ВНЗ

Джерела загроз поділяють на антропогенні, техногенні та стихійні. Антропогенні джерела це джерела, що обумовлені діями людей. До техногенних належать загрози, що обумовленні технічними засобами інформаційної системи. Стихійні джерела це джерела, що обумовлені діями природних катаклізмів. Антропогенні та техногенні джерела в свою чергу поділяються на внутрішні по відношенню до інформаційної системи та зовнішні.

До внутрішніх антропогенних джерел належать:

- студенти ВНЗ;
- викладачі;
- працівники ВНЗ;
- адміністратори інформаційної системи.

До зовнішніх антропогенних джерел належать:

- відвідувачі ВНЗ;
- кримінальні угрупування;
- ентузіасти у сфері проникнення до інформаційних систем;
- загальні користувачі інтернету.

До внутрішніх техногенних джерел належать:

- апаратне забезпечення інформаційної системи;
- програмне забезпечення інформаційної системи.

До зовнішніх техногенних джерел належать:

- системи ліній мережі Інтернет;
- системи ліній електропостачання.

До стихійних джерел загроз належать:

- повені;
- пожежі;
- землетруси,
- інші форс-мажорні обставини.

Для визначення показників небезпечності кожного джерела загрози використовують наступну формулу:

$$Кнеб(д) = \frac{(К1 \times К2 \times К3)}{125}$$

де Кнеб(д) – показник небезпеки джерела загрози;

К1 – коефіцієнт доступності джерела загрози;

К2 – коефіцієнт кваліфікації, привабливості здійснення діянь, або наявності необхідних умов;

К3 – коефіцієнт фатальності джерела загрози[5].

Можливе значення для кожного коефіцієнту складає від 1 до 5, в залежності від ступеня небезпечності.

Детальний опис ступенів небезпечності коефіцієнту доступності джерела загрози надано в таблиці 1 додатку Д.

Детальний опис ступенів небезпечності коефіцієнту кваліфікації, привабливості здійснення діянь, або наявності необхідних умов надано в таблиці 2 додатку Д.

Детальний опис степенів небезпечності коефіцієнту фатальності джерела загрози надано в таблиці 3 додатку Д.

Перелік коефіцієнтів джерел загроз, а також результати обчислення їх показників небезпеки надано в таблиці 1.2.

Перелік актуальних джерел загроз надано в таблиці 1.3.

Таблиця 1.2 – Ранжування джерел загроз інформаційних систем ВНЗ

Джерело загрози	К1	К2	К3	Кнеб(д)
Антропогенні внутрішні				
Студенти ВНЗ	4	3	4	0.38
Викладачі ВНЗ	4	2	3	0.19
Працівники ВНЗ	4	2	3	0.19
Адміністратори інформаційної системи	5	4	4	0.64
Антропогенні зовнішні				

Відвідувачі університету	2	1	2	0.03
Хакерські угрупування	3	1	4	0.09
Ентузіасти у сфері проникнення до інформаційних систем	3	3	4	0.29
Загальні користувачі інтернету	2	1	2	0.03
Техногенні внутрішні				
Апаратне забезпечення інформаційної системи	4	2	3	0.19
Програмне забезпечення інформаційної системи	4	2	3	0.19
Техногенні зовнішні				
Системи ліній мережі інтернет	2	2	2	0.06
Системи ліній електропостачання	2	1	2	0.03
Стихійні				
Повені	2	3	3	0.14
Пожежі	2	2	3	0.09
Землетруси	2	1	2	0.03
Інші форс-мажорні обставини	2	2	3	0.09

Таблиця 1.3 – Перелік актуальних джерел загроз

Джерело загрози	К1	К2	К3	Кнеб(д)
Студенти ВНЗ	4	3	4	0.38
Адміністратори інформаційної системи	5	4	4	0.64

Ентузіасти у сфері проникнення до інформаційних систем	3	3	4	0.29

1.3.2 Аналіз вразливостей інформаційних систем вищих навчальних закладів

Вразливості інформаційної системи подіяють на:

- об'єктивні;
- суб'єктивні;
- випадкові[5].

Для інформаційних систем ВНЗ існує наступний перелік об'єктивних вразливостей:

- вразливості програмного забезпечення встановленого в інформаційній системі;
- вразливості мережевої архітектури інформаційної системи.

До суб'єктивних вразливостей інформаційних систем ВНЗ належать:

- помилки налаштування конфігурації мережевого обладнання;
- організаційні вразливості інформаційної системи.

До випадкових вразливостей інформаційних системи ВНЗ належать:

- збій в роботі програмного забезпечення;
- збій в роботі апаратного забезпечення.

Для визначення показників небезпеки для кожної вразливості інформаційної системи використовують наступну формулу:

$$\text{Кнеб(в)} = \frac{(\text{К1} + \text{К2} + \text{К3})}{125}$$

де Кнеб(в) – показник небезпеки для кожної вразливості інформаційної системи

К1 – коефіцієнт фатальності вразливості;

К2 – коефіцієнт зручності використання вразливості;

К3 – коефіцієнт кількості елементів, яким характерна вразливість.

Коефіцієнт кожної вразливості може мати значення від 1 до 5 в залежності від небезпеки вразливості.

Перелік коефіцієнтів кожної вразливості, а також результати обчислень показників небезпеки вразливостей надано в таблиці 1.4.

Перелік актуальних вразливостей надано в таблиці 1.5.

Таблиця 1.4 – Ранжування вразливостей інформаційних системи ВНЗ

Вразливість інформаційних систем ВНЗ	К1	К2	К3	Кнеб(в)
Об’єктивні вразливості				
Вразливості програмного забезпечення встановленого в інформаційній системі	4	4	4	0.51
Вразливості мережевої архітектури інформаційної системи	4	4	4	0.51
Суб’єктивні вразливості				
Помилки налаштування конфігурації мережевого обладнання	3	4	4	0.38
Організаційні вразливості інформаційної системи	2	3	2	0.09
Випадкові вразливості				
Збій в роботі програмного забезпечення інформаційної системи	3	2	4	0.19
Збій в роботі апаратного забезпечення інформаційної системи	3	2	4	0.19

Таблиця 1.5 – Перелік актуальних вразливостей інформаційних систем ВНЗ

Вразливість інформаційних систем ВНЗ	К1	К2	К3	Кнеб(в)
Вразливості програмного забезпечення встановленого в інформаційній системі	4	4	4	0.51
Вразливості мережевої архітектури інформаційної системи	4	4	4	0.51
Помилки налаштування конфігурації мережевого обладнання	3	4	4	0.38

1.3.3 Зіставлення джерел загроз та вразливостей інформаційних систем ВНЗ

Після виконання аналізу джерел загроз та вразливостей інформаційних систем вищих навчальних закладів отримано перелік актуальних джерел загроз та вразливостей для цих систем.

До актуальних джерел загроз належать:

- студенти ВНЗ;
- адміністратор інформаційної системи ВНЗ;
- ентузіасти у сфері проникнення до інформаційних систем.

До актуальних вразливостей належать:

- вразливості мережевої архітектури;
- вразливості програмного забезпечення;
- помилки налаштування конфігурації мережевого обладнання.

Зіставлення актуальних джерел загроз з вразливостями інформаційної системи наведено в таблиці 1.6.

Зіставлення відбувається шляхом помноження показників небезпеки актуальних джерел загроз з показниками небезпеки актуальних вразливостей, за формулою:

$$Кнеб = Кнеб(д) \times Кнеб(в)$$

Таблиця 1.6 – Зіставлення джерел загроз та вразливостей інформаційних систем

Джерело загрози	Вразливість	Кнеб(д)	Кнеб(в)	Кнеб
Студенти ВНЗ	Вразливості мережевої архітектури	0.38	0.51	0.19
	Вразливості програмного забезпечення		0.51	0.19
	Помилки налаштування конфігурації мережевого обладнання		0.38	0.14
Адміністратор інформаційної системи	Вразливості мережевої архітектури	0.64	0.51	0.32
	Вразливості програмного забезпечення		0.51	0.32
	Помилки налаштування конфігурації мережевого обладнання		0.38	0.24

Ентузіасти у сфері проникнення до інформаційних систем	Вразливості мережевої архітектури	0.29	0.51	0.14
	Вразливості програмного забезпечення		0.51	0.14
	Помилки налаштування конфігурації мережевого обладнання		0.38	0.11

Таблиця 1.7 – Перелік актуальних загроз інформаційної системи

Загроза	Джерело загрози	Вразливість	Наслідки
Несанкціоноване внутрішнє підключення до інформаційної системи	Студенти ВНЗ, Адміністратор інформаційної системи	Вразливості мережевої архітектури, вразливість програмного забезпечення	Репутаційні або фінансові витрати для університету
Несанкціоноване віддалене підключення до інформаційної системи	Ентузіасти у сфері проникнення до інформаційних систем	Вразливості мережевої архітектури, вразливості програмного забезпечення	Репутаційні або фінансові витрати для університету.

1.4 Висновок

У першій частині кваліфікаційної роботи було виконані такі задачі:

- проаналізовано загальну структуру інформаційної системи вищих навчальних закладів;
- розроблено модель загроз для загальних інформаційних систем ВНЗ.

Уході виконання роботи було визначено, що найбільшу загрозу для інформаційної системи складає несанкціоноване вторгнення в інформаційну систему з використанням вразливостей мережевої архітектури та вразливостей програмного забезпечення.

Виходячи з переліку актуальних загроз можна сказати, що для захисту аналізованої інформаційної системи найбільш прийнятним рішенням є комбінація програмних засобів систем управління безпекою та подіями безпеки, а також систем запобігання вторгнення для нейтралізації виявлених подій. У другій частині диплому необхідно провести аналіз цих систем для обрання найкращого варіанту.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Обґрунтування вибору рішення, що до захисту інформаційної системи вищих навчальних закладів

На сьогоднішній день більшість інформаційних систем вищих навчальних закладів, має розподілений вигляд. Її компоненти територіально розташовані у різних корпусах ВНЗ, що можуть знаходитися як поруч один з одним так і на віддаленій відстані. Відповідно до моделі загроз розробленій у першому розділі кваліфікаційної роботи найбільшу загрозу для інформаційних систем ВНЗ становить несанкціоноване внутрішнє та віддалене підключення до цієї інформаційної системи. Задля своєчасного виявлення цієї загрози, а також для загального контролю безпеки інформаційної системи найбільш доцільним рішенням є системи управління безпекою та подіями безпеки. Вони дають змогу виявлення та централізованого аналізу усіх подій безпеки інформаційної системи ВНЗ. Окрім виявлення подій, що пов'язані з шкідливою активністю, системи управління безпекою та подіями безпеки дозволяють виявляти помилки конфігурації інформаційної системи, а також сигналізувати про вихід з ладу обладнання цієї системи. Все це дозволяє обмежити кількість людей необхідних для моніторингу безпеки та конфігурації системи, що є важливим для державних установ, таких як вищі навчальні заклади.

Проте значні розміри інформаційних систем ВНЗ, велика швидкість проведення атак, а також обмеженість людських ресурсів можуть значно уповільнити швидкість реакції на виявлені події SIEM систем. Це може привести до реалізації відповідних загроз, що завдасть збитків вищим навчальним закладам. З метою автоматизації реакції на виявленні події системи управління безпекою та подіями безпеки в парі з нею доцільно використовувати системи запобігання вторгнень. Такі IPS системи дозволяють налаштувати автоматичну реакцію без попередньої участі людини на відповідні виявлення SIEM систем.

На даних момент не існує готових рішень, щодо забезпечення безпеки інформаційних систем ВНЗ. Проте нині на ринку представлено багата кількість

окремих програмних продуктів SIEM та IPS систем з різними функціями та у різному ціновому діапазоні. Детальний опис та аналіз переліку цих систем надано у розділі 2.2.

2.2 Аналіз та класифікація програмних продуктів SIEM та IPS систем представлених на ринку

Проаналізувавши ринок було обрано перелік програмних продуктів SIEM та IPS систем. Серед них існує як комплексні рішення які відповідають функціоналу SIEM систем, так і часткові рішення, що відповідають функціональності IPS систем.

До часткових програмних рішень в переліку аналізованих систем належать:

- Snort
- Suricata
- Wazuh
- OSSEC
- Fail2ban

До комплексних рішень в переліку аналізованих систем належать:

- Security Onion
- SELKS
- Qradar.

Детальний перелік програмних компонентів, що аналізуються надано в таблиці 2.1.

Таблиця 2.1 – Перелік програмних компонентів, що аналізуються

Назва	Виробник	Тип системи	Актуальна версія
Snort	Sourcefire	NIPS	2.9.19
Suricata	Open Information Security Foundation	NIPS	6.0.4
Wazuh	Wazuh Ink.	HIDS	4.2.5
OSSEC	Trend Micro	HIDS	3.6.0

Fail2ban	Cyril Jaquier	HIPS	0.11.2
Security Onion	Security Onion Solutions, LLC	SIEM	2.3.91
SELKS	Stamus Networks, LLC.	SIEM	6.0.0
Qradar	IBM	SIEM	7.4.3.

Оскільки основною метою аналізу є вибір програмного продукту для запобігання вторгнень в інформаційну систему, у розділі 2.2.1 представлена класифікація систем запобігання вторгнень.

Детальний опис кожного з програмних продуктів представлено у розділі 2.2.2.

2.2.1 Класифікація систем запобігання вторгнень.

Класифікація IPS систем відбувається за наступними критеріями:

- принцип реалізації IPS систем;
- методика виявлення вторгнень.

Детальний опис критеріїв класифікації IPS систем за принципом реалізації надано у розділі 2.2.1.1.

Детальний опис критеріїв класифікації IPS систем за методикою виявлення представлено у розділі 2.2.1.2.

У розділі 2.2.1.3 надано додаткові критерії аналізу IPS систем.

2.2.1.1 Класифікація IPS систем за принципом реалізації

За принципом реалізації IPS системи поділяються на наступні типи:

- мережеві системи запобігання вторгнень;
- системи запобігання вторгнень на базі хоста;
- системи запобігання вторгнень для бездротових мереж;
- аналізатори поведінки мережі.

Зіставлення аналізованих програмних продуктів з критеріями класифікації за принципом реалізації надано в таблиці 1 додатку Е.

Мережева система запобігання вторгнення - це система, що працює на рівні мережі та використовується для моніторингу її безпеки. Основна функція NIPS полягає у відстеженні в мережі злоякісної активності або підозрілого трафіку, з подальшою можливістю його блокування.

Мережеві IPS дозволяють виявляти атаки типу відмова у обслуговуванні, сканування портів, експлойти, та шкідливе програмне забезпечення. NIPS має можливість зміни комп'ютерного трафіку, а отже у разі виявлення підозрілої події може активно запобігати та блокувати її. Задля протидії вторгненням мережева IPS може відкидати шкідливі пакети, повідомляти про тривогу, розривати з'єднання, блокувати пакети з неправильних IP адресів, виправляти помилки знаходження контрольної суми, змінювати небажані параметри транспортного та мережевого рівня, дефрагментувати потоки пакетів та усувати проблеми з послідовністю TCP. Перелік правил щодо реакції NIPS на різні виявлення задаються заздалегідь постачальниками NIPS або адміністратором системи. Приклад зображення архітектури мережевої системи запобігання вторгнень представлено на рисунку 2.1.

Система запобігання вторгнень на базі хоста - це система, що працює на рівні кінцевих вузлів мережі та використовується для захисту ресурсів розташованих на цьому вузлі. Виявлення вторгнень в IPS на базі хоста відбувається шляхом аналізу характеристик та різних подій вузла на наявність шкідливої активності. До об'єктів аналізу HIPS належать файли конфігурації вузла, файли журналів подій, системні виклики, журнали та конфігурація додатків встановлених на вузлі, компоненти файлової системи, а також стан пам'яті, ядра та виконання процесів. Для кожного об'єкту HIPS створює контрольну суму вмісту, запам'ятовує атрибути та зберігає ці данні для подальшого порівняння з актуальними об'єктами.

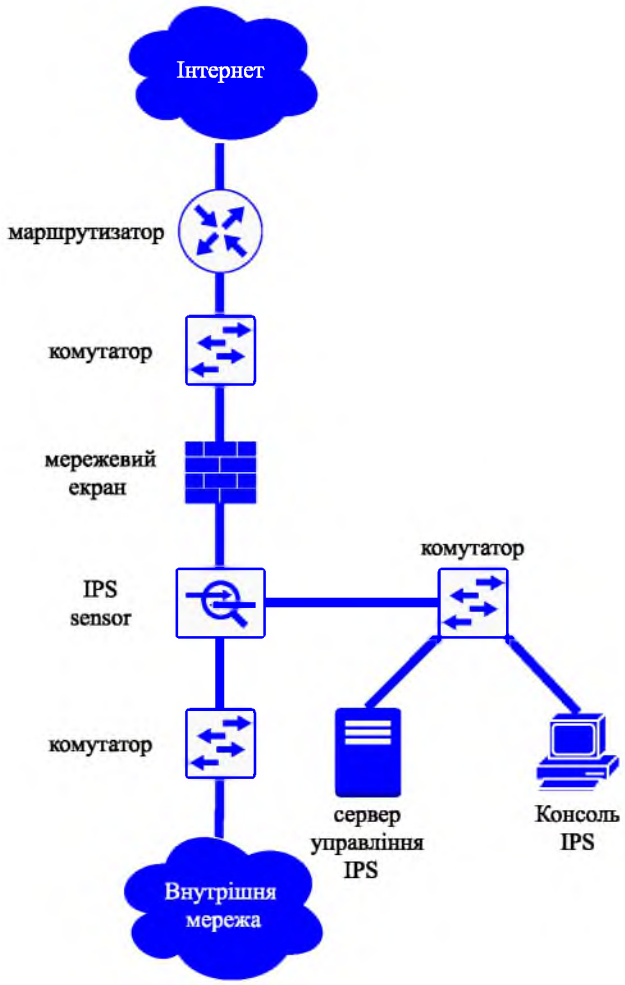

Рисунок 2.1 – Приклад архітектури мережевої IPS системи

Для якісної протидії вторгненням рішення HIPS встановлюються на кожен вузол мережі, що захищається. Для централізованого керування HIPS на всіх вузлах мережі використовується модуль централізованого керування. Реалізація HIPS повинна забезпечувати шифрування обміну даними між HIPS на вузлах та модулем централізованого керування. Приклад зображення архітектури системи запобігання вторгнень на базі хоста представлено на рисунку 2.2.

Система запобігання вторгнень для бездротових мереж - це система що працює на рівні бездротової мережі та використовується для моніторингу її безпеки.

Виявлення вторгнень в IPS для бездротових мереж відбувається завдяки аналізу радіочастотного спектру у пошуках несанкціонованого доступу до мережі зі сторони бездротових пристроїв. Аналіз відбувається шляхом виявлення MAC-адресів усіх підключених до бездротової мережі точок доступу, та подальшому

порівнянні їх з переліком відомих сигнатур заздалегідь авторизованих в мережі точок доступу. Задля усунення проблеми підробки MAC-адреса сучасні реалізації WIPS систем окрім частотного аналізу використовують також інші методі виявлення такі як класифікація та каталогізація усіх відомих бездротових пристроїв та їх унікальних радіочастотних сигнатур.

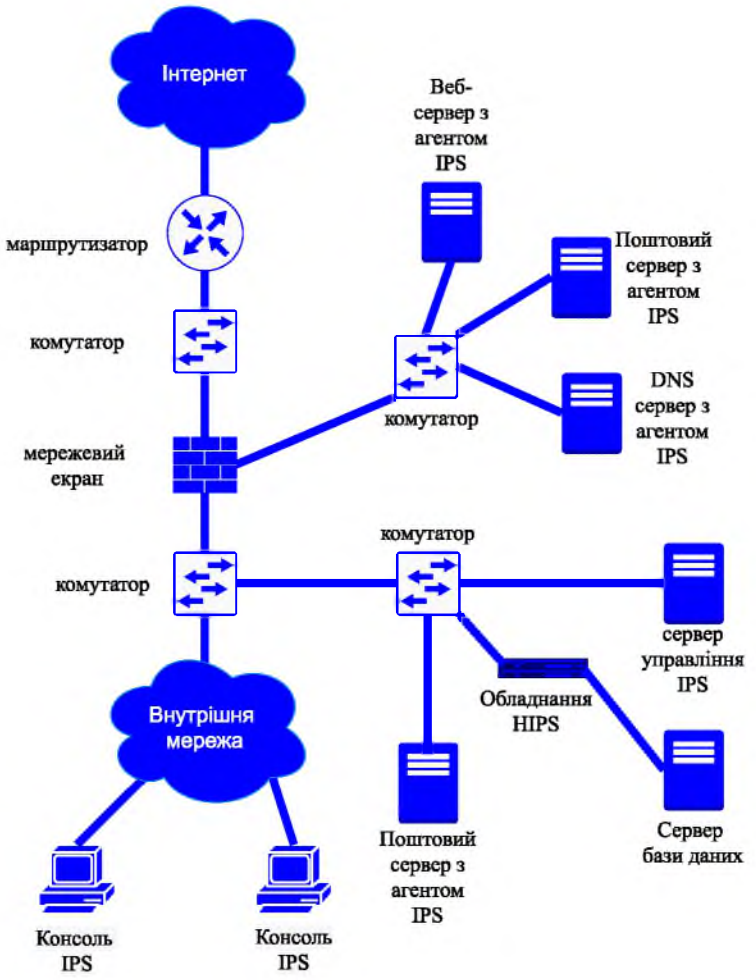

Рисунок 2.2 –Приклад архітектури IPS системи на базі хоста

У разі виявлення несанкціонованих точок доступу або підозрілих бездротових пристроїв підключених до бездротової мережі, WIPS автоматично блокує можливість з'єднання з цією точкою або пристроєм, а також повідомляє адміністратора системи про можливу загрозу. Система WIPS здатна запобігти такі атаки на бездротову мережу як атака “людина посередині”, атака з підміною MAC-адресу, атака з несанкціонованою точкою доступу, атака тупу відмова у обслуговуванні, а також атака типу “злі близнюки”. Правила реакції системи на різні виявлені загрози задаються заздалегідь адміністратором системи. Окрім

виявлення та блокування атак IPS для бездротових мереж здатна також проводити моніторинг мережі на наявність можливих помилок в конфігурації точок доступу.

Аналізатор поведінки мережі - це система IPS, що працює на рівні мережі та використовується для виявлення аномалій поведінки цієї мережі. Аномальна поведінка мережі може бути ознакою шкідливої активності, неправильної конфігурації мережевого обладнання або порушення його роботи. Аналізатор поведінки мережі допомагає виявити джерело аномальної активності, а також запобігти або усунути його.

Виявлення відбувається завдяки збору та детальному аналізу мережевих даних у різних точках мережі. Аналіз відбувається шляхом порівняння поточної активності мережі з базовою активністю. Система NBA проводить порівняння за такими характеристиками як кількість підключень та об'єм переданого трафіку до різних вузлів мережі, зміни смуги пропускання, а також зміни протоколів передачі даних всередині мережі. У разі виявлення джерела аномальної активності NBA може автоматично вжити заходи щодо його усунення у відповідності до правил, визначених заздалегідь адміністратором системи.

Як і мережеві системи запобігання вторгненням, аналізатор поведінки мережі займається відстеженням та блокуванням злоякісної активності мережі. Однак їх основна відмінність полягає в тому, що система NIPS більше орієнтована на аналіз пакетів, що передаються в мережі, а система NBA на аналіз параметрів мережі та мережевих підключень. Проте на даний момент багато продуктів NIPS об'єднують у собі функції обох систем.

2.2.1.2 Класифікація IPS систем за методикою виявлення

У якості методики виявлення IPS системи можуть використовувати наступні режими:

- виявлення на основі сигнатур;
- виявлення на основі аномалій;
- виявлення на основі аналізу стану протоколів.

Зіставлення аналізованих програмних продуктів з критеріями класифікації за методикою виявлення надано в таблиці 2 додатку Е.

Виявлення на основі сигнатур відбувається шляхом порівняння пакетів, які проходять крізь мережу або файлових систем вузлів з заздалегідь відомим переліком загроз, сигнатур атак та індикаторів компрометації. Індикатори компрометації – це комплекс ознак шкідливої активності, що взаємодіють між собою. У мережевій системі запобігання вторгненням ознаками шкідливої активності можуть бути шкідливі IP адреси, доменні імена, URL-адреси, контрольні суми пакетів, послідовності байтів в мережевому трафіку, нетипові значення в полях заголовків пакетів. Для систем запобігання вторгненням на базі хоста цими ознаками виступають сигнатури та хеш-функції шкідливих файлів та процесів, а також ключі реєстру.

Сигнатурний метод допомагає виявити атаки з відомою сигнатурою, а також атаки, з використанням відомого автоматизованого програмного забезпечення для проведення атак, оскільки таке програмне забезпечення під час кожної атаки генерує одні й ті самі сигнатури трафіка.

Перевагами виявлення на основі сигнатур є висока швидкість обробки, мала кількість помилкових спрацьовувань, а також можливість виявлення шкідливих подій без попереднього навчання системи. До недоліків сигнатурного методу належать неможливість виявлення невідомих атака та вразливостей нульового дня, а також необхідність постійного оновлення сигнатурних баз.

Виявлення на основі аномалій здійснюється завдяки спостереженню за поведінкою мережі або вузла та відстеженню аномальних подій у їх поведінці.

Для того щоб відстежити аномалії системі попередження вторгнень необхідно спочатку визначити базовий рівень об'єкту, що захищається. Під базовим рівнем розуміють нормальну поведінку мережі та вузлів, що перебувають у цій мережі. Система IPS запам'ятовує характеристики об'єкта, що захищається, і надалі порівнює ці дані з поточним станом цього об'єкта. Будь-які відхилення від базового рівня розглядаються системою запобігання вторгнень як аномалії.

Прикладами аномалій, що розглядаються системою вторгнень на базі хоста можуть бути:

- велика кількість невдалих спроб аутентифікації;
- несанкціонована зміна файлових конфігурацій та налаштувань вузла;
- нестандартна активність на портах вузла;
- незвичайне збільшення кількості звернень до одного файлу вузла.

Для мережевої системи протидії вторгнень прикладами аномалій можуть бути:

- нетипове збільшення обсягу трафіку, що передається в мережі;
- несанкціоноване додавання до мережі нових пристроїв.

Перевагами методики виявлення на основі аномалій є можливість виявлення невідомих загроз та атак нульового дня, а також можливість швидкої обробки даних та виявлення вторгнень у мережах з великим обсягом трафіку. До недоліків виявлення на основі аномалій належать велика кількість помилкових спрацьовувань, а також необхідність в додатковому часі після встановлення системи для виявлення базового рівня.

Сучасні реалізації систем запобігання вторгнень з технологією виявлення на основі аномалій використовують штучний інтелект як на етапі формування базового рівня, так і на етапі виявлення аномалій поточного стану. В першому випадку штучний інтелект допомагає збільшити швидкість навчання системи та швидше визначити базовий рівень об'єкта захисту. У другому випадку використання штучного інтелекту дає змогу зменшити кількість помилкових спрацьовувань. Це допомагає значною мірою нівелювати недоліки методики виявлення на основі аномалій.

Виявлення на основі аналізу аномального стану протоколів відбувається шляхом порівняння поточної активності мережевого трафіку з його базовими показниками безпечної активності. Базові показники визначаються виробниками IPS системи і є універсальними для кожного об'єкту захисту. Ці показники задають параметри протоколів, які використовуються в мережі, що захищається. Відхилення поточного рівня від показників базової активності ідентифікуються

системою запобігання вторгнень як аномалії. Основою базових показників є стандарти та специфікації протоколів визначених міжнародними організаціями зі стандартизації.

Перевагами даного методу є можливість відстеження стану протоколів на різних рівнях та короткий період навчання системи. Недоліками даного методу є неможливість виявлення атак які не виходить за рамки діапазону показників базової активності, а також неможливість аналізу протоколів які відхиляються від стандартів.

2.2.1.3 Додаткові критерії аналізу IPS систем

До додаткових критеріїв аналізу IPS систем належать:

- вартість;
- можливості протидії;
- наявність централізованої системи керування;
- можливості взаємодії;
- потенційні розміри об'єкта захисту.

Відповідність аналізованих програмних продуктів додатковим критеріям аналізу представлено в таблиці 3 додатку Е та таблиці 4 додатку Е.

Вартість - це один із важливих критеріїв аналізу систем запобігання вторгнень, оскільки зараз на ринку представлені системи у великому ціновому діапазоні. Існує велика кількість безкоштовних IPS систем з відкритим вихідним кодом, а також багато потужних систем з високою вартістю, призначених для великих підприємств з масштабною інформаційною системою. Аналіз допомагає зменшити варіативність, обрати найбільш прийнятний за ціною варіант та визначитись з бюджетом на захист інформаційних ресурсів.

Під можливостями протидії IPS системи розуміють здатність системи реагувати на вторгнення без попередньої участі людини. В залежності від реалізації системи запобігання вторгнення мають можливість:

- блокувати TCP з'єднання та порти для UDP з'єднання;
- відкидати шкідливі пакети;

- блокувати кінцеві вузли;
- блокувати облікові записи користувачів;
- змінювати конфігурацію обладнання інформаційної системи;
- змінювати політики мережевого екрану.

Наявність централізованої системи керування дає змогу управляти великою кількістю даних з різних вузлів та різних точок мережі. Централізована система керування допомагає виявити повну картину подій в інформаційній системі, що захищається, а також значно збільшує швидкість реакції на загрозу, акумулюючи данні з різних джерел в одному місті. Також це дозволяє значно зменшити кількість людей, необхідних для управління системою запобігання вторгнень. Пріоритетною також є наявність графічного інтерфейсу для управління IPS, оскільки це значно полегшує взаємодію з цією системою.

Можливість взаємодії системи запобігання вторгнень з іншими системи дає змогу розширити функціонал IPS системи додатковими програмними засобами, а також оперувати в своїй роботі даними з інших програмних засобів. Також можливість взаємодії дозволяє інтегрувати IPS систему як один з компонентів іншої системи запобігання вторгнення. Це допомагає збільшити її функціональні можливості посилити прозорість безпеки інформаційної системи.

Під потенційні розміри об'єкта що захищається розуміють максимально можливі розміри інформаційної системи яку технічно зможе захищати IPS. Також до цього критерію відносять пропорційність інформаційної системи та системи IPS, що необхідна для її захисту. Наприклад, для невеликої компанії з низьким або середнім об'ємом трафіку підходить безкоштовна система запобігання вторгнень з відкритим вихідним кодом, а для великого підприємства з потужною інформаційною системою, такої IPS буде замало. І навпаки продукт IPS з високою вартістю для великого підприємства, що комбінує в собі набір програмних та апаратних рішень буде надмірним для компаній с малим об'ємом трафіку.

2.2.2 Програмні компоненти SIEM та IPS систем представлені на ринку

2.2.2.1 Snort

Snort – це система запобігання вторгнення, яка представляє собою програмний продукт з відкритим вихідним кодом. За принципом реалізації Snort є мережевою IPS з підтримкою сигнатурного методу виявлення та виявлення на основі аномального стану протоколів. Відповідно до офіційної документації програмний продукт складається з наступного переліка компонентів:

- сніфер пакетів;
- декодер пакетів;
- препроцесори;
- механізм виявлення;
- модуль виводу [6].

Схематичне представлення архітектури Snort надано на рисунку 2.3

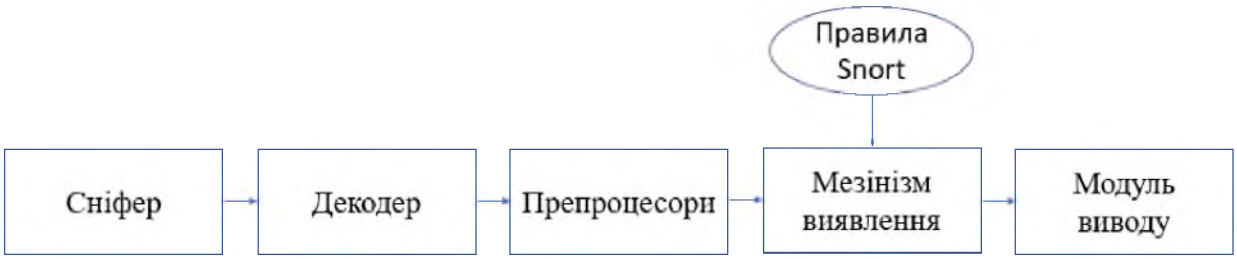

Рисунок 2.3 – Схематичне представлення архітектури Snort

Сніфер пакетів виконує захоплення пакетів і передає їх на декодер. В режимі запобігання цей модуль працює в розрив мережі, тобто пропускає через себе весь трафік, що проходить в мережу. Захоплені пакети потрапляють в декодер, де відбувається аналіз заголовків пакетів, що відповідають першим трьом рівням моделі OSI, а також пошук аномалій та відхилень у цих заголовках. Основною задачею декодера є деінкапсуляція даних з кадрів канального рівня та пакетів мережевого рівня. Об'єктом фокусу декодеру є стек протоколів TCP/IP.

Наступні модулі під назвою препроцесори займаються аналізом протоколів, що відповідають мережевому, транспортному та прикладному рівню моделі OSI. Основна задача препроцесорів полягає в підготовці даних мережевого та транспортного рівня до наступного зіставлення з правилами Snort. Також на рівні

препроцесорів відбувається контроль стану протоколів, об'єднання даних із декількох пакетів сеансу, а також нормалізація протоколів. У кінцевого користувача Snort є можливість додати власні розроблені препроцесори для аналізу специфічних промислових протоколів.

Підготовленні данні мережевого і транспортного рівня надходять до механізму виявлення. На цьому етапі відбувається порівняння наданих даних з переліком правил IPS. Правила складаються із заголовка та параметра. В заголовку задається дія, яку необхідно виконати системі у разі збігання правила та даних, що перевіряються. В заголовку також указується IP адрес джерела та призначення, тип пакету та номера портів збігання з якими сигналізує про виявлення. В параметрі задаються додаткові критерії виконання правил та описи сигнатур атак. У разі збігу правила та даних, що перевіряються система виконує дію, що заздалегідь записана у правилі. Відповідно до документації існує наступний перелік можливих реакцій IPS системи Snort:

- drop – заблокувати та записати пакет;
- sdrop – заблокувати проте не записувати;
- reject – заблокувати пакет, записати його та відправити скидання TCP з'єднання або повідомлення про недоступність порту для UDP з'єднання.

Правила Snort можуть застосовуватися як до одного пакету, так і до їх сукупності. Також правила можуть визначати порогові значення та часові інтервали для аналізу мережевих подій. Кінцевий користувач має можливість написання своїх правил. Модуль виводу надає результати виявлення в різноманітних форматах.

Оскільки Snort є однопотоковою системою з можливістю глибокого аналізу пакетів, це значно обмежує швидкість їх обробки. А отже ця IPS система краще підійде для захисту інформаційних систем малого та середнього розміру з невеликим об'ємами трафіку.

В Snort відсутня централізована система управління, а також графічний інтерфейс. Взаємодія с системою відбувається за допомогою консолі. Проте модуль виводу має можливість надавати результати своєї роботи у зовнішні системи

аналізу та генерації звітів. На сьогоднішній день існує велика кількість таких систем. Найпопулярнішими з них є Snorby, Sguil та Anaval. Вони дозволяють представити результати роботи Snort в графічному вигляді, а також надають більш детальній аналіз даних його виводу.

2.2.2.2 Suricata

Suricata – це безкоштовна система запобігання вторгнення, яка створення для виявлення і протидії загрозам, що відбуваються на рівні мережі. Для виявлення загроз вона використовує сигнатурний метод та виявлення на основі аномального стану протоколів. За архітектурою Suricata складається з наступного переліка компонентів:

- сніфер пакетів;
- декодер пакетів;
- механізм виявлення;
- модуль виводу[7].

Схематичне представлення архітектури Suricata надано на рисунку 2.4.

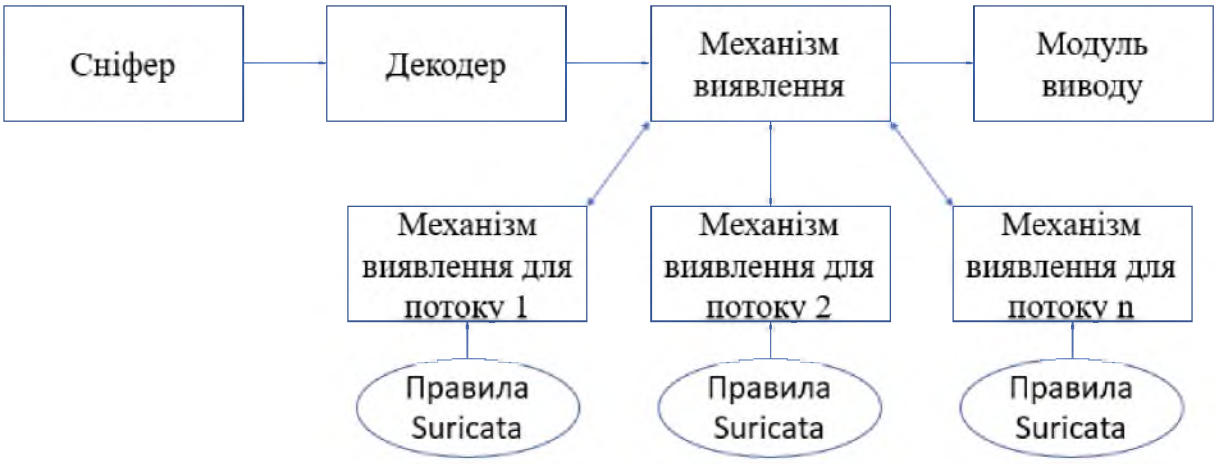

Рисунок 2.4 – Схематичне представлення архітектури Suricata

Сніфер пакетів необхідний для захоплення пакетів, що потрапляють в мережу. Після захоплення пакети передаються в декодер, основною задачею якого є деінкапсуляція заголовків та даних кожного рівня стеку протоколів, що використовувався для передачі цього пакету. Заголовок та данні кожного рівня поділяються на окремі потоки і надходять до механізму виявлення, де відбувається паралельний аналіз кожного з потоків. Аналіз полягає в зіставленні заголовку та

даних кожного потоку із заздалегідь визначеним переліком правил. На цьому ж етапі відбувається перевірка заголовків кожного рівня на наявність аномалій, задля контролю стану протоколів. У разі виявлення аномалій заголовків або збігання даних потоку та правил, Suricata може заблокувати та записати пакет, заблокувати його без запису або відправити запит на скидання з'єднання та заблокувати порт. Результати виявлення передаються до модуля виводу де вони групуються у звіти загальноприйнятих форматів.

Незважаючи на схожість компонентів архітектури Suricata на компоненти Snort, вона має суттєві від Snort відмінності. Основна відмінність полягає в здатності Suricata використовувати багатопотоковий режим роботи. Це дає можливість для описаного вище паралельного аналізу пакетів з використанням декількох ядер багатоядерних процесорів. Також Suricata має можливість використовувати графічний процесор для збільшення обчислюваної потужності. Наявність таких змін значно прискорює швидкість обробки пакетів, що дає змогу використовувати Suricata для захисту інформаційних систем середнього на великого розміру, з великими об'ємами трафіку.

Як і в системі Snort в Suricata відсутня централізована система керування та графічний інтерфейс. Проте як і в випадку Snort, вона є системою з відкритим вихідним кодом, а також має загальноприйняті функції виведення даних та прийому запитів від інших систем. Це дає змогу для її взаємодії з іншими системами безпеки та дозволяє інтегрувати Suricata як компонент загальної системи безпеки. Наразі на ринку представлено багато програмних продуктів, що дозволяють надати в графічному вигляді та зробити більш детальний аналіз результатів роботи Suricata. Такими продуктами є наприклад Sguil та Evebox. Опис програмного забезпечення Sguil надано у розділі 2.2.2.6. Опис програмного продукту Evebox надано у розділі 2.2.2.7. Також зараз існують системи протидії вторгнень які одним із компонентів захисту використовують програмний продукт Suricata. Прикладами таких систем є Security Onion та SELKS. Детальний опис системи Security Onion надано у розділі 2.2.2.6. Детальний опис системи SELKS надано у розділі 2.2.2.7.

2.2.2.3 Wazuh

Wazuh - це система запобігання вторгнень на базі хоста з відкритим вихідним кодом. Вона використовується для захисту кінцевих вузлів, серверів, віртуальних машин та екземплярів хмарного сховища.

Відповідно до офіційної документації Wazuh складається з агенту безпеки та сервера управління[8]. Агент безпеки розміщується безпосередньо на об'єкті захисту і відповідає за моніторинг безпеки цього об'єкту. Агент безпеки дозволяє здійснювати збір даних з журналів подій операційної системи та додатків, відстежувати цілісність файлової системи, а також виконувати системну інвентаризацію. Під системною інвентаризацією розуміють облік параметрів операційної системи таких як її версія, перелік запущених процесів, встановлених додатків, мережевих інтерфейсів та відкритих портів [8]. Також агент безпеки здатний реалізовувати виявлення шкідливого програмного забезпечення, відстежувати конфігурацію безпеки, а також запускати активну відповідь у разі виявлення загроз. Прикладами активної відповіді агенту можуть бути видалення виявлених шкідливих файлів, блокування мережевого з`єднання, а також зупинка запущених процесів. Усі результати роботи агенту безпеки передаються по захищеному каналу серверу управління, для подальшого аналізу цих даних.

Сервер управління виконує аналіз інформації, що передається від агентів безпеки. Потрапляючи до серверу управління дані в першу чергу потрапляють в декодер. Декодер визначає яка інформація потрапила на аналіз та вилучає відповідні елементи необхідні для аналізу цієї інформації. Наступним кроком вилученні дані порівнюються зі заздалегідь визначеним переліком правил. Як і у випадку Snort, правила описують індикатори компрометації, а також дії що необхідно виконати у разі виявлення збігу між правилом та даними, що аналізуються. У разі збігу, результати аналізу та дії, що необхідно виконати, передаються агенту безпеки, який і запускає активну відповідь на загрозу. Також сервер управління виконує функції реєстрації та налаштування агентів безпеки, а також функції управління ними.

В залежності від розмірів інформаційної системи, сервер управління може бути встановлений як на одному вузлі з агентом безпеки так і на окремій робочій станції. Задля збільшення ефективності роботи у великих інформаційних система Wazuh має можливість масштабування шляхом кластеризації, тобто об'єднання декількох серверів керування в єдину систему. Це допомагає зменшити навантаження на кожен окремий сервер та збільшити швидкість обробки інформації, що передається агентами.

Графічне представлення результатів роботи Wazuh, а також їх поглиблений аналіз можливий завдяки інтегрованому комплексу програмних продуктів Elastic Stack. Детальний опис програмних продуктів Elastic Stack представлений у розділі 2.2.2.6.

2.2.2.4 OSSEC

OSSEC – це система запобігання вторгнень на базі хоста, що має відкритий вихідний код. За переліком компонентів вона складається з агентів та центрального менеджеру[9].

Агент безпеки це розміщене на кінцевих вузлах, що захищаються, програмне забезпечення. Воно займається збором та надсиланням інформації з кінцевих вузлів до центрального серверу. Агент збирає та передає наступний перелік інформації:

- журнали подій операційної системи;
- журнали подій додатків встановлених на вузлі.

Також агент має можливість здійснювати контроль цілісності файлів та реєстрів операційної системи, а також здійснювати виявлення руткітів.

Центральний менеджер це програма, що зазвичай встановлюється на окремому вузлі системи, призначена для обробки інформації, що надходить від агентів.

До функцій центрального менеджера належать:

- зберігання та аналіз журналів, що надходять від агентів на кінцевих вузлах;
- видача попереджень, що до виявлених загроз;

- збирання та аналіз подій системних журналів комутаторів, маршрутизаторів та мережевих екранів.

Проміжок часу зберігання журналів задається у налаштуваннях менеджеру, адміністратором системи. Після потрапляння до менеджеру журнали аналізуються на наявність індикаторів загроз за допомогою заздалегідь визначеного переліка правил. Центральний менеджер допомагає оптимізувати управління декількома агентами, що дає змогу зручно контролювати стан безпеки усіх кінцевих вузлів проміжних пристроїв, що знаходяться в інформаційній системі.

Менеджер та агент можна встановити як на одній робочій станції так і на різних. Також OSSEC має можливість роботи в гібридному режимі, що дозволяє використовувати додатковий сервер, як транзитний між агентом та основним сервером. Все це дає можливість налаштувати найбільш прийнятну для інформаційної системи конфігурацію OSSEC.

OSSEC має графічний інтерфейс для представлення результатів, який може бути встановлених додатково. Однак для зручності використання, а також для більш детального аналізу, OSSEC може передавати результати роботи до інших програмних продуктів.

2.2.2.5 Fail2Ban

Fail2ban – це система запобігання вторгнень на базі хоста, яка є програмним продуктом з відкритим вихідним кодом. Основною задачею цієї системи є протидія атакам, які використовують перебір паролів для входу в систему. Fail2ban аналізує файли журналів з метою виявлення в них підозрілої активності, у вигляді великої кількості спроб входу в систему з одного адресу. У разі виявлення аномальної активності Fail2ban блокує шкідливий IP адрес на деякий час. Блокування відбувається шляхом взаємодії IPS системи з мережевим екраном. Fail2ban створює нове правило мережевого екрану в якому вказується IP адресу, що необхідно заблокувати. Після закінчення часу блокування це правило мережевого екрану деактивується. Стандартний час блокування складає 10 хвилин. Підозрілою

вважається активність у вигляді 5 невдалих спроб входу за період в 10 хвилин[10]. Проте в налаштуваннях системи є можливість зміни цих параметрів.

Fail2ban має можливість захисту багатьох служб, таких як SSH, Gmail, Apache та багато інших. Для кожної служби створюється окреме правило, яке в Fail2ban називається Jail. Ці правила складаються з фільтру, в якому вказується тип служби, та дії, яку необхідно виконати у разі виявлення.

У Fail2ban відсутня централізована система управління, а також графічний інтерфейс для виведення результатів роботи. Взаємодія з IPS системою відбувається на кожному вузлі окремо, за допомогою консолі. Також основним недоліком Fail2ban є неможливість блокування атак з розподіленим перебором паролів, а також розподілених атак відмови в обслуговуванні. Це зв'язано з тим, що Fail2ban виявляє тільки підозрілі спроби входу, що повторюються з одного IP адресу. А отже ця система запобігання вторгнення може використовуватись лише як рішення для окремих вузлів та серверів у інформаційних системах малих та середніх розмірів.

2.2.2.6 Security Onion

Security Onion – це безкоштовна платформа, яка об'єднує в собі функціональність SIEM та IPS систем. Вона реалізована у якості дистрибутиву Linux і включає в себе програмні компоненти мережевих систем запобігання вторгнень та систем запобігання вторгнень на базі хоста.

Мережеві системи виявлення та запобігання вторгнень представлені в Security Onion у вигляді програмних продуктів:

- Snort;
- Suricata;
- Zeek.

Детальний опис IPS системи Snort представлений у розділі 2.2.2.1. Повний опис системи запобігання вторгнень Suricata надано у розділі 2.2.2.2.

Zeek – це мережева система виявлення вторгнень, яка має деякі функції SIEM систем. Вона представляє собою програмний продукт з відкритим вихідним кодом.

Основним завданням Zeek є моніторинг мережі та детальний облік усіх подій, які в ній відбуваються. Це здійснюється шляхом захоплення та аналізу пакетів, що циркулюють в мережі. Однак на відміну від Snort та Suricata, Zeek не здійснює побайтову перевірку кожного пакету та порівняння його з набором сигнатур. Натомість Zeek переробляє потік пакетів у низку подій з подальшою можливістю аналізу цих подій. Події генеруються для протоколів всіх рівнів стеку. Прикладами подій можуть бути встановлення та закриття TCP з'єднання, запити DNS та HTTP. Аналіз подій відбувається завдяки переліку заздалегідь визначених сценаріїв. Сценарії описують перелік необхідних дій у разі виявлення певних видів активності. Хоча Zeek має можливості задати реакцію на виявлення, ця система, на відміну від Suricata та Snort, безпосередньо не призначена для протидії атакам, а служить скоріше для їх виявлення. Проте наявність подібного механізму дає можливість виконувати виявлення як на основі сигнатур, так і аномалій, що разом з іншими компонентами Security Onion дає великі можливості захисту мережі.

Системи виявлення та запобігання вторгнень на базі хоста представлені в Security Onion наступним переліком компонентів:

- Wazuh;
- OSSEC
- Osquery.

Детальний опис системи запобігання вторгнень Wazuh представлений у розділі 2.2.2.3. Повний опис IPS системи OSSEC надано у розділ 2.2.2.4.

Osquery – це безкоштовний програмний продукт, що використовується для аналізу безпеки, конфігурації та ефективності кінцевих вузлів інформаційної системи. Аналіз відбувається шляхом представлення компонентів операційної системи у вигляді реляційної бази даних. Osquery складається з двох компонентів osqueryi та osqueryd. Osqueryi – це інтерактивне середовище, що представляє собою консоль вводу SQL запитів. Вона необхідна для точкового разового аналізу певних компонентів операційної системи. Osqueryd – це програма-демон, що працює в фоновому режимі. Вона призначена для автоматичного виконання заздалегідь визначених SQL запитів. Запити виконуються раз в певний період часу та

визначаються для кожного компонента системи, який підлягає аналізу. Для зручного упорядкування розкладу перевірок системи osqueryd дозволяє групувати запити в пакети. Результати виконання запитів записуються в журнали Osquery, з подальшою можливістю їх аналізу, як за допомогою osqueryi, так і в зовнішніх програмних продуктах.

Окрім систем запобігання вторгнень, Security Onion також вміщує в собі програмні продукти які допомагають аналізувати дані роботи IPS систем, структурувати їх, а також представити їх в графічному вигляді. З цією метою Security Onion використовує:

- Elastic Stack,
- Sguil,
- Squert.

Elastic Stack – це набір програмних інструментів з відкритим вихідним кодом, призначений для графічного представлення, а також поглибленого аналізу результатів роботи та журналів IPS систем. Цей набір складається з наступного переліку компонентів:

- Elasticsearch;
- Filebeat;
- Kibana;
- Beats;
- Logstash[13].

Elasticsearch – це програмний продукт, що представляє собою розподілену пошукову систему. Він має можливості шукати та аналізувати усі типи даних в режимі реального часу. В Security Onion цей компонент використовується для зручного зберігання та пошуку журналів IPS систем, а також журналів подій безпеки. Потрапляючи до Elasticsearch данні автоматично індексуються, що дає змогу подальшого швидкого їх пошуку. Можливості об’єднання декількох екземплярів Elasticsearch в кластер, дозволяє масштабувати цей продукт для ефективної роботи з великою кількістю даних.

Beats – це інструмент, що в Security Onion застосовується для захоплення журналів роботи IPS систем, для подальшого відправлення їх до Elasticsearch за допомогою Filebeat або Logstash.

Filebeat використовується для швидкої передачі невеликих за розміром журналів через мережу. Альтернативою Filebeat є Logstash. На відміну від Filebeat, цей інструмент здатний працювати з даними великих розмірів, однак і споживання ресурсів є в нього набагато більшим. В залежності від розміру журналів роботи IPS систем Logstash та Filebeat використовуються в Security Onion для відправлення журналів захоплених за допомогою Beats до Elasticsearch.

Kibana це програмний інтерфейс, що використовується для графічного представлення та аналізу даних Elasticsearch.

Альтернативою набору інструментів Elastic Stack у Security Onion є Sguil та Squert.

Sguil це інструмент моніторингу та аналітики безпеки. В Security Onion Sguil взаємодіє з такими IPS системами, як Suricata, Snort, OSSEC та надає графічний інтерфейс для представлення та аналізу результатів їх роботи. Прикладами результатів роботи є перелік виявлень та дій прийнятих для їх запобігання, данні сеансу підчас якого відбулось виявлення, а також захоплені пакети.

Squert використовується як веб-додаток. Він дозволяє робити запити по базі даних Sguil та продивлятись записи які в них зберігаються. Також він дає можливість аналізувати виявлення IPS систем з використанням додаткових контекстів, шляхом використання метаданих цих виявлень.

Оскільки Security Onion є дистрибутивом на базі Linux, він має можливість встановлення додаткового програмного забезпечення, для розширення можливостей своєї функціональності. Прикладом таких програм є Stenographer та Wireshark. Stenographer дозволяє захоплювати пакети з метою їх подальшого накоплення. Це може бути корисним в відкладеному виявленні вторгнень, а також при проведенні цифрової криміналістики. Stenographer виконує повне управління захопленими пакетами включаючи їх видалення у міру заповнення дискового простору. Wireshark це програмний інструмент для проведення аналізу мережевих

протоколів. З його допомогою можливо здійснювати контроль сеансів зв'язку кінцевих вузлів інформаційної системи. Також в Security Onion є можливість додавання систем машинного навчання для виявлення аномалій в інформаційній системі, що захищається.

2.2.2.7 SELKS

SELKS – це оснований на Debian безкоштовна платформа, що представляє повний набір функцій системи запобігання вторгнень та SIEM систем. Вона складається з наступного переліка компонентів:

- Suricata;
- Elasticsearch;
- Logstash;
- Kibana;
- Stamus Scirius Community Edition;
- Arkime;
- Evebox.

Центральним компонентом SELKS є IPS система Suricata. Детальний опис Suricata надається у розділі 2.2.2.2. В платформі SELKS Suricata використовується для виявлення та запобігання мережевих загроз.

Elasticsearch, Logstash та Kibana є компонентами набору інструментів Elastic Stack, детальний опис якого надано у розділі 2.2.2.6. Основною функцією цих компонентів у SELKS є зберігання результатів роботи Suricata та швидкий пошук певних виявлень в її журналах.

Stamus Scirius Community Edition представляє собою веб інтерфейс, який застосовується для адміністрування правил IPS системи Suricata. Він допомагає зручно налаштувати правила Suricata відповідно до потреб захисту інформаційної системи. Також цей компонент дає можливість візуалізації переліка загроз виявлених Suricata.

Arkime це програмний інструмент, що в SELKS використовується для захоплення та індексування пакетів, з подальшою можливістю представлення їх у

вигляді потоків. Arkime складається з механізму захоплення пакетів, веб-інтерфейсу та сховища зберігання метаданих потоків. Механізм захоплення здатний вилучати метадані потоків пакетів, а також інформацію о протоколах їх передачі та відправляє цю інформацію до сховища. Веб-інтерфейс застосовується для забезпечення доступу до оброблених даних механізму захоплення. Сховище використовується для зберігання результатів роботи механізму захоплення.

Evebox це веб-додаток, що використовується для відображення та управління даними виявлень Suricata.

SELKS є зручним набором інструментів для моніторингу мережевої безпеки, а також протидії мережевим вторгненням у інформаційну систему. Використання високоефективної системи Suricata дозволяє застосовувати цей набір для захисту інформаційних систем середнього та великого розміру.

2.2.2.8 Qradar

Qradar – це програмний продукт, що представляє собою систему управління інформаційною безпекою та подіями безпеки. Також він включає в себе функції систем запобігання вторгнень. Qradar розглядає інформаційну систему у вигляді подій, що в ній відбуваються, та потоків даних, що ній циркулюють.

Архітектура Qradar складається з трьох рівнів:

- збір даних;
- обробка даних;
- дослідження даних[12].

На першому рівні колектори Qradar збирають данні о подіях, що відбуваються в інформаційній системі та данні о потоках інформації, що в ній циркулюють. Події, дані яких аналізуються в Qradar задаються заздалегідь адміністратором системи. Прикладами подій в інформаційній системі є блокування пакетів мережевим екраном, вхід користувачів інформаційної системи, VPN підключення [12]. Під даними потоків інформації розуміють параметри мережевої активності кінцевих вузлів інформаційної системи, а також параметри сеансів між двома вузлами. До даних потоків належать використовуванні порти та IP-адреса

кінцевих вузлів, кількість пакетів та байтів, що було передано. Збір даних потоків відбувається шляхом захоплення пакетів. Перед відправленням на другий рівень зібрані данні аналізуються та нормалізуються для подальшої зручної обробки.

На другому рівні відбувається обробка захоплених даних. Цей рівень складається з таких програмних компонентів як:

- механізм виявлення загроз;
- Qradar Risk Manager;
- Qradar Vulnerability Manager;
- Qradar Incident Forensics.

Механізм виявлення загроз обробляє дані, передані з першого рівня та зіставляє їх з переліком заздалегідь визначених правил. У разі збігу Qradar генерує попередження та запускає автоматичну дію вказану в правилі.

Qradar Risk Manager використовується для представлення карти топології мережі інформаційної системи, шляхом збору даних про конфігурацію мережевої інфраструктури. Це дозволяє імітувати різноманітні мережеві сценарії, задля можливості управління ризикам.

Qradar Vulnerability Manager дозволяє збирати та аналізувати данні про вразливості інформаційної системи з подальшою можливістю виявлення різноманітних загроз безпеки.

Qradar Incident Forensics має можливість відтворення повноцінних мережевих з'єднань. Цей інструмент є дуже корисним при проведенні криміналістичних досліджень.

Результати роботи програмних компонентів другого рівня зберігаються для подальшої можливості представлення їх компонентами третього рівня.

На третьому рівні архітектури Qradar відбувається представлення результатів роботи перших двох рівнів. Компоненти цього рівня надають можливості адміністраторам системи для проведення пошуку результатів виявлень та протидій та засоби їх представлення, а також складання звітів по цим даним. Дані аналізу Qradar збираються, обробляються та зберігаються централізовано на окремій робочій станції.

2.2.3 Вибір програмних компонентів, що найбільше відповідають вимогам інформаційних системи ВНЗ

Відповідно до пункту 2.1 для захисту інформаційних систем ВНЗ найбільш прийнятним рішенням є комбінація програмних продуктів SIEM та IPS систем. Проаналізувавши представлені на ринку варіанти можемо прийти до висновку, що найбільш прийнятним варіантом серед SIEM систем є програмна платформа Security Onion. У порівнянні з Qradar, Security Onion є кращім варіантом оскільки оскілки ця платформа є безкоштовною для встановлення, а також не потребує оплату за подальший супровід продукту від виробника. Цей критерій є важливим оскільки такі бюджетні установи, як вищі навчальні заклади, обмежені в фінансуванні та не мають можливості виділення великих коштів для придбання систем захисту. У порівнянні з комплексним рішенням SELKS, Security Onion також є кращим варіантом. На відміну від SELKS, основними компонентами якого є програмні продукти для захисту від мережевих вторгнень, до складу компонентів Security Onion входять також програмні продукти систем запобігання вторгнень на базі хоста. Збільшена функціональність дає змогу захистити більше аспектів безпеки інформаційних систем ВНЗ.

Серед часткових програмних рішень систем запобігання вторгнень також можна виділити найкращі варіанти. У якості мережевої IPS системи найліпшим варіантом є Suricata. У порівнянні зі Snort, Suricata є кращим варіантом, оскільки цей продукт краще адаптований к роботі в багатоядерних системах. Наявність багатопотокового режиму роботи, дозволяє підтримувати велику швидкість аналізу пакетів, що є важливим в інформаційних системах ВНЗ великих розмірів. Серед систем запобігання вторгнень на базі хоста, найкращім варіантом є Wazuh. Превагою Wazuh перед його конкурентом OSSEC є більші можливості масштабування за рахунок кластерів, а також можливості інтеграції з Elastic Stack. Наявність цих переваг дає можливість Wazuh краще адаптуватися під великі розміри інформаційних систем ВНЗ, а також більш детальний аналіз його результатів виявлень. Також серед часткових програмних продуктів, слід визначити Fail2ban. Він є потужним інструментом, що в інформаційній системі

ВНЗ, може використовуватись для обмеження спроб авторизації за допомогою протоколу SSH.

2.3 Інтеграція обраних програмних рішень в інформаційні системи ВНЗ

Задля представлення можливостей інтеграції обраних програмних рішень в інформаці системи вищих навчальних закладів, було обрано інформаційну систему Національного технічного університету «Дніпровська політехніка». У розділі 2.3.1 представлено загальні характеристики цієї інформаційної системи, перелік її сервісів, а також загрози кожного сервісу, що відповідають переліку загроз наданому у розділі 1.3.

2.3.1 Загальні характеристики інформаційної системи Національного технічного університету «Дніпровська політехніка»

Інформаційна система університету складається з кластеру віртуалізації, на якому розташовується більшість сервісів інформаційної систем, та фізичної локальної мережі.

Фізична мережа складається з комунікаційного обладнання та внутрішніх робочих станцій підключених до цієї мережі. До комунікаційного обладнання належать маршрутизатори, комутатори та точки бездротового доступу, що розташовані по всій території університету. Магістральні комутатори знаходяться в контрольованих приміщеннях кожного корпусу та об’єднані між собою оптоволоконними кабелями. Комутатори нижчі за ієрархією розташовуються рівномірно по території відповідного корпусу. Внутрішні робочі станції підключаються до цих комутаторів. Ці станції розташовані в навчальних аудиторіях та кабінетах працівників університету. Фізична мережа університету надає доступ до інтернету для користувачів за допомогою робочих станцій або бездротового підключення з власних девайсів.

Кластер віртуалізації розташований на серверному обладнані, що знаходиться в контрольованому приміщені університету. Цей кластер оснований на системі віртуалізації Proxmox версії 6.4. Загальні характеристики кластеру представлені в таблиці 2.2.

Таблиця 2.2 – Характеристики кластеру інформаційної системи

Назва характеристики	Кількісне значення
Кількість процесорів	236
Обсяг оперативної пам’яті	2 Терабайт
Обсяг дискового масиву	120 Терабайт
Кількість встановлених віртуальних машин	59 основних та 28 тестових

На кластері розгорнута віртуальна мережа, що складається з шести вузлів. Назва та детальні характеристики вузлів кластеру надано в таблиці 2.3. На кожному з вузлів встановлені віртуальні машини, що необхідні для надання користувачам інформаційної системи певних сервісів. Загальну кількість віртуальних машин встановлених в кластері надано в таблиці 2.2.

Відповідно до класифікації сервісів, наданій у розділі 1.2.1, інформаційні системи ВНЗ можуть надавати наступний перелік сервісів:

- система управління навчанням;
- сервіс доступу до веб-ресурсів вищого навчального закладу та його підрозділів;
- сервіс надання інтернету мешканцям гуртожитків ВНЗ;
- сервіс репозиторію;
- сервіс надання бездротового доступу до інтернету на території ВНЗ;
- сервіс електронного каталогу та інші сервіси бібліотеки;
- автоматизована система бухгалтерського обліку;
- автоматизована система управління навчальним процесом;
- автоматизована система відділу кадрів.

Інформаційна системи Національного технічного університету «Дніпровська політехніка» надає усі сервіси з цього переліку. У розділі 1.3.1.1 наведено опис цих сервісів, технології що вони використовують, а також місце їх розташування.

Таблиця 2.3 – Характеристика вузлів кластеру інформаційної системи

Назва вузлу	Кількість процесорів	Обсяг оперативної пам’яті , гігабайт	Обсяг дискового масиву, терабайт
Node 0	64	192	42
Node 1	40	128	12
Node 2	32	128	12
Node 3	32	128	24
Node 4	4	32	8
Node 5	64	512	25

На вузлі кластеру під назвою Node 0 була розгорнута система Security Onion в режимі моніторингу подій мережі. За рік використання цією системою було зроблено приблизно чотири мільярди виявлень. Детальні характеристики віртуальної машини зі встановленим Security Onion надано в таблиці 2.4.

Таблиця 2.4 – Характеристики віртуальної машини зі встановленим Security Onion

Назва характеристики	Кількісне значення
Кількість процесорів	8
Обсяг оперативної пам’яті	64 Гігабайт
Обсяг дискового масиву	1 Терабайт

2.3.1.1 Перелік сервісів інформаційної системи Національного технічного університету «Дніпровська політехніка»

Система управління навчанням надає послугу доступу до навчальних ресурсів для студентів університету. В своїй роботі використовує систему управління курсами Moodle версії 3.11 , а також систему управління базами даних MySQL. Система управління навчанням розташований на віртуальній машині, що знаходиться на вузлі під назвою Node 1.

Сервіс доступу до веб-ресурсів надає послуги доступу до веб-сайту університету, а також до веб-сайтів підрозділів університету. У своїй роботі використовує Apache HTTP Server версії 2.4.52 для забезпечення роботи серверної

частини, та Бітрікс 24 для забезпечення клієнтської частини веб-сервісу. Цей сервіс розташований на віртуальних машинах, що знаходиться на вузлі кластеру під назвою Node 0.

Сервіс надання інтернету мешканцям гуртожитків університету функціонує завдяки білінговій системі ABills версії 0.90. Хоча сервіс є публічним, доступ до інформації про оплати за інтернет надається лише для авторизованих користувачів. Сервіси надання інтернету мешканцям гуртожитків розташовані віртуальних машинах двох вузлів кластеру під назвою Node 1 та Node 2.

Сервіс репозиторію використовується для надання послуг зберігання да публічного представлення кваліфікаційних робіт студентів, а також наукових робіт співробітників університету. Сервіс дозволяє продивлятися ці данні без необхідності попередньої авторизації. Для своєї роботи цей сервіс використовує платформу для створення та управління електронними архівами DSpace версії 6. Сервіс репозиторію розташованих на віртуальних машинах вузла Node 0.

Сервіс надання бездротового доступу до інтернету на території університету поширюється по всій території університету та надає безкоштовний, відкритий доступ до інтернету для всіх його відвідувачів. Задля забезпечення цього сервісу в кожному корпусі університету встановлений магістральний комутатори, що з'єднані між собою оптоволоконним кабелем. До цих комутаторів підключаються комутатори, що нижчі за ієрархією та розташовуються рівномірно по всій території відповідного корпусу. Точки доступу підключаються до цих локальних комутаторів. Для підключення пристроїв до бездротової мережі використовується сервіс DHCP.

Сервіс електронного каталогу та інші сервіси бібліотеки університету використовується для надання каталогу архіву документів, представлених у бібліотеці університету та загального представлення інформації о цих документах. У своїй роботі цей сервіс використовує систему управління змістом сайтів WordPress версії 5.8.3. Сервіс електронного каталогу та інші сервіси бібліотеки розташовані на віртуальних машинах вузла Node 0.

Автоматизована система бухгалтерського обліку забезпечує управління бухгалтерською звітністю університету. Сервіс розташований на віртуальних машинах вузла Node 3. Хоча ця система фізично розташований у спільному з іншими сервісами кластеру, логічно вона виділена в окрему віртуальну мережу.

Автоматизована система управління навчальним процесом представлений в інформаційній системі системою «Деканат». Сервіс складається з клієнтської частини встановленій на робочих станціях користувачів та серверної частини що встановлена на віртуальних машинах вузла кластеру Node 3. В своїй роботі цей сервіс використовує систему управління базами даних MySQL.

Автоматизована система відділу кадрів використовується для обліку працівників та студентів університету.

2.3.1.2 Перелік загроз для сервісів інформаційної системи Національного технічного університету «Дніпровська політехніка»

Відповідно до моделі загроз розробленій у розділі 1.3 найбільшу загрозу для інформаційних систем вищих навчальних закладів становлять несанкціоноване вторгнення в інформаційну систему з використанням вразливостей мережевої архітектури. Під вразливостями архітектури розуміють вразливості, що з'явились в результаті розробки інформаційної системи, а також вразливості технологій, що використовуються для її реалізації. Оскільки актуальними джерелами загроз для інформаційної системи ВНЗ є студенти та ентузіасти у сфері проникнення в інформаційні системи то найбільшу небезпеку вони становлять для публічних сервісів інформаційної системи таких як:

- система управління навчанням;
- сервіс доступу до веб-ресурсів вищого навчального закладу та його підрозділів;
- сервіс надання інтернету мешканцям гуртожитків університету;
- сервіс репозиторію;
- сервіс надання бездротового доступу до інтернету на території університету;

- сервіс електронного каталогу та інші сервіси бібліотеки.

Через схожість технологій, що використовуються в система управління навчанням, сервіс доступу до веб-ресурсів , сервіси бібліотеки, сервісу репозиторію та сервісу надання інтернету мешканцям гуртожитків, найбільшу загрозу для них становлять:

- сканування портів;
- атака перебору паролів для авторизації через службу SHH;
- SQL-ін'єкція;
- Розподілена атака відмови в обслуговуванні.

Для сервісу надання бездротового доступу до інтернету на території вищого навчального закладу найбільшу загрозу становлять:

- атака типу людина посередині;
- атака з фальшивим DHCP сервером
- атака відмови в обслуговувані.

2.3.2 Реалізація обраних програмних компонентів для запобігання загроз сервісів інформаційної системи Національного технічного університету «Дніпровська політехніка»

На базі мережі науково-технічної бібліотеки, що входить до загальної мережі університету, була встановлена SIEM система Security Onion.

До складу мережі входять такі сервіси інформаційної системи як:

- сервіс репозиторію документів створених співробітниками та студентами;

  сервіс електронного каталогу та інші сервіси бібліотеки

Загальний перелік інформаційних сервісів та структуру мережі науково-технічної бібліотеки надано на рисунку 2.5

В мережі бібліотеки система Security Onion встановлена у якості системи моніторингу та не використовується для запобігання атак на цю мережу.

За рік після встановлення системою було зроблено приблизно чотири мільйони сповіщень, що до подій мережі. Через таку велику кількість сповіщень, оперативна реакція адміністратора системи у разі виявлення атаки не є можливою.

У цьому випадку доцільно використовувати систему запобігання вторгнення за для того, щоб система могла давати автоматичну відповідь на виявлені загрози.

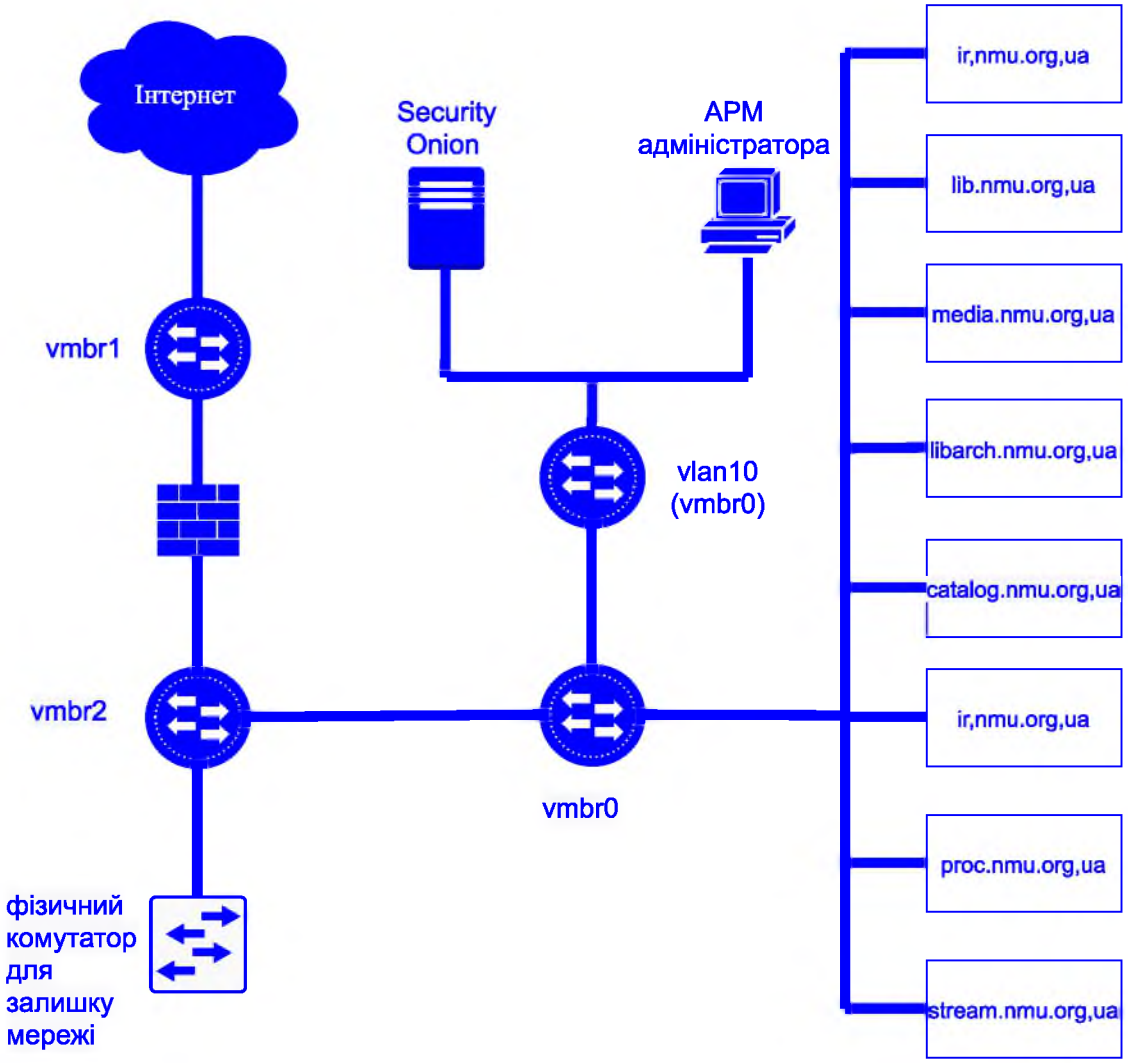

Рисунок 2.5 – Структура мережі науково-технічної бібліотеки університету

Основною проблемою IPS систем велика відповідальність разі у разі хибнопозитивних спрацьовувань. А отже налаштування системи запобігання вторгнень слід лише для актуальних загроз інформаційної системи. У розділ 2.3.1.2 було визначено наступний перелік загроз для сервісів бібліотеки:

- SQL-ін’єкції;
- мережева розвідка;
- атака перебору паролів для авторизації через службу SHH.

За для запобігання цих загроз доцільно використовувати як мережеві IPS системи, так і IPS системи на базі хоста.

В описаній системі Security Onion у якості мережевої системи виявлення вторгнень використовується програмний продукт Suricata. Як було описано у розділі 2.2.2.2 Suricata також має можливість працювати у якості системи запобігання вторгнень. А отже необхідно змінити налаштування цієї системи задля того, щоб вона почала самостійно блокувати визначений перелік загроз.

За для можливості роботи в режимі запобігання вторгнень Suricata повинна бути встановлена в розрив мережі, тобто весь трафік має проходити безпосередньо через систему. В цьому режимі Suricata має два варіанти конфігурації. У першому варіанті Suricata аналізує трафік, що проходить через комп'ютер на якому вона встановлена. У другому випадку система аналізує трафік, що генерується комп'ютером на якому вона встановлена.

Оскільки Suricata використовується для захисту мережі бібліотеки необхідним є перший варіант конфігурації. Структурне зображення обраного варіанту конфігурації зображено на рисунку 2.5.

Рисунок 2.6 – Структурне зображення конфігурації Suricata

Для налаштування конфігурації при якій Suricata аналізує трафік, що проходить через комп'ютер на мережевому рівні необхідно виконати наступну команду:

```
sudo iptables -I FORWARD -j NFQUEUE
```

Для в Suricata параметру аналізу тільки TCP трафіка необхідно виконати наступну команду:

```
sudo iptables -I INPUT -p tcp  -j NFQUEUE
sudo iptables -I OUTPUT -p tcp -j NFQUEUE
```

Також Suricata має можливість аналізу конкретних портів. Наприклад наступна команда вказує Suricata на необхідність сканування лише порту веб-сервісу:

```
sudo iptables -I INPUT -p tcp --sport 80  -j NFQUEUE
sudo iptables -I OUTPUT -p tcp --dport 80 -j NFQUEUE
```

Для налаштування IPS режиму в Suricata на канальному рівні необхідно задати наступну конфігурацію:

```
af-packet:
  - interface: eth0
    threads: 1
    defrag: no
    cluster-type: cluster_flow
    cluster-id: 98
    copy-mode: ips
    copy-iface: eth1
    buffer-size: 64535
    use-mmap: yes
  - interface: eth1
    threads: 1
    cluster-id: 97
    defrag: no
    cluster-type: cluster_flow
    copy-mode: ips
    copy-iface: eth0
    buffer-size: 64535
    use-mmap: yes
```

Ця конфігурація вказує інтерфейси між якими Suricata виконує аналіз трафіку с наступною можливістю його блокування.

2.4 Висновок

У другій частині кваліфікаційної роботи були вирішені такі задачі:

- виконано обґрунтування вибору рішень, що до захисту інформаційної системи;
- виконано опис критеріїв класифікації систем запобігання вторгнень;
- проаналізовано перелік програмних продуктів систем запобігання вторгнень представлених на ринку
- наведено приклад реалізацій запобігання вторгнень в інформаційній системі вищого навчального закладу.

РОЗДІЛ 3. ЕКОНОМІНИЙ РОЗДІЛ

Метою виконання економічного розділу дипломного проекту є техніко-економічне обґрунтування доцільності запропонованих в проекті рішень по впровадженню системи запобігання вторгнень в інформаційну систему Національного технічного університету «Дніпровська політехніка».

Основною задачею техніко-економічного обґрунтування є визначення економічної ефективності використання основних та супутніх результатів, що мають бути отримані при виконанні дипломного проекту.

Виконання цієї задачі складається з наступних етапів:

- розрахунок капітальних витрат на придбання та впровадження системи запобігання вторгнень;
- розрахунок річних експлуатаційних витрат на утримання та обслуговування системи запобігання вторгнень;
- оцінка можливого збитку від атаки на сегмент інформаційної системи;
- визначення та аналіз показників економічної ефективності впровадження системи запобігання вторгнень.

Розрахунок капітальних витрат наведено у розділі 3.1. Розрахунок експлуатаційних витрат представлено у розділі 3.2. У розділі 3.3 наведена оцінка можливого збитку від атаки на сегмент інформаційної системи. Визначення та аналіз показників економічної ефективності надано у розділі 3.4.

3.1 Розрахунок капітальних витрат на придбання та впровадження система запобігання вторгнень

Капітальні витрати – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації. До капітальних витрат на впровадження системи запобігання вторгнення належать:

- витрати на придбання програмного продукту Security Onion;
- витрати на придбання програмного продукту Fail2ban;
- витрати на встановлення та тестування програмних компонентів системи запобігання вторгнень.

Витрати на встановлення та тестування програмних компонентів системи запобігання вторгнень розраховуються за формулою:

$$Квп = Ззп + Змч$$

де Квп – витрати на встановлення та тестування програмних компонентів системи запобігання вторгнень;

Ззп – заробітна плата виконавця;

Змч – вартість машинного часу впровадження.

Заробітна плата виконавця розраховується за формулою:

$$Ззп = Зіб \times t$$

де Зіб – середньогодинна заробітна плата адміністратора інформаційної системи;

t – загальна тривалість робіт.

Середньогодинна заробітна плата адміністратора інформаційної системи з нарахуваннями складає 15000 гривень. Отже при 40-годиному робочому тижні середньогодинна заробітна плата становить 85.22 гривень/годину.

Перелік часу витраченого на встановлення та тестування програмних продуктів надано в таблиці 3.1.

Таблиця 3.1 Перелік часу на встановлення та тестування програмних продуктів

Позначення	Пояснення	Витрачений час (годин)
t1	Тривалість встановлення програмних компонентів	2
t2	Тривалість налаштування програмних компонентів	3
t3	Тривалість тестування програмних компонентів	3

Отже загальна тривалість виконання робіт складає:

$$t = 2 + 3 + 2 = 8 \text{ годин}$$

Тоді заробітна плата виконавця складає:

$$Ззп = 85.22 \times 8 = 681.76 \text{ гривень}$$

Встановлення та тестування програмних компонентів відбувається на серверному обладнанні інформаційної системи, яке знаходиться постійно в робочому стані, задля забезпечення функціонування цієї системи. А отже додатково вартість машинного часу враховуватись не буде. Змч = 0 гривень.

Тоді витрати на встановлення та тестування програмних компонентів системи запобігання вторгнень становлять:

$$Крп = 681.76 + 0 = 681.76 \text{ гривень}$$

Перелік капітальних витрат із зазначенням вартості цих витрат наведено в таблиці 3.2.

Таблиця 3.2 -Перелік капітальних витрат

№	Назва витрати	Опис	Ціна, гривень	Примітка
1	Придбання програмного продукту Security Onion	Security Onion призначених для виявлення та протидії вторгненням в інформаційну систему	0	Security Onion є безкоштовним програмним продуктом
2	Придбання програмного продукту Fail2Ban	Fail2ban призначених для виявлення та протидії вторгненням в інформаційну систему	0	Fail2ban є безкоштовним програмним продуктом
3	Встановлення та налаштування	Встановлення придбаних програмних продуктів в	681.76	

	програмних компонентів	інформаційну систему університету		

Загальна сума капітальних витрат на впровадження системи протидії вторгнень становить:

$$К = 0 + 0 + 681.76 = 681.76 \text{ гривень}$$

3.2 Розрахунок річних експлуатаційних витрат на утримання і обслуговування системи протидії вторгнень

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені в грошовій формі.

Розрахування експлуатаційних витрат відбувається за формулою:

$$С = Св + Ск + Сак$$

де С – загальні експлуатаційні витрати;

Св – витрати на відновлення та модернізацію системи;

Ск – витрати на керування системою;

Сак ¬– витрати викликані активністю користувачів.

Витрати на оновлення та на модернізацію системи складають 0 гривень, оскільки програмні продукти встановлені в ній є безкоштовними.

$$Св = 0 \text{ гривень}$$

Витрати на керування системою розраховуються за формулою:

$$Ск = Сн + Са + Сз + Сєв + Сел + Со + Стос$$

де Сн – витрати на навчання адміністративного персоналу та кінцевих користувачів;

Са – річний фонд амортизаційних відрахувань;

Сз – річний фонд заробітної плати інженерно-технічного персоналу;

Сєв – витрати на єдиний річний внесок;

Сел – вартість електроенергії, що споживається апаратурою системи інформаційної безпеки;

Со – витрати на залучення сторонніх організацій ;

Стос – витрати на технічне й організаційне адміністрування.

Витрати на навчання адміністративного персоналу складають 0 гривень, оскільки наявної кваліфікації, достатньо для управління системою.

$$Сн = 0 \text{ гривень}$$

Оскільки встановлене в системі програмне забезпечення є безкоштовним вартість фонду амортизації складає 0 гривень.

$$Са = 0 \text{ гривень}$$

Річний фонд заробітної плати інженерно-технічного персоналу розраховується за формулою:

$$Сз = Зосн + Здод$$

де Зосн – основна заробітна плата;

Здод – додаткова заробітна плата.

Основна заробітна плата технічного персоналу складає 180000 на рік.

Додаткова заробітна плата визначається у розмірі 8 % від основної заробітної плати та становить 14400 гривень на рік.

Отже річний фонд заробітної плати становить:

$$Сз = 180000 + 14400 = 194400 \text{ гривень}$$

Єдиний річний внесок у 2022 році складає 22% від річного фонду заробітної плати.

$$Сєв = 194400 * 22\% = 42768 \text{ гривень}$$

Оскільки програмні продукти встановлюється на серверне обладнання системи, яке знаходиться постійно в робочому стані, задля забезпечення функціонування інформаційної системи, то додаткові витрати на електроенергію не враховуються.

$$Сел = 0 \text{ гривень}$$

Оскільки у уряді університету є кваліфіковані працівники, витрати на залучення сторонніх організацій складають 0 гривень.

$$Со = 0 \text{ гривень}$$

Витрати на технічне та організаційне адміністрування складають 2% від суми капітальних витрат.

$$Стос = 681.76 * 2\% = 13.63 \text{ гривень}$$

Отже загальні витрати на керування системою складають:

$$Ск = 0 + 0 + 194400 + 42768 + 0 + 0 + 13.63 = 237181.63 \text{ гривень.}$$

Витрати викликані активністю користувачів розраховуються як 46% від суми капітальних витрат

$$Сак = 46\% * 681.76 = 313.6$$

Отже загальні експлуатаційні витрати становлять:

$$С = 0 + 237181.63 + 313.6 = 238132$$

3.3 Оцінка від можливого збитку від атаки на сегмент інформаційної системи

У якості сегмента атакованої системи Оцінка можливого збитку від атаки на сегмент інформаційної системи, оцінюється як упущена вигода від простою атакованого сегменту та розраховується за формулою:

$$U = Пп + Пв + V$$

де Пп – оплачувані витрати робочого часу на простої співробітників атакованого вузла або сегмента корпоративної мережі;

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі.

Витрати на зниження продуктивності співробітників сегменту інформаційної системи розраховуються за формулою:

$$Пп = \frac{\sum Зс}{F} \times tп$$

де Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі;

F – місячний фонд робочого часу;

tп – час простою сегмента інформаційної системи внаслідок атаки.

Заробітна плата одного співробітника атакованого вузла складає 7000 гривень на місяць. Кількість співробітників сегменту інформаційної системи 10 чоловік.

$$Зс = 7000 \times 10 = 70000 \text{ гривень}$$

Місячний фонд робочого часу за умови 40 годинного робочого тижня складає 176 годин.

Час простою сегменту інформаційної системи складає 24 години.

$$Пп = \frac{70000}{176} \times 24 = 9545 \text{ гривень}$$

Вартість відновлення працездатності сегменту розраховується за формулою

$$Пв = Пви + Ппв + Пзч$$

де Пви – витрати на повторне введення інформації;

Ппв- витрати на відновлення сегменту інформаційної системи;

Пзч – витрати на заміну устаткування апаратного забезпечення сегменту.

Витрати на повторне введення інформації розраховуються за формулою:

$$Пви = \frac{\sum Зс}{F} \times tви$$

де Зс – заробітна плата співробітників атакованого сегменту;

F – місячний фонд робочого часу;

tви – час повторного введення інформації.

Час повторного введення інформації складає 120 годин.

$$Пви = \frac{70000}{176} \times 120 = 47727 \text{ гривень}$$

Витрати на відновлення сегменту інформаційної системи розраховуються за формулою:

$$Ппв = \frac{\sum Зо}{F} \times tв$$

де Зо – заробітна плата обслуговуючого персоналу;

F – місячний фонд заробітної плати;

tв – час відновлення після атаки.

Заробітна плата обслуговуючого персоналу складає 15000 гривень.

Час відновлення складає 24 години.

$$\text{Ппв} = \frac{15000}{176} \times 24 = 2045 \text{ гривень}$$

Реалізація атаки не передбачає ушкодження апаратного забезпечення сегменту інформаційної системи. А отже витрати на заміну устаткування складають 0 гривень.

$$\text{Пв} = 47727 + 2045 + 0 = 49772 \text{ гривень}$$

Діяльність аналізованого сегменту не є комерційної, а отже витрати від зниження обсягу продажів складає 0 гривень.

$$\text{U} = 9\,545 + 49772 + 0 = 59317 \text{ гривень}$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі обчислюється на формулою:

$$\text{B} = \sum_i \sum_n U$$

де $\sum_i$ – сума атак на рік;

$\sum_n$ – сума атакованих вузліз.

$$\text{B} = 7 \times 1 \times 59317 = 415219 \text{ гривень}$$

Загальний ефект від впровадження системи інформаційної безпеки обчислюється за формулою:

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

де R -очікувана імовірність атаки.

$$E = 415219 \times 0.6 - 238132 = 10999 \text{ гривень}$$

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Визначення економічної ефективності реалізації системи запобігання вторгнень, здійснюється шляхом підрахування коефіцієнта ROSI. Цей коефіцієнт показує яка кількість коштів повертається з однієї гривні капітальних інвестицій на впровадження системи.

Коефіцієнт ROSI обчислюється за формулою:

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

$$\text{ROSI} = \frac{10999}{681} = 16{,}15$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти розрахункове значення ROSI з бажаним значенням показника ефективності Ен.

Показник ефективності Ен обчислюється за формулою:

$$\text{Ен} = \frac{N\text{деп} - N\text{інф}}{100}$$

де Nдеп – річна депозитна ставка;

Nінф – річний рівень інфляції.

Річна депозитна ставка для бюджетних установ складає 5.3%.

Річний рівень інфляції складає 2%.

$$\text{Ен} = \frac{\text{Nдеп} - \text{Nінф}}{100} = \frac{5.3\% - 2\%}{100} = 0.051$$

Оскільки коефіцієнт ROSI більший показника ефективності Ен то проект системи інформаційної безпеки є доцільним.

Термін окупності капітальних інвестицій визначається за формулою:

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

$$T = \frac{681}{10999} = 0.06 \text{ роки}$$

Висновок

При аналізі показників ефективності було визначено, що проект впровадження системи запобігання в інформаційну систему вищого навчального закладу є економічно доцільним.

Вартість капітальних витрат на реалізацію проекту складає 681 гривню.

Вартість річних експлуатаційних витрат на утримання і обслуговування системи складає 238132 гривні.

Загальний ефект від впровадження системи складає 10999 гривень.

Термін окупності капітальних інвестицій 0.06 роки.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було вирішено ряд задач. Проведено аналіз загальної структури інформаційних систем вищих навчальних закладів. На основі проведених даних було складено модель загроз інформаційних систем вищих навчальних закладів. Найбільшу загрозу для інформаційної системи складає несанкціоноване вторгнення в інформаційну систему з використанням вразливостей мережевої архітектури та вразливостей програмного забезпечення.

Но основі отриманих актуальних загроз було виконано обґрунтування вибору рішення, що до захисту інформаційних систем вищих навчальних закладів. Згідно з рішенням, щодо захисту інформаційних систем, було описано критерії класифікації систем запобігання вторгнень. Було проведено аналіз переліку систем запобігання вторгнень представлених на ринку.

З цього переліку було обрано програмні компоненти, що найбільше відповідають інформаційним системам вищих навчальних закладів.

Перелік обраних сервісів становить:

- Security Onion;
- Suricata;
- Wazuh;
- Fail2ban

Також було наведено приклад реалізації програмних компонентів в інформаційній системі вищого навчального закладу.

В економічному розділі було економічно обґрунтовано доцільність використання систем запобігання вторгнень в інформаційних системах вищих навчальних закладів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / Упоряд.: О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв, О.В. Кручінін. – Дніпро: НГУ, 2018. – 50 с.

2. Закон України «Про вищу освіту» // Відомості Верховної Ради. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1556-18#Text.

3. Наказ №446 «Про затвердження Положення про дистанційне навчання» [Електронний ресурс] // Міністерство освіти і науки України. – 2013. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0703-13#Text.

4. НД ТЗІ 1.1-003:Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf.

5. Вихорев С. В. Классификация угроз информационной безопасности / Сергей Викторович Вихорев. – 2001. –Режим доступу до ресурсу:https://elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf

6. Snort User Manual [Електронний ресурс] // -. – 2020. – Режим доступу до ресурсу: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

7. Suricata User Guide [Електронний ресурс] // -. – 2019. – Режим доступу до ресурсу: https://suricata.readthedocs.io/en/suricata-6.0.4/.

8. Wazuh documentation [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://documentation.wazuh.com/current/getting-started/index.html.

9. OSSEC Manual [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.ossec.net/docs/docs/manual/index.html.

10. Fail2ban Manual [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.fail2ban.org/wiki/index.php/MANUAL_0_8#Introduction.

11. Security Onion Documentation [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://docs.securityonion.net/en/2.3/.

12. IBM QRadar SIEM 7.4.3 documentation [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.ibm.com/docs/en/qsip/7.4?topic=SS42VS_7.4/com.ibm.qradar.doc/c_qradar_pdfs.htm

13. Elastic Stack and Product Documentation [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.elastic.co/guide/index.html.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат		
2	А4	Список умовних скорочень		
3	А4	Зміст		
4	А4	Вступ		
5	А4	1 Розділ		
6	А4	2 Розділ		
7	А4	3 Розділ		
8	А4	Висновки		
9	А4	Список літератури		
10	А4	Додаток А		
11	А4	Додаток Б		
12	А4	Додаток В		
13	А4	Додаток Г		
14	А4	Додаток Д		
15	А4	Додаток Е		
16	А4	Додаток Ж		
17	А4	Додаток И		

ДОДАТОК Б. Перелік документів на оптичному носії

01 Пояснювальна записка Високос М.А.docx

02 Пояснювальна записка Високос М.А.pdf

03 Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125м-20-1

Високос Максима Андрійовича

на тему «Аналіз реалізацій систем запобігання вторгнень в інформаційних системах вищих навчальних закладів»

Пояснювальна записка складається з вступу, трьох розділів і висновків викладених на сторінках.

Метою кваліфікаційної роботи є забезпечення безпеки сервісів інформаційної системи вищих навчальних закладів.

Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проаналізована структура та розроблена модель загроз інформаційних систем вищих навчальних закладів.

Запропоновані реалізації програмних продуктів систем запобігання вторгнень, за для усунення цих загроз.

Практичне значення роботи полягає в підвищені рівню захисту інформаційних систем вищих навчальних закладів за рахунок впровадження описаних в кваліфікаційній роботі засобів.

За час дипломування Високос М.А. проявив себе фахівцем, здатним в цілому вирішувати поставлені задачі, та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Кваліфікаційна робота заслуговує оцінки «_____»

Керівник доц. кафедри БІТ _____ Флоров С.В.

(підпис) (прізвище, ініціали)

ДОДАТОК Д

Додаток Д. Таблиця 1 – Критерій ступеню доступності до захищеного об’єкта

Оцінка	Антропогенний	Техногенний	Стихійний
1	Джерело загроз не має доступу до технічних і програмних засобів	Об'єкт захисту розташовується на значній відстані від джерела техногенної загрози, що повністю виключає можливість будь-якого впливу на об'єкт, що захищається, в тому числі і від вторинних проявів	Об'єкт захисту знаходиться поза межами зони дії природних катаклізмів
2	Джерело загроз має низьку доступність до технічних і програмних засобів	Об'єкт захисту розташовується на відстані від джерела техногенної загрози, що виключає можливість її прямого впливу на об’єкт захисту	Об'єкт захисту знаходиться поза межами зони дії природних катаклізмів, проте на об'єкті є передумови виникнення стихійних джерел загроз

Продовження таблиці 1

Оцінка	Антропогенний	Техногенний	Стихійний
3	Джерело загроз має обмежену можливість доступу до програмних засобів в силу введених обмежень у використанні технічних засобів, функціональних обов'язків або за родом своєї діяльності	Об'єкт захисту розташовується на відстані від джерела техногенної загрози, на якій прояв впливу цієї загрози може вчинити не істотний вплив на об'єкт захисту	Об'єкт захисту розташований в зоні в якій по проведеним спостереженням протягом довгого періоду відсутні прояви природних катаклізмів, але є передумови виникнення стихійних джерел загроз на самому об'єкті
4	Джерело загроз має доступ до технічних і програмних засобів, але не визначений його функціональними обов'язками	Об'єкт захисту розташований в безпосередній близькості від джерела техногенної загрози і будь-який прояв цієї загрози може вчинити	Об'єкт захисту розташований в зоні, в якій багаторічні спостереження показують можливість прояву

		істотний вплив на об'єкт захисту	природних катаклізмів

Продовження таблиці 1

5	Джерело загроз має повний доступ до технічних і програмних засобів обробки інформації	Об'єкт захисту сам містить джерело техногенної загрози і їх територіальний поділ неможливий	Об'єкт захисту розташований в зоні дії природних катаклізмів

Додаток Д. Таблиця 2 – коефіцієнт ступені кваліфікації джерела загроз, привабливість здійснення діянь або наявність необхідних умов

Оцінка	Антропогенний	Техногенний	Стихійний
1	Відсутність можливості будь-якого використання програм	Інформаційні ресурси, що захищаються, містять інформацію, яка не представляє інтерес для джерела загрози	Відсутні передумови для реалізації передбачуваної події
2	Можливість запуску завдань / програм з фіксованого набору, призначеного для обробки інформації, що захищається	Інформаційні ресурси, що захищаються містять інформацію, яка при її накопиченні і узагальненні протягом певного періоду може завдати шкоди	На об’єкті є передумови, що перешкоджають реалізації загрози

		організації, що здійснює захист	

Продовження таблиці 2

Оцінка	Антропогенний	Техногенний	Стихійний
3	Можливість створення і запуску користувачем власних програм з новими функціями по обробці інформації	Інформаційні ресурси, що захищаються, містять інформацію, розголошення якої може завдати шкоди окремим особам	Умови сприятливі для реалізації загрози, проте можливість її реалізації дуже мала
4	Можливість управління функціонуванням мережи, тобто впливом на базове програмне забезпечення, її склад і конфігурацію	Інформаційні ресурси, що захищаються, містять інформацію, яка може бути використана для отримання вигоди на користь джерела загрози або третіх осіб	Умови дають можливість прояву джерела загрози
5	Визначається всім обсягом можливостей суб'єктів, які здійснюють проектування і ремонт технічних засобів, аж до включення до складу мережі власних технічних засобів з	Інформаційні ресурси, що захищаються, містять інформацію, яка може завдати непоправної шкоди і привести до краху організації, що здійснює захист	Умови сприятливі або можуть бути сприятливі для реалізації загрози

	новими функціями з обробки інформації		

Додаток Д. Таблиця 3 – Коефіцієнти ступенів фатальності наслідків реалізації загрози

Оцінка	Опис
1	Результати прояви загрози не можуть вплинути на діяльність об'єкта захисту
2	Результати прояву загрози можуть призвести до часткового руйнування об'єкта захисту, які не потребують великих витрат на його відновлення і, практично не впливають на обмеження часу доступу до інформаційних ресурсів, що захищаються
3	Результати прояви загрози можуть призвести до часткового руйнування об'єкта захисту і, як наслідок, до значних витрат на відновлення, обмеження часу доступу до ресурсів, що захищаються
4	Результати прояву загрози можуть призвести до руйнування об'єкта і до значних витрат на відновлення наслідків, порівнянних з витратами на створення нового об'єкту і суттєвого обмеження часу доступу до ресурсів, що захищаються
5	Результати прояву загрози можуть призвести до повної руйнації об'єкта захисту, як наслідок до непоправних втрат і виключення можливості доступу до інформаційних ресурсів, що захищаються

ДОДАДОК Е

Додаток Е. Таблиця 1 - Класифікація програмних продуктів за принципом реалізації

Назва IPS системи	Мережева IPS	IPS на базі хоста	IPS для бездротових мереж	Аналізатор поведінки мережі
Snort	+	–	–	–
Suricata	+	–	–	–
Wazuh	–	+	–	–
OSSEC	–	+	–	–
Security Onion	+	+	–	+
SELKS	+	–	–	–
Fail2ban	–	+	–	–
Qradar	+	+	–	+

Додаток Е. Таблиця 2 – Класифікація програмних продуктів за методикою виявлення

Назва IPS системи	Виявлення на основі сигнатур	Виявлення на основі аномалій	Виявлення на основі аналізу стану протоколів
Snort	+	–	+
Suricata	+	–	+
Wazuh	+	–	–
OSSEC	+	–	–
Security Onion	+	+	+
SELKS	+	–	+

Fail2ban	–	+	–
Qradar	+	+	+

Додаток Е. Таблиця 3 – Аналіз програмних продуктів за додатковими критеріями

Назва IPS системи	Вартість	Можливості протидії	Наявність централізованої системи керування
Snort	Безкоштовна	Має можливість блокування пакетів з записом або без, а також можливість розриву мережевого з'єднання	Немає
Suricata	Безкоштовна	Має можливість блокування пакетів з записом або без, а також можливість розриву мережевого з'єднання	Немає
Wazuh	Безкоштовна	Має можливість видалення шкідливих файлів, блокувати мережеве з'єднання, а також	Наявна

		зупинка запущених процесів	
OSSEC	Безкоштовна	Має можливість блокування шкідливих запущених процесів, та мережевих з'єднань	Наявна

Продовження таблиці 3

Назва IPS системи	Вартість	Можливості протидії	Наявність централізованої системи керування
Security Onion	Безкоштовна	Компоненти мережевих IPS дозволяють блокувати шкідливі пакети та з'єднання. Компоненти IPS на базі хоста дозволяють зупиняти та блокувати шкідливі запущені процеси	Наявна
SELKS	Безкоштовна	Має можливість блокування пакетів з записом або без, а також можливість	Наявна

		розриву мережевого з’єднання	
Fail2ban	Безкоштовна	Має можливість блокування шкідливих IP адресів на певний період часу	Немає
Qradar	800 доларів на місяць або 9230 доларів назавжди	Має можливість блокування шкідливих з’єднань, запущених процесів, а також облікових записів користувачів інформаційної системи	Наявна

Додаток Е. Таблиця 4- Аналіз програмних продуктів за додатковими критеріями

Назва IPS системи	Можливість взаємодії з іншими системами захисту	Потенційні розміри об’єкта, що захищається
Snort	Має можливість передавати результати своєї роботи для аналізу іншим програмним забезпеченням, а також може бути інтегрована як компонент іншої ISP системи	Інформаційні системи малих та середніх розмірів
Suricata	Має можливість передавати результати своєї роботи для аналізу іншим програмним забезпеченням, а	Інформаційні системи середніх та великих розмірів

	також може бути інтегрована як компонент іншої ISP системи	
Wazuh	Має можливість передавати результати своєї роботи для аналізу іншим програмним забезпеченням, а також може бути інтегрована як компонент іншої ISP системи	Інформаційні системи середніх та великих розмірів
OSSEC	Має можливість передавати результати своєї роботи для аналізу іншим програмним забезпеченням, а також може бути інтегрована як компонент іншої ISP системи	Інформаційні системи середніх та великих розмірів
Security Onion	Платформа яка об'єднує в собі декілька IPS систем, а також надає засоби для управління ними	Інформаційні системи середніх та великих розмірів
SELKS	Платформа яка об'єднує в собі декілька IPS систем, а також надає засоби для управління ними	Інформаційні системи середніх та великих розмірів

Продовження таблиці 4

Назва IPS системи	Можливість взаємодії з іншими системами захисту	Потенційні розміри об'єкта, що захищається
Fail2ban	Має можливість взаємодії з мережевим екраном для подальшого блокування шкідливих IP-адресів.	Інформаційні системи малих та середніх розмірів

Qradar	Закритий продукт, що має можливості взаємодії с обмеженою кількістю програмного забезпечення заздалегідь дозволеного розробниками системи	Інформаційні системи великих розмірів