Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Кійко Ростислава Євгеновича*

академічної групи 125-17-1

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Підсистема виявлення аномального стану інформаційної системи бібліотеки НТУ "Дніпровська Політехніка"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Галушко О.М.			
розділів:				
спеціальний	ст. викл. Святошенко В.О.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер				

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Кійко Р.Є.* **академічної групи** **125-17-1**

(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Підсистема виявлення аномального стану інформаційної системи бібліотеки НТУ "Дніпровська Політехніка"*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-С

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Нормативно-правова база до сфери захисту інформації, актуальність захисту від кібератак, задачі на розробку та впровадження системи	22.04.21
Розділ 2	Обстеження ОІД відповідно до захисту мережі, аналіз та вибір системи виявлення аномального стану, встановлення, налаштування, випробування системи на об'єкті.	13.05.21
Розділ 3	Розрахунки витрат, втрати від нереалізації розрахунки що до доцільності впровадження системи виявлення аномального стану.	9.06.21

Завдання видано _____ Святошенко В.О

(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Кійко Р.Є.

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., __ табл., __ додатка, __ джерел.

Об'єкт розробки: інформаційна система науково-технічної бібліотеки НТУ "Дніпровська Політехніка".

Мета роботи: підвищення захищеності інформаційної системи бібліотеки НТУ "Дніпровська Політехніка" через контроль її стану.

В першому розділі було описано актуальність проблеми кібератак на інформаційні ресурси в країні та світі, було наведено три крупні кібератаки за останні роки, було зроблено перелік нормативно-правової бази, було поставлено задачі для роботи в спеціальній частині.

В спеціальній частині проведено обстеження об’єкту, проаналізовано всі технічні засоби, розроблено модель порушника, розглянуто всі реалі, потенційні загрози, обрано систему виявлення аномального стану, проведено встановлення системи, проведено випробування на об'єкті з реальними загрозами.

В третьому розділі було доведено доцільність впровадження підсистеми виявлення аномального стану. Розраховано капітальні, експлуатаційні витрати, величина збитку та показник економічної ефективності.

Практичне значення роботи полягає в моніторингу аномальних дій в інформаційній мережі, своєчасному усуненню реальних та потенційних загроз мережі.

ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕР БЕЗПЕКА, ІНФОРМАЦІЙНІ МЕРЕЖІ, АНОМАЛЬНИЙ СТАН.

РЕФЕРАТ

Пояснительная записка: __ стр., __ рис., __ табл., __ приложений, __ источников.

Объект разработки: информационная система научно-технической библиотеки НТУ "Днепровская Политехника".

Цель работы: реализация подсистемы обнаружения аномального состояния в информационной системе библиотеки НТУ "Днепровская Политехника".

В первом разделе была описана актуальность проблемы кибератак на информационные ресурсы в стране и мире, были приведены три крупные кибератаки за последние годы, был сделан перечень нормативно-правовой базы, были поставлены задачи для работы в специальной части.

В специальной части было проведено обследование объекта, проанализированы все технические средства, разработана модель нарушителя, рассмотрены все реальные, потенциальные угрозы, выбрана система обнаружения аномального состояния, проведена установка системы, проведены испытания на объекте с реальными угрозами.

В третьем разделе было доказано целесообразность внедрения подсистемы обнаружения аномального состояния. Рассчитано капитальные, эксплуатационные расходы, величина ущерба и показатель экономической эффективности.

Практическое значение работы состоит в мониторинге аномальных действий в информационной сети, своевременном устранению реальных и потенциальных угроз сети.

ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, КИБЕРБЕЗОПАСНОСТЬ, ИНФОРМАЦИОННЫЕ СЕТИ, АНОМАЛЬНОЕ СОСТОЯНИЕ.

ABSTRACT

Explanatory note: __ p., __ pic., __ tab., __ additions, __ sources.

Object of development: information system of the scientific and technical library of " Dnipro University of Technology ".

Purpose of work: implementation of the abnormal state detection subsystem in the information system of the " Dnipro University of Technology " library.

The first section described the relevance of the problem of cyberattacks on information resources in the country and the world, cited three major cyberattacks in recent years, made a list of the regulatory framework, and set tasks for work in a special part.

In a special part, an inspection of the facility was carried out, all technical means were analyzed, a model of the intruder was developed, all real, potential threats were considered, an anomalous state detection system was selected, the system was installed, tests were carried out at the facility with real threats.

In the third section, the expediency of introducing an abnormal state detection subsystem was proved. The capital, operating costs, the amount of damage and the indicator of economic efficiency have been calculated.

The practical significance of the work consists in monitoring anomalous actions in the information network, in the timely elimination of real and potential threats to the network.

OBJECT OF INFORMATION ACTIVITY, INTEGRATED INFORMATION PROTECTION SYSTEM, CYBER SECURITY, INFORMATION NETWORKS, ABNORMAL STATE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

DDoS - distributed denial of service

HIDS - host-based intrusion detection system

IDS - intrusion detection systems

IPS - intrusion prevention systems

NIDS - network-based intrusion detection system

OVS - open vswitch

SOS - security onion solution

АРМ – автоматизоване робоче місце

ДСТУ - державні стандарти України

ІзОД – інформація з обмеженим доступом;

НД ТЗІ – нормативний документ технічного захисту інформації

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності

ПКМУ – постанова кабінету міністрів України

ЗМІСТ

ВСТУП

В сучасних інформаційних системах зберігається і обробляється велика кількість інформації різного ступеня відкритості. Створення інформаційної мережі є зручним способом отримання і передачі інформації. Разом з тим зростаючий рівень складності мережевих архітектур, підвищення ступеня відкритості мереж і все більш близький їх зв'язок до інтернету роблять актуальним питання безпеки інформації. Отримання несанкціонованого доступу до мережі, розголошення, зміна або знищення інформації, нелегальне використання ресурсів або виведення системи з ладу може мати катастрофічні наслідки. На сьогоднішній день існує велика кількість способів і засобів несанкціонованого доступу: мережеві атаки, комп'ютерні віруси, зломщики паролів.

В останні роки число атак, зафіксованих в інформаційних системах, стрімко зростає. Причин цього явища кілька. Перш за все, зросла кількість вразливостей, які що дня з'являються в програмному і апаратному забезпеченні. Крім того, кількість користувачів мереж, зокрема, інтернету, зростає з кожним днем. З ростом числа користувачів збільшується і кількість потенційних джерел і об'єктів атаки. Слід також зазначити, що сьогодні програмні засоби для здійснення атак стали досить простими, і поводження з ними не вимагає спеціальних знань. В інтернеті з легкістю можна знайти чимало програм, за допомогою яких будь-який недосвідчений користувач зможе організувати будь-яку атаку.

Одним з найактуальніших напрямків розвитку засобів захисту інформації на сьогоднішній день є системи виявлення вторгнень, що використовують методи виявлення аномалій. Методи виявлення аномалій базуються на тому, що аналізуючи дані і виявляючи відхилення між поточними даними і даними, отриманими за минулий період часу, можна розрізняти простих користувачів від зловмисників.

Розглядаючи проблему з економічної точки зору, її реалізація вимагає одноразових вкладень в обладнання на тривалий термін, що в свою чергу є

великим плюсом. По відношенню до збереженої інформації яка в сучасному світі досягає великих сум.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

На сьогоднішній день кожна країна світу підвергається мільйонам кібератак, державні уряди та інформаційні мережі не стали винятком атак зловмисників, а навпаки, ці сфери стали якщо не першими в списку зловмисник, то точно займають лідируючі позиції по величезному наступному ряду причин: потужне обладнання дозволяє реалізувати любу ідею, інформація як особиста так і з обмеженим доступом яка коштує великих грошей, виведення ресурсу з працездатності з метою нанесення шкоди, збитків. Найпоширенішим способом атак є BotNet, яка завдяки певній кількості пристроїв з запущеними на них спеціальним програмам виконують автоматично в заздалегідь задані команди за розкладом. Однією з найпопулярніших атак на сьогоднішній день є DDoS атака яка реалізується завдяки наступного ряду проблем: помилки в програмному коді; не до перевірка введених користувачем даних, що призводить до збільшення часу відповіді ресурсу; велика кількість одночасних запитів до системи, що призводить її практично в неробочий стан або повністю може відключити; "Помилкові атаки" які призводять систему в критичний стан так само сповільнюючи її працездатність. Однією з найпростіших, але не менш ефективних атак є простий підбір паролів, для його реалізації необхідно лише час, але чим потужніше обчислювальне обладнання, тим швидше проводиться підбір. Так само небезпеку для установи може представляти не тільки зловмисник, а так само і його співробітники, як навмисно так і ненавмисно.

Спеціалізований структурний підрозділ реагування на кіберінциденти державної служби спеціального зв'язку та захисту інформації України лише в період з 1 по 7 липня заблокував 1 тисяча 888 кібератак на державні органи влади, що на 80,3% менше, ніж з 24 по 30 червня. Зокрема, за вказаний період служба держспецзв'язку заблокувала 9 DDoS-атак, більшість з яких були здійснені на сайт офісу президента України. З 24 по 30 червня служба держспецзв'язку заблокувала 9 тисячі 608 кібератак на державні органи влади, що на 7% більше, ніж з 15 по 23 червня. В цілому для України атаки типу DDoS не є чимось новим. За даними

"Центру кібербезпеки при Нацкомісії з регулювання у сфері зв'язку та інформатизації", у другому кварталі 2020 року такі заклади як "Укрпошта", "Укрзалізниця", сайт Кабінету міністрів і ряду інших підприємств, стало причиною 46% кіберінцидентів в державному секторі. Основним завданням науково-технічної бібліотеки університету є інформаційне забезпечення навчального та наукового процесу. З розвитком форм навчання збільшується і кількість сервісів, що надаються бібліотекою.

Спеціалізований структурний підрозділ реагування на кіберінциденти державної служби спеціального зв'язку та захисту інформації України лише в період з 1 по 7 липня заблокував 1 тисяча 888 кібератак на державні органи влади, що на 80,3% менше, ніж з 24 по 30 червня. Зокрема, за вказаний період служба держспецзв'язку заблокувала 9 DDoS-атак, більшість з яких були здійснені на сайт офісу президента України. З 24 по 30 червня служба держспецзв'язку заблокувала 9 тисячі 608 кібератак на державні органи влади, що на 7% більше, ніж з 15 по 23 червня. В цілому для України атаки типу DDoS не є чимось новим. За даними "Центру кібербезпеки при Нацкомісії з регулювання у сфері зв'язку та інформатизації", у другому кварталі 2020 року такі заклади як "Укрпошта", "Укрзалізниця", сайт Кабінету міністрів і ряду інших підприємств, стало причиною 46% кіберінцидентів в державному секторі. Основним завданням науково-технічної бібліотеки університету є інформаційне забезпечення навчального та наукового процесу. З розвитком форм навчання збільшується і кількість сервісів, що надаються бібліотекою.

Через великий вплив бібліотеки в сучасному світі на навчальний процес, вона є одним з найбільш бажаних об'єктів атаки для зловмисників, та ще через те, що має сучасне та потужне обладнання. Оскільки бібліотека є часткою державного уряду, та вважається великою інформаційною системою на неї постійно проводять атаки різного характеру. Нижче представлено декілька атак на державні уряди та інформаційні мережі: - У 2015 році кіберзлочинці атакували систему управління трьох українських енергетичних компаній і дистанційно відключили подачу електроживлення. Найбільше тоді постраждала

«Прикарпаттяобленерго» 80 тисяч споживачів в Івано-Франківську і в інших містах Прикарпаття на шість годин опинилися без світла.

- У червні 2017 року на Українські заклади були зроблені хакерські атаки, які привели в непрацездатність мережі аеропорту "Бориспіль", "Укрпошти", "Укрзалізниці", сайт Кабінету міністрів і ряду інших підприємств. Програма-шифрувальник поширилася через сервер оновлень ПЗ для бухгалтерської звітності.

- У 2021 році 5 березня було проведено кібератака на Міністерства праці та соціальних справ Чехії, а також мерія Праги піддалися атаці, комп'ютерна мережа мерії піддалася масивної атаці зловмисників, але власна система кібербезпеки змогла її відобразити. Метою атаки була спроба злому робочої електронної пошти співробітників.

1.2 Нормативно-правова база

Захист інформації здійснюється відповідно до Законів і нормативними актами чинного законодавства України.

До законодавчих актів відносяться Закони, Укази, постанови Кабінету Міністрів України (ПКМУ) і Державні стандарти. До нормативних актів належать рекомендації, положення, методичні вказівки.

Обробка інформації в уряді здійснюється у відповідності з наступними законодавчими та нормативно-правовими документами:

- Закон України «Про інформацію» [1];
- Закон України «Про захист інформації в автоматизованих системах» [2];
- Закон України «Про науково-технічну інформацію» [3];
- Закон України «Про бібліотеки і бібліотечну справу» [4];
- ПКМУ № 611 «Про перелік відомостей, що не становлять комерційну таємницю» [5]
- ПКМУ № 1126 «Про затвердження концепції технічного захисту інформації в Україні» [6];

Державні стандарти України:

- ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення" [7];
- ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт» [8];
- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» [9];
- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [10];
- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [11];
- НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [12];
- НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання по створенню комплексної системи захисту інформації в автоматизованій системі» [13];
- НД ТЗІ 3.7-003-2005 «Порядок проведення робіт по створенню комплексної системи захисту інформації в інформаційних телекомунікаційних системах» [14]

1.3 Постановка задачі

Під час розробки дипломного проекту було сформовано та поставлено наступні задачі:

- провести обстеження ОІД;
- розробити модель порушника, існуючих та потенційних загроз;
- на базі існуючих загроз вибрати систему моніторингу;
- реалізація вибраної системи в мережі ОІД;
- економічне доведення необхідності впровадження системи моніторингу в ОІД.

1.4 Висновки до першого розділу

В першому розділі було описано актуальність проблеми кібератак на інформаційні ресурси в країні та світі, було наведено три крупні кібератаки за останні роки, прописані документи нормативно-правової бази які мають пряме

відношення до проблеми цієї галузі, було поставлено задачі для роботи в спеціальній частині.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про бібліотеку НТУ «Дніпровська політехніка»

Об’єктом інформаційної діяльності є науково-технічна бібліотека НТУ "Дніпровська Політехніка". Напрямом діяльності науково-технічної бібліотеки є забезпечення студентів, аспірантів, викладачів та співробітників університету підручниками, словниками та довідниками з загальноосвітніх і спеціальних дисциплін.

Науково-технічна бібліотека заснована у 1899 році. Бібліотека відноситься до першої категорії бібліотек закладів вищої освіти України. Фонд бібліотеки становить більше, ніж мільйон томів, більше 400 назв періодичних видань передплачує бібліотека щорічно, у тому числі реферативні журнали в електронному вигляді. Фонд бібліотеки щорічно поповнюється на 20 тисяч примірників друкованих документів. Електронний каталог нараховує понад 650 тисяч бібліографічних записів.

Науково-технічна бібліотека розташована на першому поверсі, вищого навчального закладу освіти НТУ "Дніпровська Політехніка", за адресою: місто Дніпро, проспект Дмитра Яворницького 19, перший корпус, перший поверх.

Режим роботи:

Робочі дні: понеділок - п’ятниця

Час роботи: 08:00 – 17:00

Перерва: 12:00 - 12:30

Штат працівників складає 37 осіб.

2.2 Організаційна структура бібліотеки

Під організаційною структурою управління розуміється склад, взаємодію, підпорядкованість, а так же розподіл роботи по підрозділам і управлінським органам, між якими формуються певні відносини, пов'язані з реалізацією владних повноважень, потоків розпоряджень та інформації.

Основою для появи і функціонування того чи іншого типу організаційної структури управління на підприємстві, а так само запорукою збільшення

продуктивності э горизонтальний поділ праці, при якому весь обсяг роботи розбивається на компоненти. [15]

Організаційна структура науково-технічної бібліотеки НТУ "Дніпровська Політехніка" складається з багатьох відділів, основні з них представлені нижче.

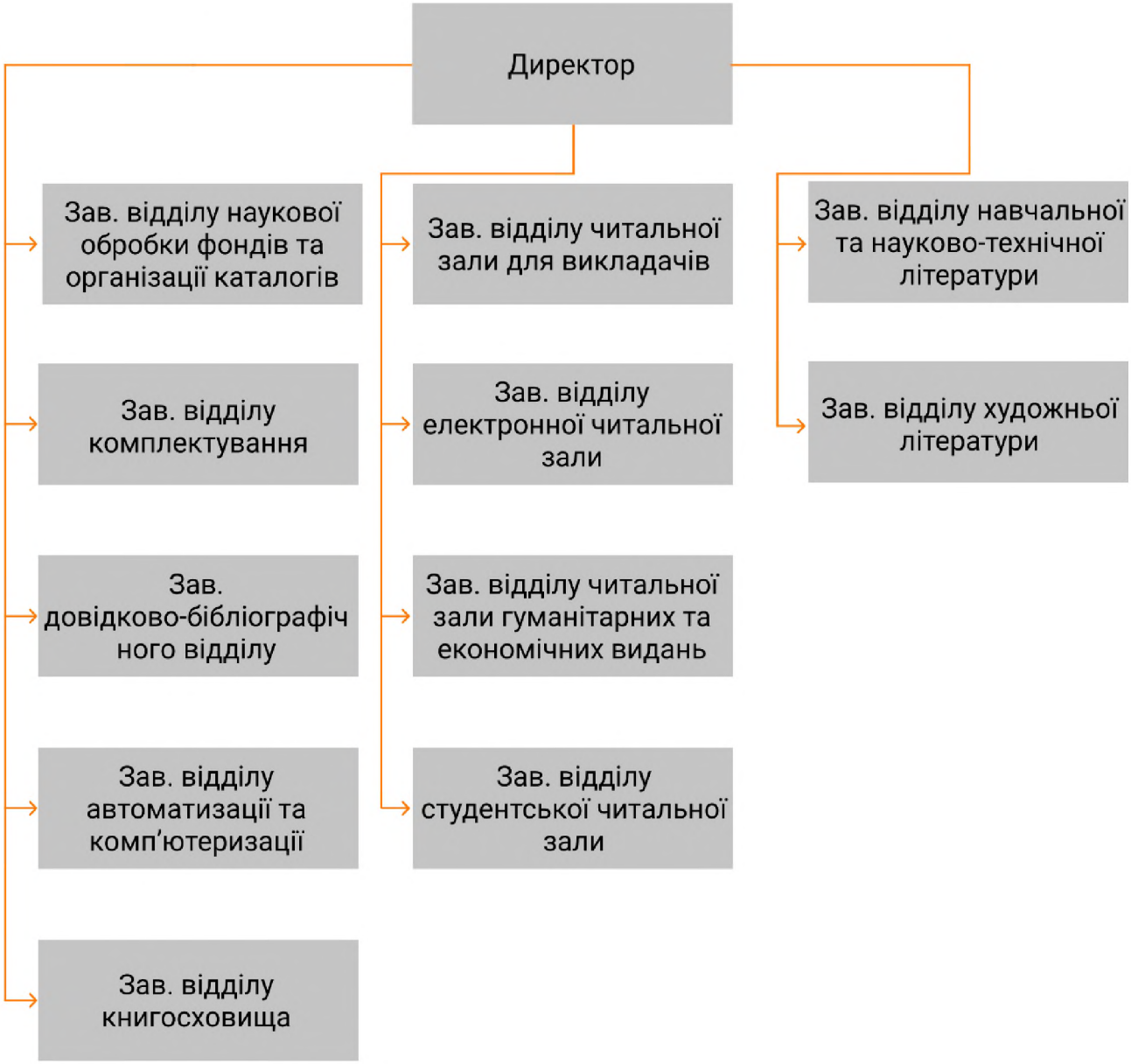


Рисунок 2.1 - організаційна структура

Директор – відповідає за організовану роботу бібліотеки.

Зав. відділу наукової обробки фондів та організації каталогів відповідає за науково-технічну обробку, тобто отримують повний бібліографічний опис, індекси класифікації та ключові слова. Надруковані картки потім розставляються до каталогів, користувачі дізнаються про нові надходження.

Зав. відділу комплектування – забезпечує формування фонду бібліотеки інформаційними ресурсами, а також удосконалення його відповідно з напрямками навчальної та наукової діяльності.

Зав. довідково-бібліографічного відділу – відповідає за відбір, розкриття змісту книг, журнальних статей, складання бібліографічних покажчиків, введення статей до електронного каталогу, визначення індексів бібліотечної класифікації для документів

Зав. відділу автоматизації та комп'ютеризації – побудову, супровід та розвиток інформаційної системи бібліотеки.

Зав. відділу книгосховища – забезпечує навчальними та науковими документами професорсько-викладацький склад, студентів та співробітників університету.

Зав. відділу читальної зали для викладачів – відповідає за доступність до довідкових та енциклопедичних видань, словників, автореферати дисертацій, дисертації, звіти про науково-дослідні роботи.

Зав. відділу електронної читальної зали – формування контенту та організацію доступу до нього для користувачів бібліотеки.

Зав. відділу читальної зали гуманітарних та економічних видань – відповідає за надання доступу до літератури з усіх дисциплін, що викладаються в «Інституті економіки» та «Інституті гуманітарних і соціальних наук».

Зав. відділу студентської читальної зали – видання із зазначених галузей знань з книгосховища.

Зав. відділу навчальної та науково-технічної літератури – забезпечує студентів, аспірантів, викладачів та співробітників університету підручниками, словниками та довідниками з загальноосвітніх і спеціальних дисциплін.

Зав. відділу художньої літератури – відповідає за підтримку зв'язку з громадськими організаціями міста, координувати роботу із підрозділами університету, підготовку та проведенням різноманітних заходів відділами бібліотеки.

2.3 Обстеження ОІД

Науково-технічна бібліотека НТУ "Дніпровська Політехніка" знаходиться у 3 поверховій будівлі на 1 першому поверсі та підвальних приміщеннях, першого корпусу вищого навчального закладу освіти НТУ "Дніпровська Політехніка", за адресою: місто Дніпро, проспект Дмитра Яворницького 19. ОІД займає 9 дев'ять аудиторій. Контрольована зона обмежена стінами приміщень.

Доступ на територію у денний час надається завдяки першому контрольному пункту охорони з вулиці Олеся Гончара 2 два, та другому контрольному пункту охорони на першому поверсі зі сторони центрального двору та перепустками.

У нічний час територія ОІД знаходиться під контролем внутрішньої охорони університету та системи сигналізації будівлі.

Далі наведений генеральний план кімнат які відносяться до ОІД

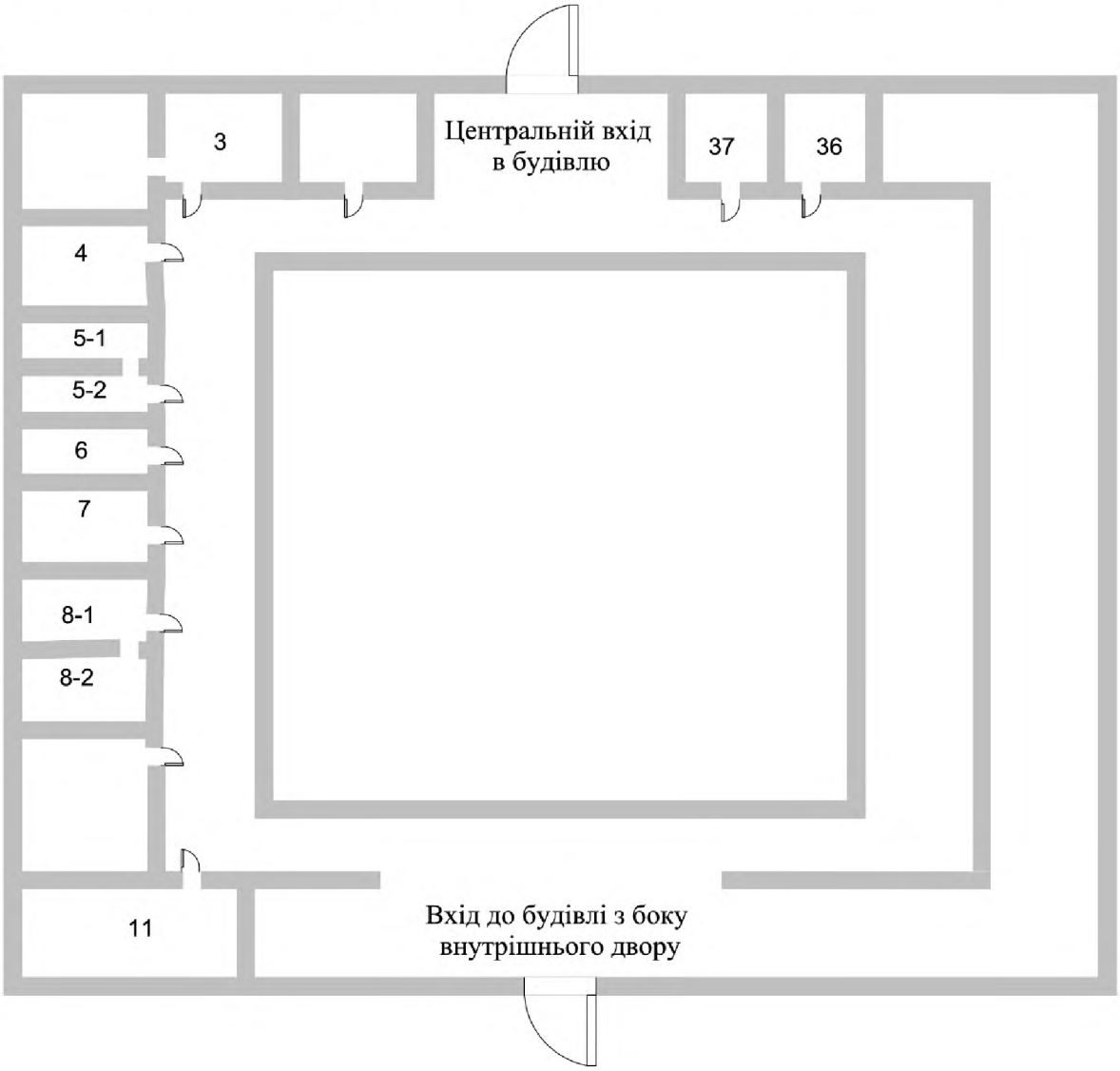


Рисунок 2.2 - генеральний план кімнат

На наступних кресленнях буде зображена комп'ютерна мережа ОІД:

На рисунку 2.3 зображено кімнату 3-1 в якій розташовано одне АРМ яке підключено до комутатора, який в свою чергу підключений до головного комутатора в кімнаті 5-2.

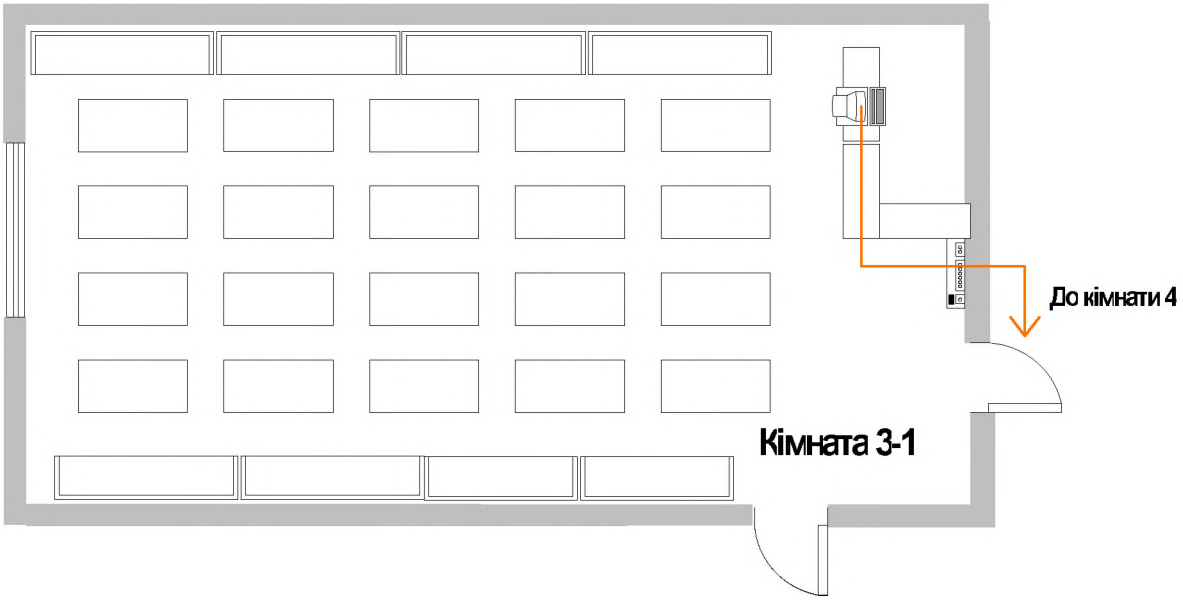


Рисунок 2.3 – кімната 3-1

На рисунку 2.4 зображено кімнату 4-1 в якій розташовано три АРМ які підключено до головного комутатора, через мережу в кімнаті 5-2.

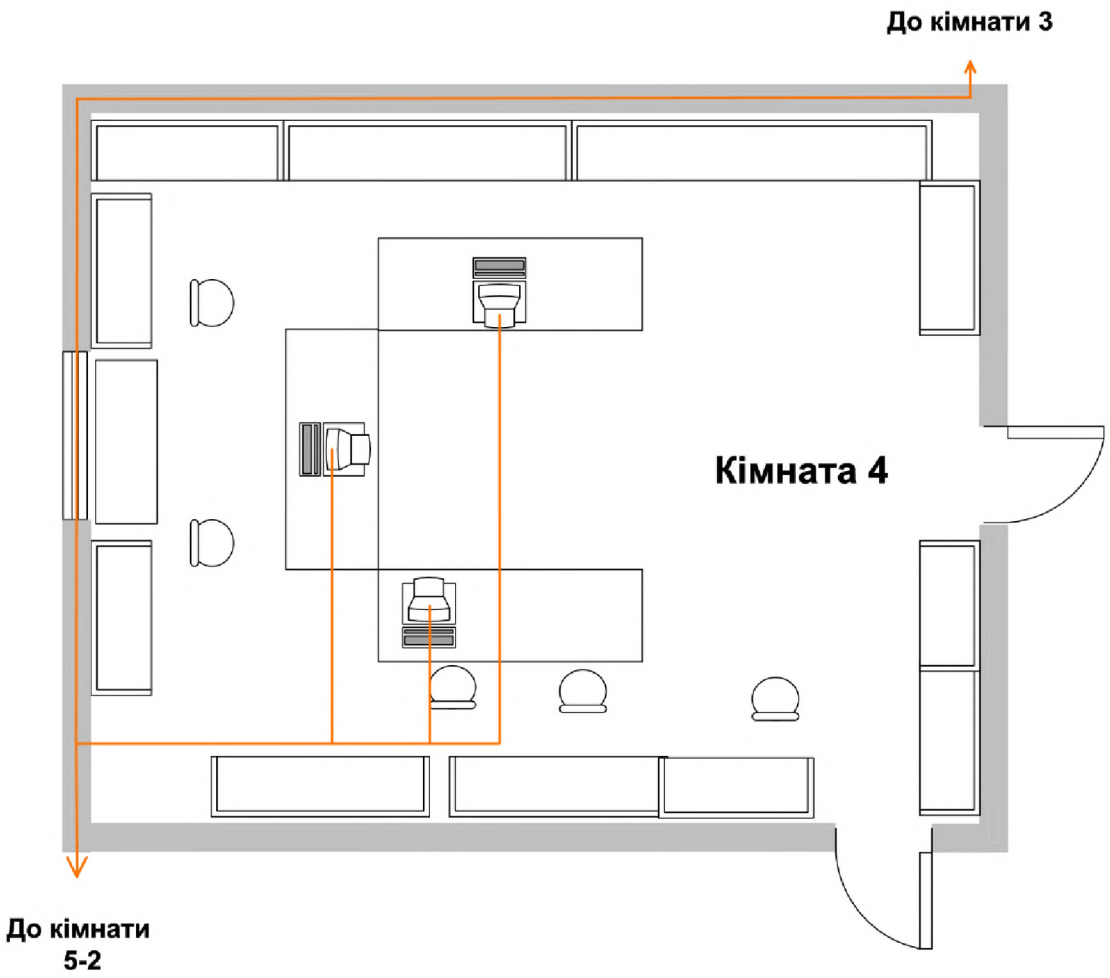


Рисунок 2.4 – кімната 4

На рисунку 2.5 зображено кімнату 5-1 та 5-2. В кімнаті 5-1 розташовано 4 АРМ які підключено до головного комутатора в кімнаті 5-2. В кімнаті 5-2 знаходиться 1 АРМ адміністратора мережі, сервер та головний комутатор мережі.

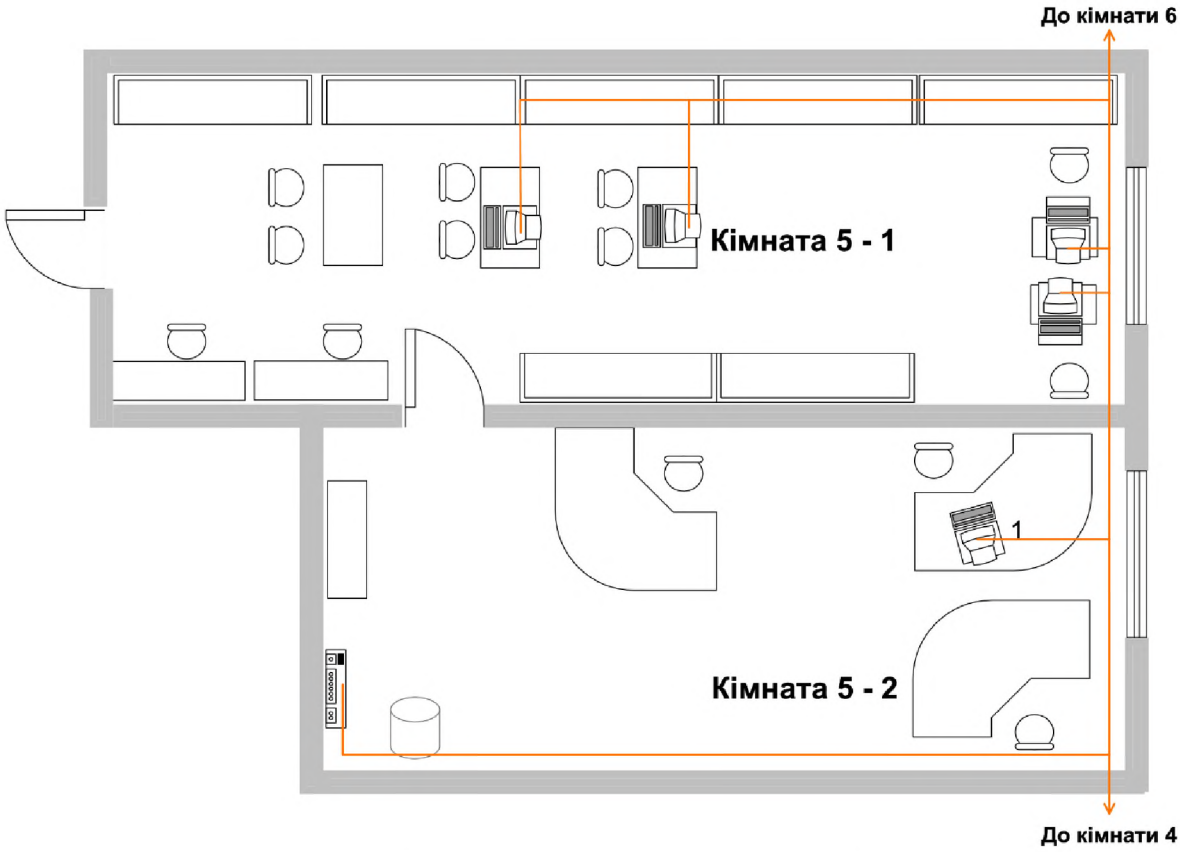


Рисунок 2.5 – кімната 5-1 та 5-2

На рисунку 2.6 зображено кімнату 6 в якій розташовано одне АРМ яке підключено до головного комутатора, через мережу в кімнаті 5-2.

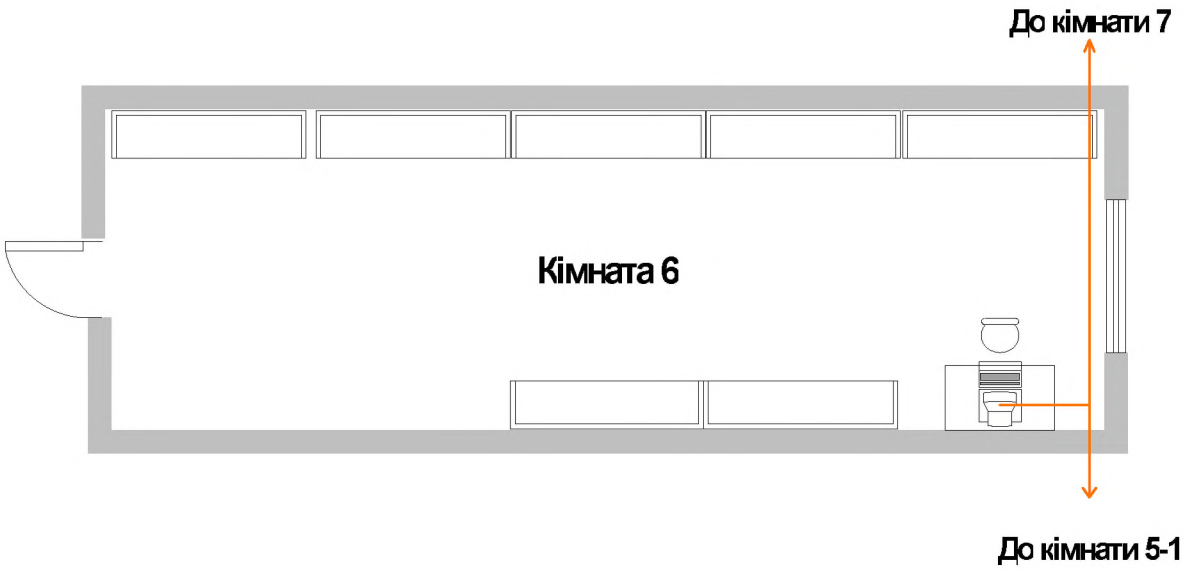


Рисунок 2.6 – кімната 6

На рисунку 2.7 зображено кімнату 7 в якій розташовано одне АРМ яке підключено до головного комутатора, через мережу в кімнаті 5-2.

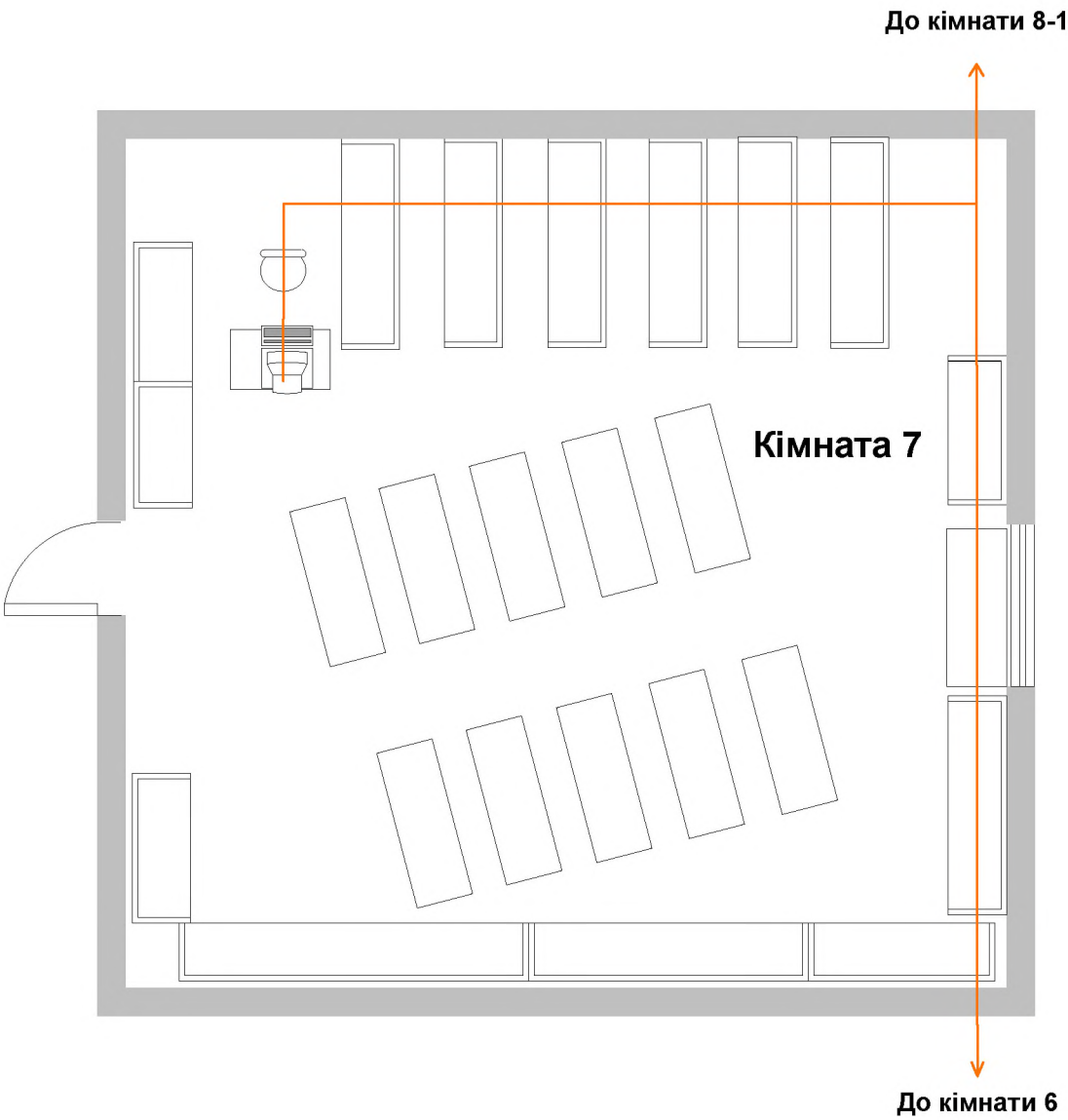


Рисунок 2.7 – кімната 7

На рисунку 2.8 зображено кімнати 8-1 та 8-2. Кімната 8-1 має 4 АРМ, та комутатор який підключено до кімнати 5-2. Кімната 8-2 має 5 АРМ, комутатор який підключено до кімнати 8-1.

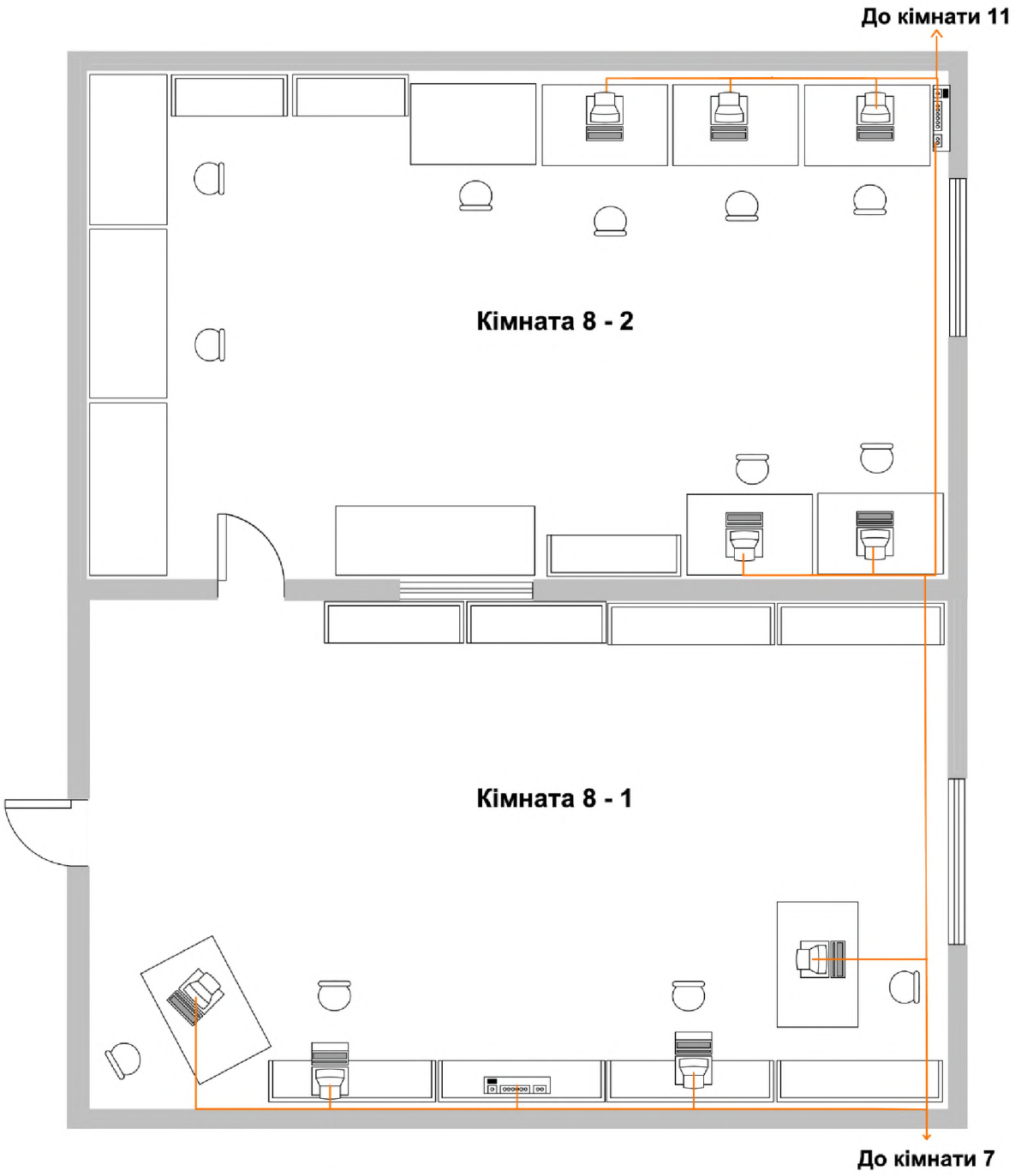


Рисунок 2.8 – кімната 8-1 та 8-2

На рисунку 2.9 зображено кімнату 11 в якій розташовано сім АРМ. Головне робоче місце підключено до мережі через комутатор в кімнаті 8-2. Останні шість АРМ підключено до мережі завдяки wi-fi з'єднанню.

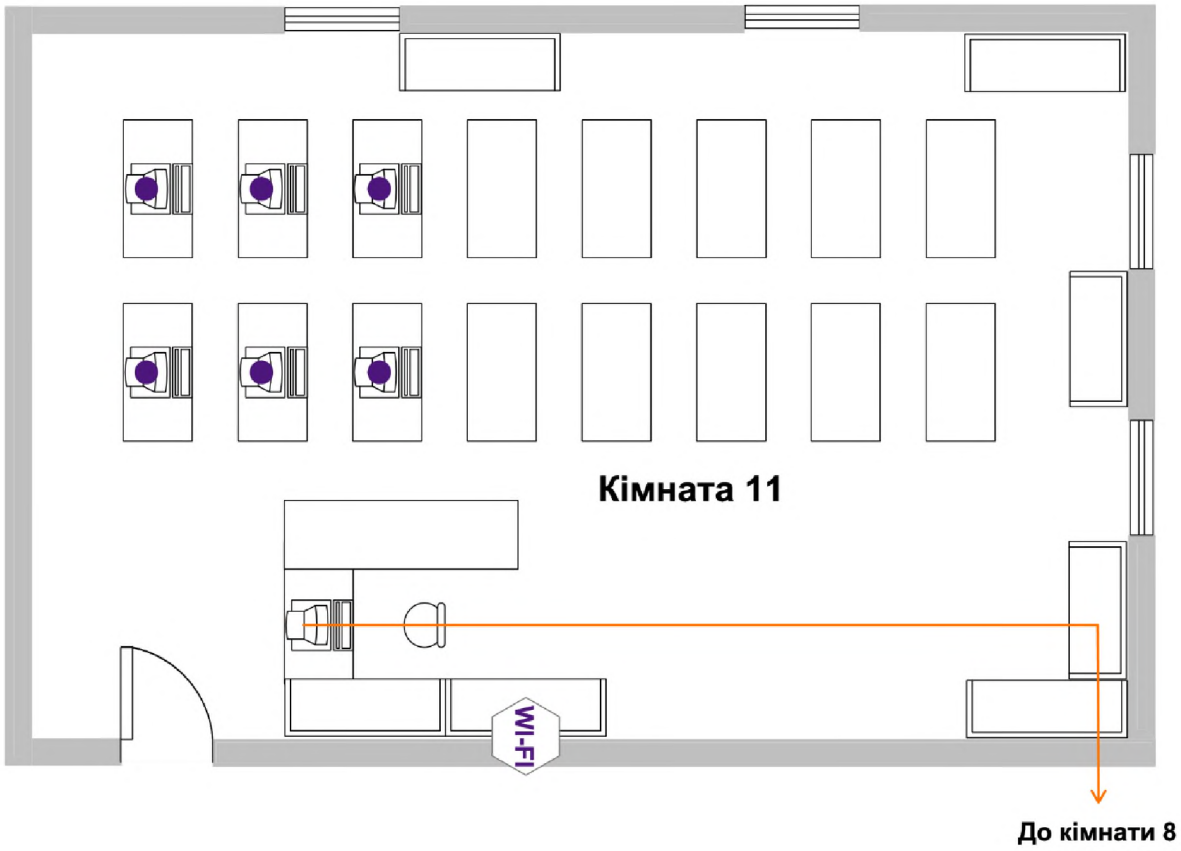


Рисунок номер 2.9 – кімната 11

На рисунку 2.10 зображено кімнату 36 в якій розташовано одне АРМ яке підключене до свого комутатора, який в свою чергу підключений до головного комутатора в кімнаті 5-2.

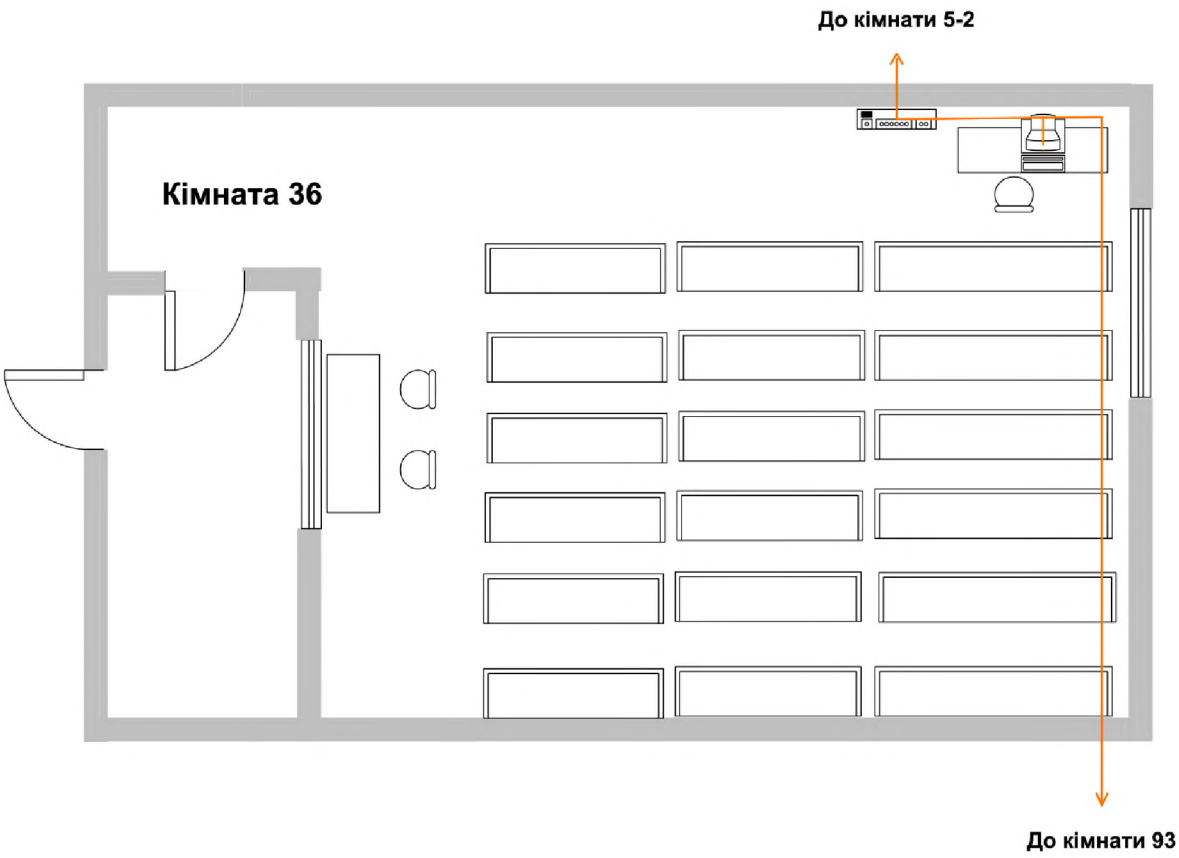


Рисунок 2.10 – кімната 36

На рисунку 2.11 зображено кімнату 37 в якій розташовано три АРМ які підключене до локального комутатора, який в свою чергу підключений до головного комутатора в кімнаті 5-2.

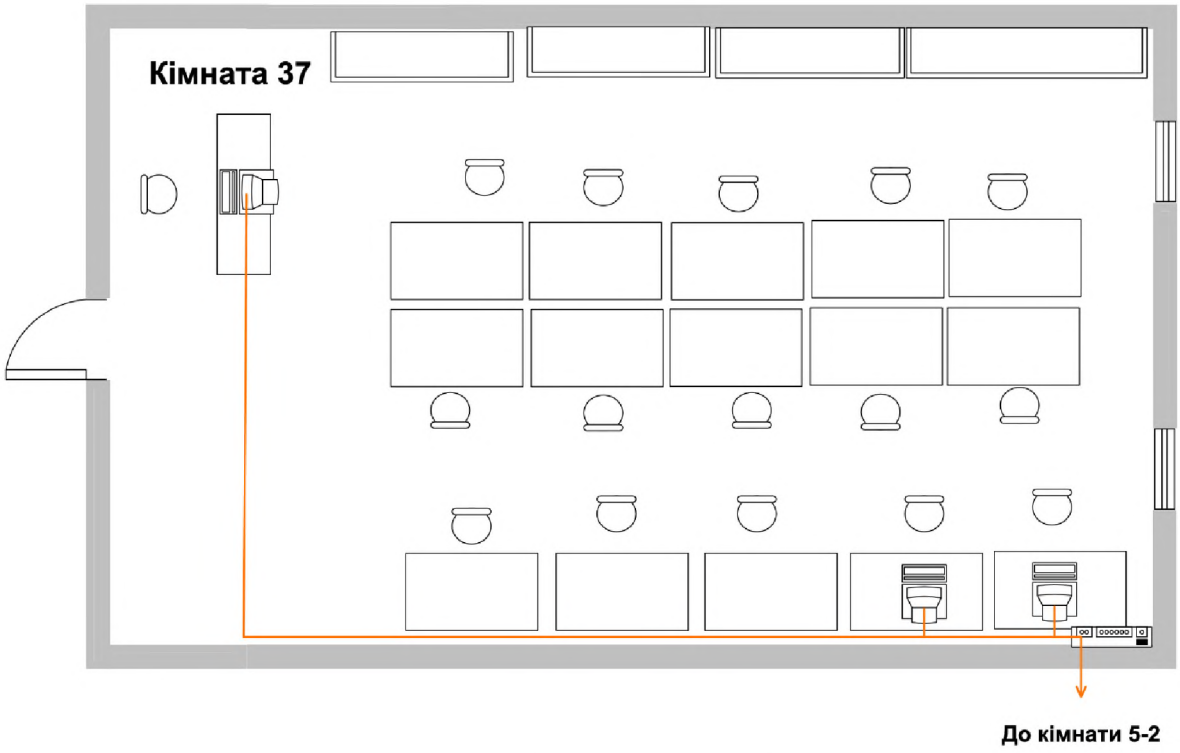


Рисунок 2.11 – кімната 37

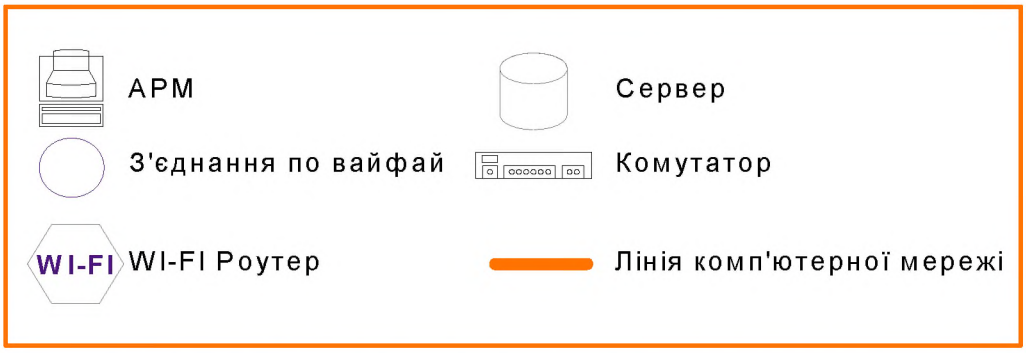


Рисунок 2.12 – Умовні позначення до рисунків

2.4 Основні технічні засоби

На генеральному плані приміщень приблизно зображені основні технічні засоби, більш детально описані в таблиці нижче.

Таблиця 2.1 - Інвентаризаційна відомість апаратного забезпечення:

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
1	АРМ 1 Робочий	монітор	Samsung Syncmaster 940	Кімната №3-1 (на столі)	0.3
		системний блок	CLF-815		0.3
		клавіатура	Logitech MK 120		0.4
		миша	Logitech M 100		0.4
2	АРМ 2 Робочий	монітор	Samsung Syncmaster 940	Кімната №4 (на столі)	1.2
		системний блок	CLF-815		1.2
		клавіатура	Logitech MK 120		1.4
		миша	Logitech M 100		1.4
3	АРМ 3 Робочий	монітор	Samsung Syncmaster 940	Кімната №4 (на столі)	1.2
		системний блок	CLF-815		1.2
		клавіатура	Logitech MK 120		1.4
		миша	Logitech M 100		1.4

Продовження таблиці 2.1

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
4	АРМ 4 Робочий	монітор	Samsung Syncmaster 940	Кімната №4 (на столі)	1.2
		системний блок	CLF-815		1.2
		клавіатура	Logitech MK 120		1.4
		миша	Logitech M 100		1.4
5	АРМ 5 Робочий	монітор	Samsung Syncmaster 940	Кімната №5-1 (на столі)	0.3
		системний блок	CLF-815		0.3
		клавіатура	Logitech MK 120		0.4
		миша	Logitech M 100		0.4
6	АРМ 6 Робочий	монітор	Samsung Syncmaster 940	Кімната №5-1 (на столі)	0.3
		системний блок	CLF-815		0.3
		клавіатура	Logitech MK 120		0.4
		миша	Logitech M 100		0.4
7	АРМ 7 Робочий	монітор	Samsung Syncmaster 940	Кімната №5-1 (на столі)	0.4
		системний блок	CLF-815		0.4
		клавіатура	Logitech MK 120		0.5
		миша	Logitech M 100		0.5
8	АРМ 8 Робочий	монітор	Samsung Syncmaster 940	Кімната №5-1 (на столі)	0.4
		системний блок	CLF-815		0.4
		клавіатура	Logitech MK 120		0.5
		миша	Logitech M 100		0.5
9	АРМ 9 Робочий	монітор	Samsung Syncmaster 940	Кімната №6 (на столі)	0.1
		системний блок	CLF-815		0.1
		клавіатура	Logitech MK 120		0.2
		миша	Logitech M 100		0.2

Продовження таблиці 2.1

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
10	АРМ 10 Робочий	монітор	Samsung Syncmaster 940	Кімната №7 (на столі)	0.5
		системний блок	CLF-815		0.5
		клавіатура	Logitech MK 120		0.6
		миша	Logitech M 100		0.6
11	АРМ 10 Робочий	монітор	Samsung Syncmaster 940	Кімната №8-1 (на столі)	0.4
		системний блок	CLF-815		0.4
		клавіатура	Logitech MK 120		0.5
		миша	Logitech M 100		0.5
12	АРМ 12 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №8-1 (на столі)	0.4
		системний блок	CLF-815		0.4
		клавіатура	Logitech MK 120		0.5
		миша	Logitech M 100		0.5
13	АРМ 13 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №8-1 (на столі)	0.2
		системний блок	CLF8-15		0.2
		клавіатура	Logitech MK 120		0.3
		миша	Logitech M 100		0.3
14	АРМ 14 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №8-1 (на столі)	0.2
		системний блок	CLF-815		0.2
		клавіатура	Logitech MK 120		0.3
		миша	Logitech M 100		0.3
15	АРМ 15 Робочий	монітор	Samsung Syncmaster 940	Кімната №8-2 (на столі)	0.1
		системний блок	CLF-815		0.1
		клавіатура	Logitech MK 120		0.2
		миша	Logitech M 100		0.2

Продовження таблиці 2.1

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
16	АРМ 16 Робочий	монітор	Samsung Syncmaster 940	Кімната №8-2 (на столі)	0.1
		системний блок	CLF-815		0.1
		клавіатура	Logitech MK 120		0.2
		миша	Logitech M 100		0.2
17	АРМ 17 Робочий	монітор	Samsung Syncmaster 940	Кімната №8-2 (на столі)	0.1
		системний блок	CLF-815		0.1
		клавіатура	Logitech MK 120		0.2
		миша	Logitech M 100		0.2
18	АРМ 18 Робочий	монітор	Samsung Syncmaster 940	Кімната №8-2 (на столі)	0.1
		системний блок	CLF-815		0.1
		клавіатура	Logitech MK 120		0.2
		миша	Logitech M 100		0.2
19	АРМ 19 Робочий	монітор	Samsung Syncmaster 940	Кімната №8-2 (на столі)	0.1
		системний блок	CLF-815		0.1
		клавіатура	Logitech MK 120		0.2
		миша	Logitech M 100		0.2
20	АРМ 20 Робочий	монітор	Samsung Syncmaster 940	Кімната №11 (на столі)	0.4
		системний блок	CLF-815		0.4
		клавіатура	Logitech MK 120		0.5
		миша	Logitech M 100		0.5
21	АРМ 21 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №11 (на столі)	0.5
		системний блок	CLF-815		0.5
		клавіатура	Logitech MK 120		0.6
		миша	Logitech M 100		0.6
22	АРМ 22 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №11 (на столі)	0.5
		системний блок	CLF-815		0.5
		клавіатура	Logitech MK 120		0.6
		миша	Logitech M 100		0.6

Продовження таблиці 2.1

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
23	АРМ 23 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №11 (на столі)	0.5
		системний блок	CLF-815		0.5
		клавіатура	Logitech MK 120		0.6
		миша	Logitech M 100		0.6
24	АРМ 24 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №11 (на столі)	0.5
		системний блок	CLF-815		0.5
		клавіатура	Logitech MK 120		0.6
		миша	Logitech M 100		0.6
25	АРМ 25 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №11 (на столі)	1
		системний блок	CLF-815		1
		клавіатура	Logitech MK 120		1.1
		миша	Logitech M 100		1.1
26	АРМ 26 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №11 (на столі)	1
		системний блок	CLF-815		1
		клавіатура	Logitech MK 120		1.1
		миша	Logitech M 100		1.1
27	АРМ 17 Робочий	монітор	Samsung Syncmaster 940	Кімната №36 (на столі)	0.2
		системний блок	CLF-815		0.2
		клавіатура	Logitech MK 120		0.3
		миша	Logitech M 100		0.3
28	АРМ 28 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №37 (на столі)	0.2
		системний блок	CLF-815		0.2
		клавіатура	Logitech MK 120		0.3
		миша	Logitech M 100		0.3
29	АРМ 29 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №37 (на столі)	0.2
		системний блок	CLF-815		0.2
		клавіатура	Logitech MK 120		0.3
		миша	Logitech M 100		0.3

Продовження таблиці 2.1

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
30	АРМ 30 Для читачів	монітор	Samsung Syncmaster 2243	Кімната №37 (на столі)	0.6
		системний блок	CLF-815		0.6
		клавіатура	Logitech MK 120		0.7
		миша	Logitech M 100		0.7
31	Комутатор №1	-	3C16754-ME	Кімната №3-1 (в шафі)	0.1
32	Комутатор №2	-	HP Pro-Curve Switch 2910al	Кімната №5-2 (в шафі)	0.1
33	Комутатор №3	-	HP Pro-Curve Switch 1910	Кімната №8-1 (в шафі)	0.1
34	Комутатор №4	-	HP Pro-Curve Switch 1910	Кімната №8-2 (в шафі)	0.1
35	Комутатор №5	-	Planet 16100	Кімната №36 (в шафі)	0.1

Продовження таблиці 2.1

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
36	Комутатор №6	-	D-Link DGS-1016A	Кімната №37 (в шафі)	0.1
37	Маршрутизатор №1	-	D-Link DAP-2690	Кімната №11 (на шафі)	0.2
38	Принтер №1	-	LP 2824 S	Кімната №5-1 (на столі)	0.4
39	Принтер №2	-	HP LJ 1200	Кімната №8-1 (на столі)	0.3
40	Принтер №3	-	HP LJ 1320tn	Кімната №8-1 (на столі)	0.4
41	Сканер №1	-	HP LJ 1300	Кімната №5-1 (на столі)	0.4

Продовження таблиці 2.1

№	Назва в ІТС	Характеристика		Розміщення	Відстань до межі ОІД в м.
		Найменування	Модель		
42	Сервер №1	-	Supermicro AS-2022G-TRF	Кімната №5-2 (в шафі)	0.2
43	Сервер №2	-	Supermicro AS-2042G-TRF	Кімната №101 (в шафі)	0.2

2.5 Обчислювальна система ОІД

На рисунку 2.13 зображена загальна топологія мережі бібліотеки, до якої входить до 8 груп об'єднаних мережевими комутаторами. Загальна кількість робочих місць 28, виділена демілітаризована зона в якій знаходиться сервер на якому розміщені усі інформаційні сервіси бібліотеки.

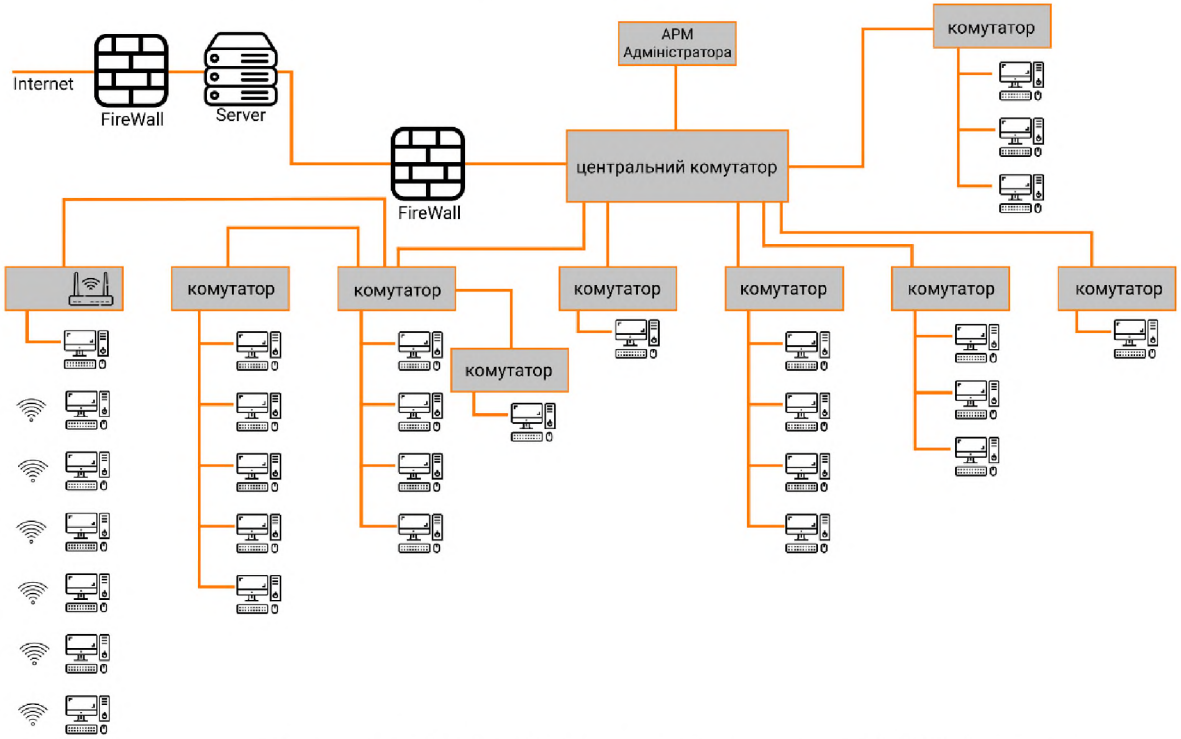


Рисунок 2.13 – Загальна схема мережі бібліотеки

На наступному рисунку 2.14 зображені основні інформаційні сервіси бібліотеки, до яких входить:

- ir.nmu.org.ua – інститутський репозиторій;
- lib.nmu.org.ua – сайт бібліотеки;
- media.nmu.org.ua – сховище медіа даних бібліотеки;
- libarch.nmu.org.ua – архів документів в публічному доступі / книги;
- catalog.nmu.org.ua – електронний каталог;
- ir.nmu.org.ua – бібліотечний хмарний сервіс;
- proc.nmu.org.ua – ресурс для обробки документів;
- stream.nmu.org.ua – поточний медіа сервіс.

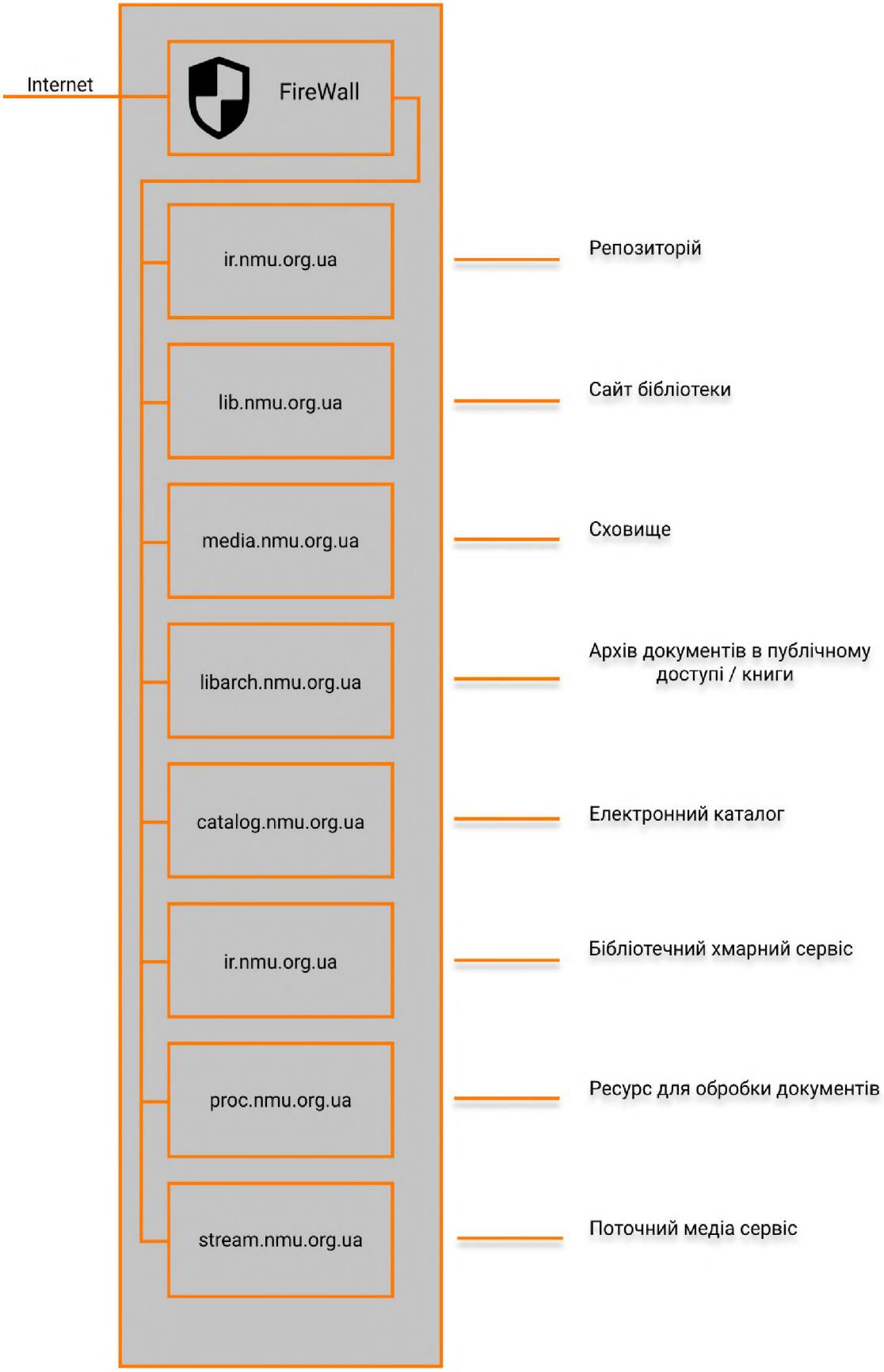


Рисунок 2.14 – Інформаційні сервіси бібліотеки

Таблиця 2.2 – Характеристика складу ІТС

№	Назва	Характеристика
1	АРМ для читачів	MB E45M1-M CPU AMD Fusion E-450 GPU Integrated RAM 4Gb DDR3 HDD 250 GB
2	АРМ Робочі	MB E45M1-M CPU AMD Fusion E-450 GPU Integrated RAM 4Gb DDR3 HDD 250 GB
3	Комутатор №1	3C16754-ME
4	Комутатор №2	HP Pro-Curve Switch 2910al-24G
5	Комутатор №3	HP Pro-Curve Switch 1910-16G
6	Комутатор №4	HP Pro-Curve Switch 1910-16G
7	Комутатор №5	Planet 16-port 10/100Base
8	Комутатор №6	D-Link DGS-1016A
9	Маршрутизатор №1	D-Link DAP-2690
10	Принтер №1	LP 2824 S
11	Принтер №2	HP LJ 1200
12	Принтер №3	HP LJ 1320tn
13	Сканер №1	HP LJ 1300
14	Сервер №1	Supermicro AS-2022G-TRF CPU: 2x Opteron 6476 RAM: 64 Gb DDR3 HDD: 21 Tb
15	Сервер №2	Supermicro AS-2042G-TRF CPU: 4x Opteron 6476 RAM: 192 Gb DDR4 HDD: 42 Tb

Таблиця 2.3 – Програмне забезпечення

№	Назва	Версія	Тип	Де встановлено
1	Windows	10	Системне	На всіх АРМ
2	Debian Linux	10	Системне	На сервері
3	УФД / Бібліотека	2.69	Прикладне	На сервері
4	Proxmax	6	Системне	На сервері
5	Adobe acrobat reader	8	Прикладне	На всіх АРМ
6	Office 365	2019	Прикладне	На всіх АРМ

2.6 Опис інформаційних потоків в ОІД

В бібліотечно-інформаційних системах при характеристиці інформації як предмета праці виділяють види інформації, відображені в наведеній нижче таблиці:

Таблиця 2.4 – Характеристика оброблюваної інформації.

Класифікація інформації	Види інформації
За місцем, займаному в виробничому процесі.	Вхідна, початкова, похідна, вихідна.
За місцем виникнення.	Зовнішня, внутрішня.
За відповідності відбиваним об'єктів.	Достовірна, недостовірна.
За рівнем відповідності важливість справ.	Корисна, некорисна, дезінформація.
По повноті.	Повна, неповна, надлишкова.
За ступенем релевантності.	Релевантна, що не релевантна.
За ступенем стабільності.	Умовно-постійна, змінна.
За ступенем аналітико-синтетичної переробки.	Первинна, вторинна.
За формою подання.	Текстова, графічна, числова, звукова, цифрова, візуальна, аудіовізуальна, мультимедійна.
За способом подання.	Аналогова, знакова.
За способом генерації і типу носія.	Документальна, вербальна, телекомунікаційна.
За періодичністю надходження.	Періодична, неперіодична.
За рівнем доступності.	Відкрита, закрита, конфіденційна.
За новизною.	Поточна, ретроспективна, оперативна.
За цільовим призначенням.	Наукова, науково-технічна, технічна, виробнича, суспільно-політична, науково-популярна.

Продовження таблиці 2.4

Класифікація інформації	Види інформації
За сферою застосування.	Економічна, юридична, політична, фінансова, сільськогосподарська, медична, історична, географічна, бухгалтерська, кадрова, маркетингова, управлінська, навчальна, бізнес-інформація.
За виконуваними функціями.	Нормативна, патентна, довідкова, технологічна, цінова, оперативно-виробнича, допоміжна, директивна, новинна.
За функціями управління.	Планова, контрольна, регулююча, аналітична, облікова, звітна, підсумкова.
За характером відомостей про об'єкт.	Бібліографічна, фактографічна, повнотекстова.
За охопленням відображених об'єктів.	Повна, вибіркова.
За ступенем точності відображення сукупності вибіркових об'єктів.	Репрезентативна, нерепрезентативна.
За умовами поширення.	Комерційна, некомерційна.
За рівнем структурованості.	Жорстко структурована, неструктурована, слабо структурована, неструктурована.

Вимоги до змісту інформаційного забезпечення пов'язані з такими його характеристиками, як:

- повнота інформації, необхідної для реалізації функцій і рішення задач;
- інтегративність, що виключає невиправдане дублювання інформації;
- надійність інформації, необхідної для прийняття управлінських рішень;
- сумісність з інформаційним забезпеченням суміжних інформаційних систем;
- достовірність;

- захищеність;

- доступність;

- своєчасність актуалізації;

- адаптованість до зовнішніх умов;

-можливість розширення, модернізації.

2.7 Розробка моделі порушника

Модель порушника розробляється з метою подальшого аналізу та вибору системи виявлення аномальних дій. Модель порушника відображає його практичні та теоретичні можливості, апріорні знання, час і місце. Порушники поділяються на внутрішніх порушників (ПВ) та зовнішніх порушників (ПЗ). Далі наведено таблиці з 2.6 – 2.10 які формують модель порушника.

Таблиця 2.5 – Модель порушника за мотивом здійснення

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок	4

Таблиця 2.6 – Модель порушника за рівнем кваліфікації та знань щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.7 – Модель порушника за показником можливостей використання засобів таметодів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.8 – Модель порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час оновлення або ремонту ІТС	1
Ч2	Під час оновлення або технічного обслуговування ІТС	2
Ч3	Під час функціонування ІТС	3
Ч4	Як у процесі функціонування ІТС, так і під час при зупинки компонентів системи	4

Таблиця 2.9 – Модель порушника за місцем дії

Позначення	Місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць працівників	2
Д3	З доступом у зону зберігання баз даних	3
Д4	З робочого місця адміністратора	4

Таблиця 2.10 – Модель порушника

Посада	Категорія	Специфікація / Рівень загроз					Сума загроз
		М/	К/	З/1	Ч/	Д/	
Директор	ПВ	М/1	К/2	З/2	Ч/1	Д/1	7
Адміністратор системи	ПВ	М/1	К/3	З/1	Ч/1	Д/4	11
Працівник	ПВ	М/1	К/1	З/1	Ч/3	Д/2	8
Технічний персонал	ПВ	М/1	К/2	З/1	Ч/3	Д/2	9
Представники служби безпеки	ПВ	М/1	К/1	З/1	Ч/1	Д/1	5
Читач	ПВ	М/2	К/1	З/1	Ч/1	Д/1	6
Зловмисник	ПЗ	М/3	К/3	З/4	Ч/4	Д/1	13
Конкуренти	ПЗ	М/3	К/3	З/2	Ч/2	Д/2	12
Представники комунальних служб	ПЗ	М/1	К/1	З/1	Ч/1	Д/1	5

Таким чином с зібраних та проаналізованих даних в таблиці (2.10) було виявлено, що найбільшу загрозу представляє зовнішній зловмисник

2.8 Аналіз існуючих та потенційних загроз

У цьому розділі було розглянуто основні та потенційні загрози причинами яких є порушення функціонування інформаційної системи, збої і відмови в роботі інформаційної системи, які частково або повністю перешкоджають функціонуванню, можливостям доступу до інформаційних ресурсів і послуг системи, причин втрати ІзОД. Далі представлено список загроз:

- Віддалене проникнення - інформаційні атаки, які дозволяють реалізувати дистанційне керування комп'ютером користувача інформаційних ресурсів системи по мережі на базі віддаленого доступу;

- Локальне проникнення це атака, що призводить до отримання несанкціонованого доступу до вузла, на якому вона запущена;

- Віддалений відмова в обслуговуванні це атаки, які дозволяють порушити функціонування інформаційної системи за умовами реалізації її послуг або мають можливість контрольованого перезавантаження системи шляхом віддаленого доступу;

- Локальний відмову в обслуговуванні це атаки, що дозволяють порушити функціонування системи або перезавантажити систему, на якій вони реалізуються. Перевантаження центрального процесора нескінченним циклом, що унеможливлює обробку запитів;

- Мережеві сканери це програми, які аналізують топологію мережі і виявляють сервіси, доступні для атаки;

- Зломщики паролів це програми, які підбирають паролі користувачів інформаційних ресурсів системи для подальших дій зловмисника;

- Аналізатори протоколів це програми, які прослуховують мережевий трафік. За допомогою цих програм можна автоматично знайти таку інформацію, як ідентифікатори і паролі користувачів.

2.9 Обґрунтування вибору системи

Найбільшою загрозою є зовнішній зловмисник який намагається захопити ресурси для створення бот мережі, або отримання НСД до документі з обмеженим доступом. Для запобігання цим загрозам пропонується використання системи виявлення вторгень. Велика кількість інформаційних сервісів потребує автоматизації виявлення аномального стану інформаційної системи, для цього пропонується використовувати систему моніторингу яка дозволяє отримати стан роботи окремих інформаційних сервісів та накопичення їх в одному місці з метою їх подальшої обробки.

Intrusion Detection Systems (IDS) - Система виявлення вторгнень, Intrusion Prevention Systems (IPS) - Система запобігання вторгнень.

IDS призначена для виявлення вторгнень в мережу. При виявленні потенційної кібератаки система видасть попередження. Сама система нічого не

робить для запобігання атаки, залишаючи цю відповідальність на адміністратора системи.

IPS працює, щоб запобігти успішну атаку. Якщо вторгнення виявлено, IPS відповість на основі заздалегідь визначених формул. Відповіді можуть включати блокування вхідного мережевого трафіку, знищення шкідливого процесу, розміщення файлу в карантин.

Недолік IPS полягає в тому, що вона може неправильно виявляти загрози та вживати заходів проти користувача, процесу, з'єднання. IDS краще використовувати, коли необхідно зберегти контроль над рішенням брати участь в реагуванні на інциденти, в той час як IPS має перевагу більш швидкого реагування на виявлені загрози без стороннього втручання.

Існує два основних видів систем виявлення вторгнень:

- Host-based Intrusion Detection System (HIDS) - Система виявлення вторгнень на основі хоста, вивчає події в комп'ютері в мережі;

- Network-based Intrusion Detection System (NIDS) - Мережева система виявлення вторгнень перевіряє трафік в мережі.

HIDS створює резервну копію файлів конфігурації мережі, щоб відновити настройки, якщо шкідливий вірус послабить безпеку системи, змінивши настройки комп'ютера. Наступний важливий елемент, від якого необхідно захиститися, - це root-доступ. HIDS не зможе заблокувати ці зміни, але зможе попередити, якщо такий доступ буде проведений неправомірно.

NIDS заснований на правилах, що дозволяють створювати так же вибірковий збір даних. Якщо є правило для типу викликає занепокоєння HTTP-трафіку, NIDS повинен приймати і зберігати тільки ті HTTP-пакети, які відображають ці характеристики.

Виявлення на основі аномалій шукає несподівані або незвичайні шаблони дій. Ця категорія також може бути реалізована як хостовою, так і мережевими системами виявлення вторгнень. Для HIDS аномалією можуть бути повторювані невдалі спроби входу в систему або незвичайна активність на портах пристрої, що означає сканування портів. Для NIDS підхід аномалій вимагає встановлення

базового рівня поведінки для створення стандартної ситуації, з якої можна порівнювати поточні моделі трафіку. Діапазон шаблонів трафіку вважається прийнятним і коли поточний трафік в реальному часі виходить за межі цього діапазону, викликається попередження про аномалії.

Вибір системи для реалізації полягає на унікальному середовищі організації, потреби виходячи з моделі порушника і розглянутих загроз. Далі представлена таблиця на базі якої обиралось система [16, 17] :

Таблиця 2.11 – характеристики елементів системи

Назва	ids/ ips	hids/ nids	Платформа	Плюси	Мінуси	Ціна в доларах
OSSEC	ips	hids	Linux MacOS Windows	-Відкрите джерело -Моніторинг реєстру Windows -Виявлення ескалації привілеїв MacOS -Відстежує контрольні суми файлів журналу для виявлення фальсифікації	-Обмежена підтримка Windows -Складне навчання	Безкоштовно
Snort	ips	nids	Windows Linux	-Велика бібліотека попередньо побудованих правил виявлення -Велика видимість мережевого трафіку	-Нестабільне оновлення	Безкоштовно

Продовження таблиці 2.11

Назва	ids/ ips	hids/ nids	Платформа	Плюси	Мінуси	Ціна в доларах
Suracata	ips	nids	MacOS Windows Linux	-Відкрите джерело -Збір даних на рівні програми -Велика видимість мережевого трафіку -Інтеграція з низкою сторонніх інструментів -Зручний інтерфейс -Паралельна обробка з підтримкою графічного процесора	-Велике навантаження на процесор	Безкоштовно
Zeek	ips	nids	MacOS Linux	-Відкрите джерело -Велика видимість мережевого трафіку -Інтегрована реєстрація трафіку -Завдання дозволяють налаштовувати автоматизацію	-Складне навчання	Безкоштовно
Sagan	ips	+	MacOS Linux	-Відкрите джерело. -Сумісний із даними Snort. -Багато сторонніх інтеграцій. -Інтеграція з брандмауерами для блокування IP.	-Складне навчання	Безкоштовно

Продовження таблиці 2.11

Назва	ids/ ips	hids/ nids	Платформа	Плюси	Мінуси	Ціна в доларах
SOS	ips	+	Linux	-Дистрибутив Linux з відкритим кодом. -Інтегрує низку інструментів.	-Немає автоматизації дій. -Деякі інтерфейси не зручні для користувача.	Безкоштовно
McAfee	ips	nids	Windows	-Захист від ботів. -Блокує шкідливі сайти.	-Помилкові спрацьовування для виявлення шкідливих ділянок. -Негативно впливає на продуктивність мережі.	Від 11.000
Palo Alto Networks	ips	nids	Linux	-Постійне оновлювання профілю захисту від загроз. -Блокує шкідливі сайти.	-Не гнучка настройка. -Відсутність видимості підписів.	Від 9.500
Fail2Ban	ips	hids	MacOS Linux	-Аналіз журналу файлів для виявлення підозрілих подій. -Автоматичне блокування підозрілих / зловмисних IP-адрес.	- Зосереджується на повторних зловмисних діях з однієї IP-адреси, що може призвести до DDos-атаки.	Безкоштовно

На базі розглянутої таблиці було обрано систему Security Onion Solution (SOS) через наявність протоколу IPS, NIDS та HIDS, працездатність на системі Linux та відсутності ціни.

2.10 Встановлення та налаштування системи моніторингу

Для створення дзеркала моста використовується Open vSwitch (ovs). Копію всіх мережевих пакетів дзеркало надсилає через інтерфейс, який було підключено до системи безпеки Onion VM для аналізу.

На схемі нижче показано який вигляд має мережа до додавання лабораторії загроз:

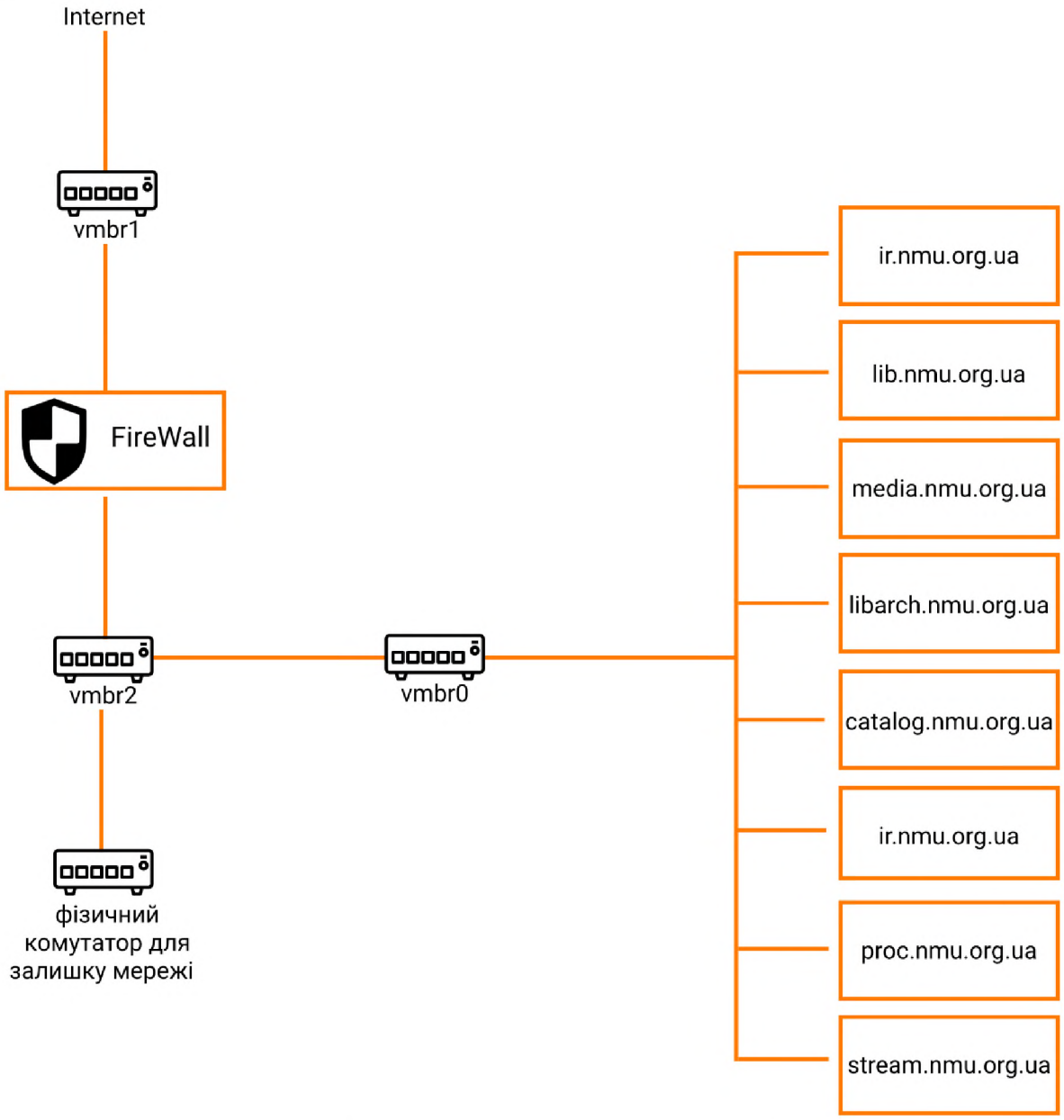


Рисунок 2.15 - мережа до додавання системи моніторингу

Яким був `/etc/network/interfaces` до переходу на ovs:

```
auto lo
iface lo inet loopback
auto enp7s0
iface enp7s0 inet manual
```

```
auto enp2s0
iface enp2s0 inet manual
auto enp3s0
iface enp3s0 inet manual

auto vmbr0
iface vmbr0 inet static
        address 10.11.1.124/24
        gateway 10.11.1.1
        bridge-ports enp7s0
        bridge-stop off

auto vmbr1
iface vmbr1 inet manual
        bridge-ports enp2s0
        bridge-stp off
        bridge-fd 0

auto vmbr2
iface vmbr2 inet manual
        bridge-ports enp3s0
        bridge-stp off
        bridge-fd 0
```

Зазначаємо як розміщений файл `/etc/network/interfaces` для роботи з ovs і vlan загрози (vlan10), де буде знаходиться Security Onion Solution (SOS) та будь які інші лабораторні машини:

```
iface lo inet loopback
auto enp7s0
iface enp7s0 inet manual
auto enp2s0
iface enp2s0 inet manual
auto enp3s0
iface enp3s0 inet manual

# VMBR0
allow-ovs vmbr0
iface vmbr0 inet static
        address 10.11.1.124
        netmask 255.255.255.0
        gateway 10.11.1.1
        ovs_type OVSBridge
```

```
        ovs_ports enp7s0 vlan10
allow-vmbr0 enp7s0
iface enp7s0 inet manual
        ovs_bridge vmbr0
        ovs_type OVSPort
allow-vmbr0 vlan10
iface vlan10 inet static
        ovs_type OVSIntPort
        ovs_bridge vmbr0
        ovs_options tag=10

# VMBR1
allow-ovs vmbr1
iface vmbr1 inet dhcp
        ovs_type OVSBridge
        ovs_ports enp2s0
allow-vmbr1 enp2s0
iface enp2s0 inet manual
        ovs_bridge vmbr1
        ovs_type OVSPort

# VMBR2
allow-ovs vmbr2
iface vmbr2 inet manual
        ovs_type OVSBridge
        ovs_ports enp3s0 vlan10
allow-vmbr2 enp3s0
iface enp3s0 inet manual
        ovs_bridge vmbr2
        ovs_type OVSPort
allow-vmbr2 vlan10
iface vlan10 inet static
        ovs_type OVSIntPort
        ovs_bridge vmbr2
        ovs_options tag=10
```

Цей варіант є доцільнішим, то що SOS спостерігає за всім трафіком мережі, включаючи все машини та пристрої, які підключені до мережі.

На схемі нижче показано який вигляд має мережа зараз:

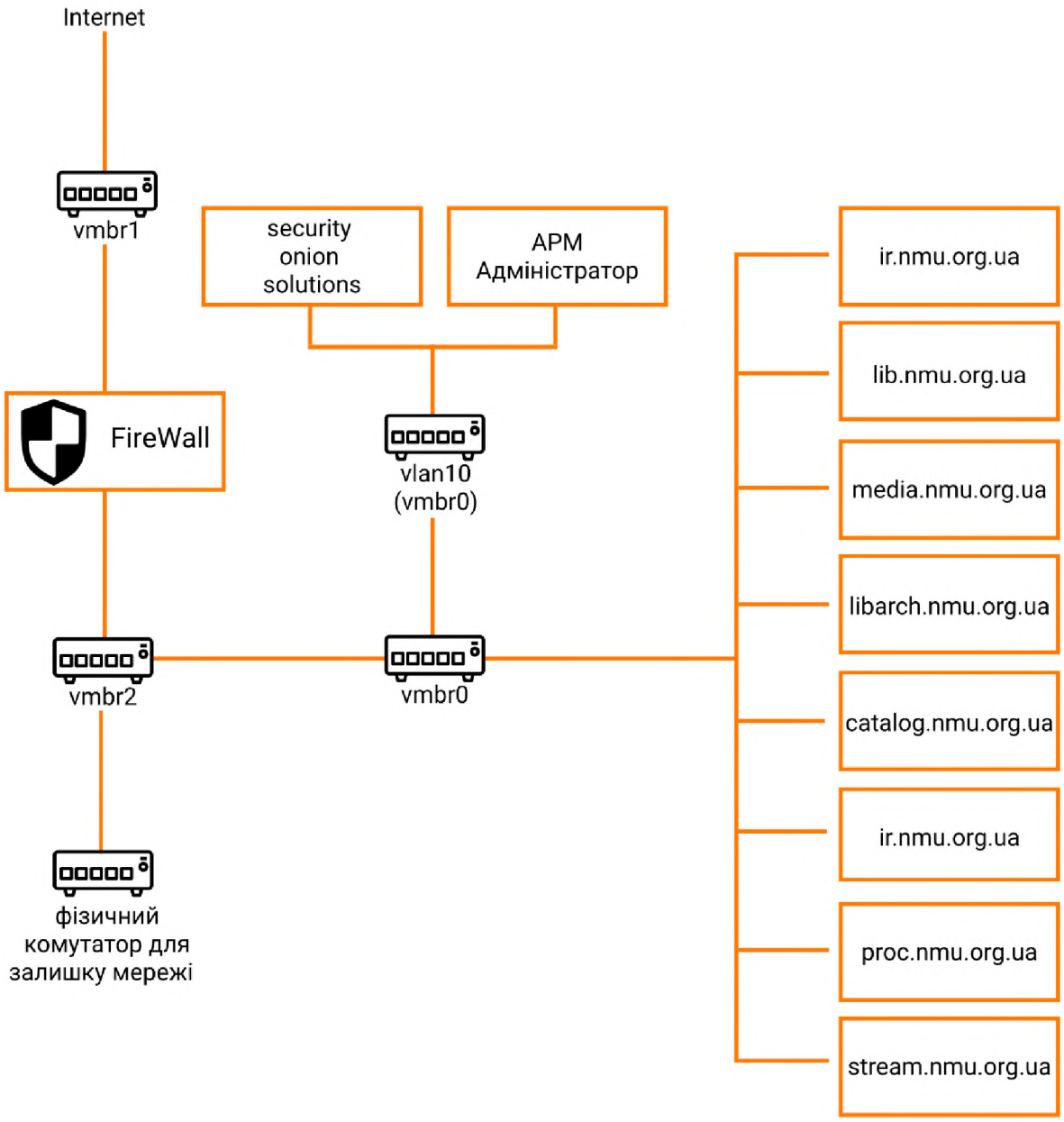


Рисунок 2.16 - мережа після додавання системи моніторингу

SOS перевантажений програмами, що працюють над ресурсами у докеризованих контейнерах. Для реалізації було виділено 1 терабайт пам'яті , та 32 гігабайти оперативної пам'яті, в результаті коливання дорівнювали 60 % відсоткам. Було встановлено версію PROD. [18]

Необхідно два мережевих інтерфейси управління: управління та sniffing interface. Інтерфейс управління, який має значення eth0 і має статичний IP, це адреса, з якої надається доступ до веб-інтерфейсу або ssh до машини. Sniffing interface, eth1 це порожній інтерфейс, для якого proxmox автоматично зробить пристрій, який

використовується для з'єднання дзеркального відображення порту ovs. На наступному рисунку 2.17 зображено характеристики системи.

Memory	8.00 GiB/64.00 GiB
Processors	8 (1 sockets, 8 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
Hard Disk (scsi0)	storage:151/vm-151-disk-0.qcow2,size=1T
Network Device (net0)	virtio=12:B7:58:A5:A3:84,bridge=vmbr0,firewall=1
Network Device (net1)	e1000=7A:17:97:D6:F0:6B,bridge=vmbr0,firewall=1
Network Device (net2)	virtio=E2:20:B6:5C:99:8B,bridge=vmbr1,firewall=1

Рисунок 2.17 – технічні характеристики віртуаьної системи моніторингу.

Необхідно застосувати ovs для налаштування порту дзеркала `/span port`. Цю команду необхідно виконувати з терміналу proxmox.

```
ovs-vsctl -- --id=@p get port tap151i1 \
    -- --id=@m create mirror name=span1 select-all=true output-port=@p \
    -- set bridge vmbr2 mirrors=@m
```

У рядку 1, `--id=@p get port tap151i1` надає ідентифікатор того порту tap, який proxmox створює для кожного мережевого інтерфейсу, підключеного до віртуальної машини і встановлює для нього змінну `@p tap151i1` пристрої з'єднання для ідентифікатора vm 151, а другий інтерфейс eth1.

У рядку 2, `--id=@m create mirror name=span1 select-all=true output-port=@p`, створюється саме дзеркало, вказується що весь трафік виводиться до визначеного порту @p.

У рядку 3 закріплюємо дзеркало за мостом vmbr2.

Низче приведений код який має вийти:

```
root@pve:~# ovs-vsctl -- --id=@p get port tap151i1 \
>     -- --id=@m create mirror name=span1 select-all=true output-port=@p \
>     -- set bridge vmbr2 mirrors=@m
982bcd81-6185-4cfc-a5b2-cd34d4a8ac61
root@pve:~# ovs-vsctl list Mirror
_uuid               : 982bcd81-6185-4cfc-a5b2-cd34d4a8ac61
external_ids        : {}
name                : "span1"
output_port         : a1ab59be-754f-43b3-ba2e-7900e11ee343
```

```
output_vlan          : []
select_all           : true
...
```

У терміналі SOS є можливість перевірки вихідних даних завдяки команді: tcpdump `-vv -i eth1`.

2.11 Тестування системи виявлення аномалій

Було налаштовано необхідний діапазон пристроїв з ovs. Для перевірки чи все працює, було запущено простий tcpdump тест. При введені команди tcpdump –vv –I eth1, повинні захоплюватися пакети. Нижче зображені строки коду як саме відбувається захоплення пакетів з ssh:

```
05:36:50.821537 IP (tos 0x0, ttl 127, id 25346, offset 0, flags [DF], proto TCP
(6), length 104)
    10.11.1.3.57393 > onion.ssh: Flags [P.], cksum 0xc661 (correct), seq
4801:4865, ack 1193088, win 8212, length 64
05:36:50.821620 IP (tos 0x0, ttl 127, id 25347, offset 0, flags [DF], proto TCP
(6), length 40)^C
    10.11.1.3.57393 > onion.ssh: Flags [.], cksum 0x717a (correct), seq 4865, ack
1193664, win 8210, length 0

4557 packets captured
4560 packets received by filter
0 packets dropped by kernel
```

Коли була доведена правильна робота встановленого та налаштованого SOS. Наступним відбувається більш складне випробування для перевірки SOS на доцільність відправки попереджень завдяки скрипту tmNIDS, який зроблен для тестування мережевих систем виявлення вторгнень завдяки повторенню файлів, які повинні запускати сповіщення SOS. [19]

Для запуску скрипта потрібно ввести в термінал наступні строки:

```
curl-sSL
https://raw.githubusercontent.com/0xtf/testmynids.org/master/tmNIDS-o
/tmp/tmNIDS && chmod +x /tmp/tmNIDS && /tmp/tmNIDS
```

Після вводу цих строк скрип почне свою роботу і повинен виглядати наступним чином:

```
_              _   _ _____ _____    _____
| |            | \ | |_   _|  __ \ / ____|
| |_ _ __ ___ |  \| | | | | |  | | (___
| __|  _   _ \| .   | | | | |  | |\___ \
| |_| | | | | | |\  |_| |_| |__| |____) |
 \__|_| |_| |_|_| \_|_____|_____/|_____/

tmNIDS - NIDS detection tester - @0xtf
Project: https://github.com/0xtf/testmynids.org

Choose which test you'd like to run:

 1) Linux UID
 2) HTTP Basic Authentication
 3) HTTP Malware User-Agent
 4) Bad Certificate Authorities
 5) Tor .onion DNS response and known IPs connection
 6) EXE or DLL download over HTTP
 7) PDF download with Embedded File
 8) Simulate SSH Outbound Scan
 9) Miscellaneous domains (TLD's, Sinkhole, DDNS, etc)
10) MD5 in TLS Certificate Signature
11) CHAOS! RUN ALL!
12) Quit!
#? 11
```

Через хвилину скрипт закінчить свою роботу і на сторінці сповіщень SOS повинні бути наступні результати:

	Count	rule.name	event.module	event.sev
	10	ET POLICY Signed TLS Certificate with md5WithRSAEncryption	suricata	low
	4	ET POLICY curl User-Agent Outbound	suricata	medium
	2	ET SCAN Potential SSH Scan OUTBOUND	suricata	medium
	1	ET DNS Query for .su TLD (Soviet Union) Often Malware Related	suricata	medium
	1	ET DNS Reply Sinkhole - sinkhole.cert.pl 148.81.111.111	suricata	high
	1	ET INFO DYNAMIC_DNS Query to a Suspicious no-ip Domain	suricata	medium
	1	ET INFO Packed Executable Download	suricata	low
	1	ET MALWARE Cryptowall .onion Proxy Domain	suricata	high
	1	ET MALWARE Delphi Trojan Downloader User-Agent (JEDI-VCL)	suricata	high
	1	ET MALWARE SuperFish Possible SSL Cert Signed By Compromised Root CA	suricata	high
	1	ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR	suricata	high
	1	ET POLICY Executable served from Amazon S3	suricata	medium
	1	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	suricata	high
	1	ET POLICY PDF With Embedded File	suricata	medium
	1	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
	1	ET TOR Known Tor Exit Node Traffic group 110	suricata	medium
	1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 110	suricata	medium
	1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 272	suricata	medium
	1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 285	suricata	medium
	1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 608	suricata	medium
	1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 653	suricata	medium
	1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 821	suricata	medium
	1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 825	suricata	medium
	1	ET USER_AGENTS Suspicious User Agent (BlackSun)	suricata	high
	1	ET USER_AGENTS Suspicious User Agent (agent)	suricata	high
	1	ET USER_AGENTS Suspicious User-Agent (HttpDownload)	suricata	high
	1	ET USER_AGENTS Suspicious User-Agent (MSIE)	suricata	high
	1	ET WEB_CLIENT Possible eDellRoot Rogue Root CA	suricata	high
	1	GPL ATTACK_RESPONSE id check returned root	suricata	medium

Рисунок 2.18 – результати сповіщень.

2.12 Розгортання агента кінцевої точки

Osqury реалізує можливість створювати запити до кінцевих точок так, ніби то вони знаходяться у базі даних. SOS використовує Kolid Fleet для керування завданнями та надання інформації про кінцеві точки мережі. Після відкриття Fleet в SOS, ви побачите машину для самого SOS. Воно надає можливість переглядати інформацію про кінцеві точки, та надсилати запити до SQL що до цієї інформації.

Встановлення агенту Osquery здійснюється через первинну загрузку з веб-інтерфейсу SOS за посиланням [https://sos.nmu.org.ua/#/downloads][20]. Пакет заздалегідь поставляється налаштованим для правильного та швидкого налаштування. Все що необхідно було зробити, це після завантаження через scp для завантаження на нову віртуальну машину, яка була запущена під управлінням Debian 10.

Після відкриття Fleet в інтерфейсі відображається нова зареєстрована кінцева точка.

Wazuh це система виявлення вторгнень на основі хоста, яка надає більше даних та сповіщень на основі системних даних, таких як журнали та хеші файлів, надіслані з кінцевих точок. Для установки агенту Wazuh були виконані наступні дії:

```
apt-get install curl apt-transport-https lsb-release gnupg2
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
echo "deb https://packages.wazuh.com/3.x/apt/ stable main" | tee
/etc/apt/sources.list.d/wazuh.list
apt update
```

На диспетчері SOS додаємо агент та витягуємо ключ, запустивши команду: `so-wazuh-agent-manage`:

```
root@onion ~]# so-wazuh-agent-manage


****************************************
* Wazuh v3.13.1 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: agent1
   * The IP Address of the new agent: 192.168.1.72
Confirm adding it?(y/n): y
Agent added with ID 002.


****************************************
* Wazuh v3.13.1 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
```

```
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: onion, IP: 192.168.1.70
   ID: 002, Name: agent1, IP: 192.168.1.72
Provide the ID of the agent to extract the key (or '\q' to quit): 2

Agent key information for '002' is:
MDAyIGFnZW50MSAxOTIuMTY4LjEuNzIgNzEzODA3NDI4Y2JhMDYxZTIxZjYxMDAyZjU1NmQ1MmU1MDIzMW
Q4OTNkZmI0YjM4NWEyMDhmYWRkYjYxNWNlOA==
```

В агенті запускаємо `/var/ossec/bin/manage_agents`, щоб додати до нього ключ:

```
root@agent1 ~# /var/ossec/bin/manage_agents


****************************************
* Wazuh v3.13.1 Agent manager.         *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: i

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAyIGFnZW50MSAxOTIuMTY4LjEuNzIgNzEzODA3NDI4Y2JhMDYxZTIxZjYxMDAyZjU1NmQ1MmU1MDIzMW
Q4OTNkZmI0YjM4NWEyMDhmYWRkYjYxNWNlOA==

Agent information:
   ID:002
   Name:agent1
   IP Address:192.168.1.72

Confirm adding it?(y/n): y
Added.
```

В агенті відредаговано `/var/ossec/bin/manage_agents` і замінено manager_ip на ip хост SOS та перезапущено:

```
sed -i 's/MANAGER_IP/192.168.1.70/g' /var/ossec/etc/ossec.conf
systemctl restart wazuh-agent
```

При первинній перевірці веб-графічного інтерфейсу на наявність сповіщень, можливо побачити значну кількість центрі тестів безпеки.

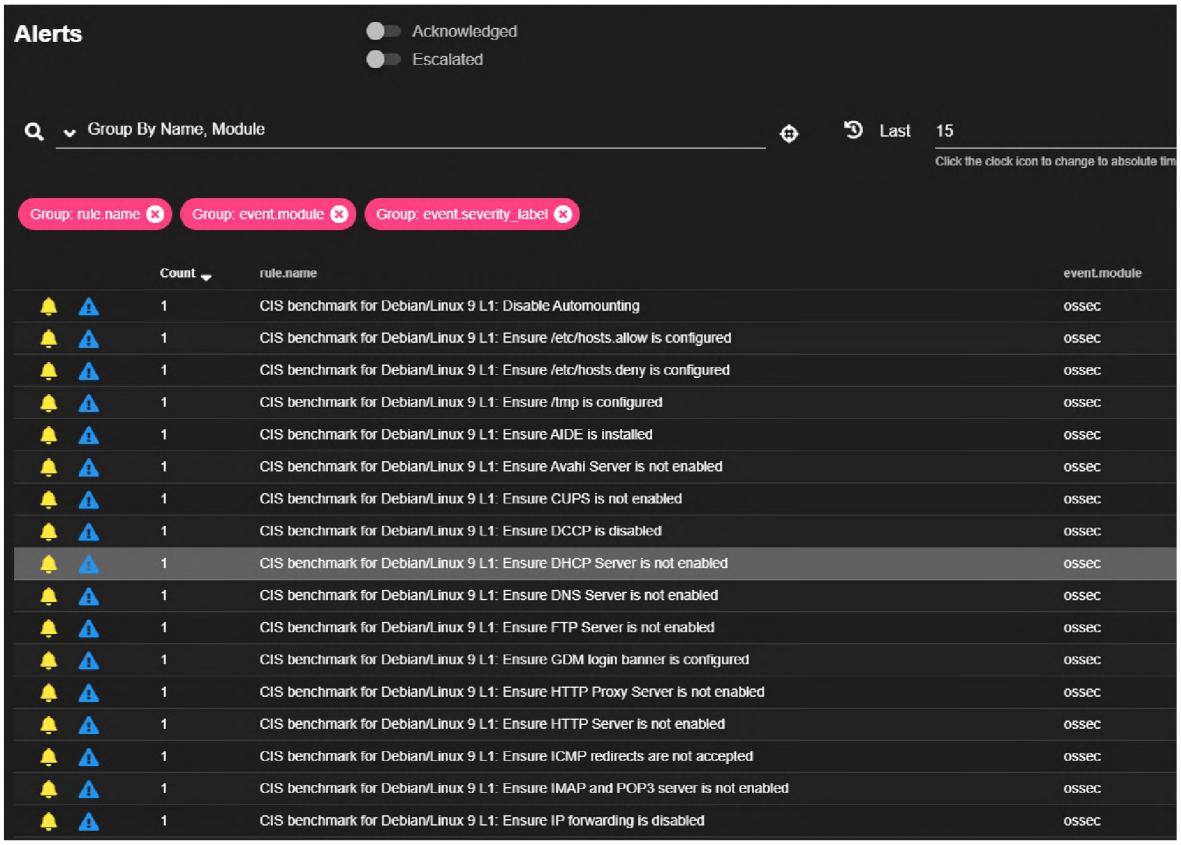


Рисунок 2.20 – реакція системи на тести безпеки

Призначенням компоненту репутації IP є ранжування IP-адресів в агенті Suricata, який відповідає за зберігання, збирання, оновлення та розповсюдження інформації про репутацію в IP-адресах. Було знайдено випробувальний список IP-адрес з низькою репутацією. Далі буде додавання цього списку до агенту, та його налаштування, для використання списку IPREP, щоб він попереджав, якщо відповідно до мережі будуть якісь дії цих IP адресів. Усіма службами керує SaltStack. Зміна конфігурації для suricata.yaml буде виконана в `/opt/so/saltstack/local/pillar/minions/oniin_eval.sls`. Для налаштування Suracata додається список IPREP до конфігурації:

```
suricata:
  config:
   reputation-categories-file: /etc/suricata/iprep/categorylist.txt
   default-reputation-path: /etc/suricata/iprep
   reputation-files:
```

```
    - sunburst.txt
    - testing.txt
```

Після чого створюємо файл конфігурації в SOS машині:

```
mkdir /opt/so/conf/suricata/iprep
cd /opt/so/conf/suricata/iprep
touch categorylist.txt
touch sunburst.txt
touch testing.txt
chown suricata: -R ./
categorylist.txt
1,sunburst,Known Sunburst IP
2,test,Testing IPREP

testing.txt
192.168.1.71,2,10
```

sunburst.txt: Використовується цей одношаровий вкладиш, щоб додати ідентифікатор категорії та оцінку репутації до списку ip-адрес:

curl https://raw.githubusercontent.com/bambenek/research/main/sunburst/ipv4-addresses.txt | sed 's/$/,1,10/' > sunburst.txt

Щоб додати правила IPREP відповідно документу потрібно ввести наступну команду: `/opt/so/saltstack/local/salt/idstools/local.rules.`

```
# Custom Suricata rules go in this file
alert ip any any -> any any (msg:"IPREP LOW - Sunburst"; iprep:src,sunburst,<,11; sid:1996611; rev:1;)
alert ip any any -> any any (msg:"IPREP LOW - Sunburst"; iprep:dst,sunburst,<,11; sid:1996612; rev:1;)
alert ip any any -> any any (msg:"IPREP HIGH - Testing"; iprep:src,test,<,11; sid:1996621; rev:1;)
alert ip any any -> any any (msg:"IPREP HIGH - Testing"; iprep:dst,test,<,11; sid:1996622; rev:1;)
```

IPREP приймає наступні чотири аргументи:

- перший аргумент для scr або dst;
- коротка назва категорії, яка була додана до categorylist.txt
- оператор, either>, or <, or =
- Останнє значення обчислюється оператором

Отже, вищезазначені правила викликатимуть попередження про будь-які ips у sunburst або test категорії, як src або dst, якщо ці IP адреси мали репутацію менше чим одинадцять одиниць. Хоча було збережено ці файли в SOS машині, жоден з них насправді не знаходиться в контейнері док-станції suricata. Для того, щоб потрапити туди, потрібно прив'язати раніше створені файли до контейнера suricata. Через це доведеться у розділі so-suricata знайти список binds та ввести наступну команду: `/opt/so/saltstack/default/salt/suricata/init.sls`. Вводимо наступні строки:

```
      -
/opt/so/conf/suricata/iprep/categorylist.txt:/etc/suricata/iprep/categorylist.txt:
ro
      -
/opt/so/conf/suricata/iprep/sunburst.txt:/etc/suricata/iprep/sunburst.txt:ro
      - /opt/so/conf/suricata/iprep/testing.txt:/etc/suricata/iprep/testing.txt:ro
```

Щоб впровадити зміни, було зроблено перезавантаження Suracata:

```
salt-call state.highstate; so-rule-update; salt onion_eval state.apply suricata;
so-suricata-restart
```

За для перевірки доцільності впровадження змін було запущено наступну команду: `docker exec so-suricata find /etc/suricata`.

Якщо все було зроблено правильно, то буде відображатися доданий IPREP каталог:

```
[root@onion iprep]# docker exec so-suricata find /etc/suricata
/etc/suricata
/etc/suricata/classification.config
/etc/suricata/reference.config
/etc/suricata/suricata.yaml
/etc/suricata/threshold.config
/etc/suricata/threshold.conf
/etc/suricata/bpf
/etc/suricata/rules
/etc/suricata/rules/all.rules
/etc/suricata/rules/local.rules
/etc/suricata/iprep
/etc/suricata/iprep/categorylist.txt
/etc/suricata/iprep/testing.txt
/etc/suricata/iprep/sunburst.txt
```

Перевірка коректності роботи відбувалась між двома хостами мережі, один, який був доданий до списку iprep від sunburst, а інший - до перевіряючого списку iprep. На наступному зображенні ілюстрована сторінка сповіщень:

	Count	rule.name	event.module
	6	IPREP LOW - Sunburst	suricata
	2	IPREP HIGH - Testing	suricata
	1	GPL ICMP_INFO PING *NIX	suricata

Рисунок 2.21 - сторінка сповіщень Suricata.

Існують такі бази даних Threat Intel, як CINS Score, які використовують свої ресурси для розробки ip-списків поганих користувачів та публікації їх безкоштовно. Тож рекомендується додати більше списків репутації та попереджень, як це було зроблено вище, щоб підвисити захист мережі.

2.13 Робота системи виявлення аномального стану

За тридцять днів роботи системи було захоплено 221 Гігобайт пакетів циркулюючих в мережі бібліотеки, для можливої кіберкріміналістичної експертизи. Було виявлено майже чотириста тисяч аномальних подій. Більш детально зображено на рисунку (2.22).

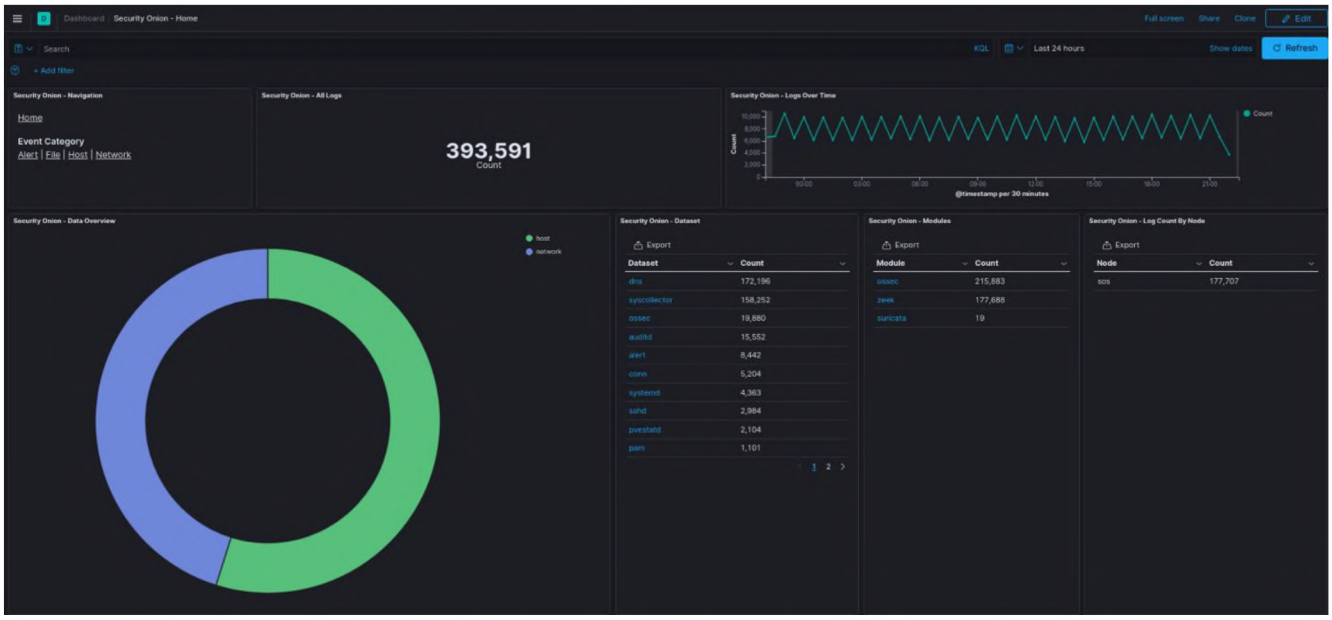


Рисунок 2.22 - сторінка сповіщень Kibana.

З загальної кількості сповіщень до попереджень відноситься 8500. (2.23)

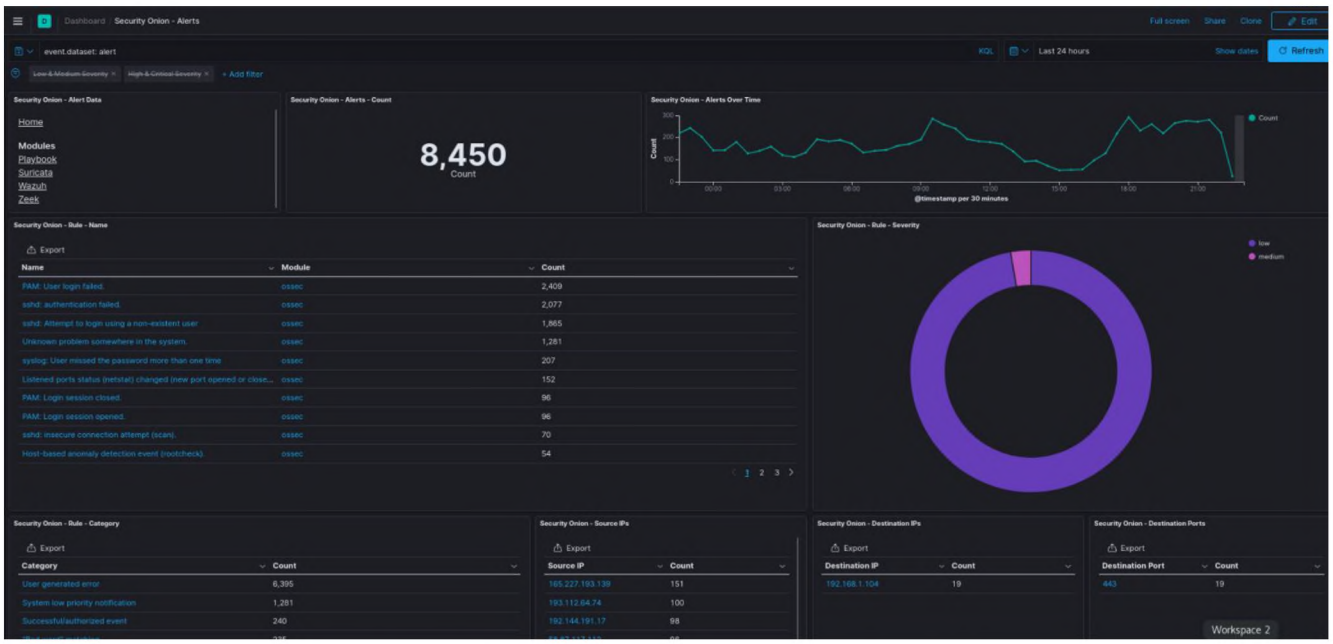


Рисунок 2.23 - сторінка попереджень Kibana.

З загальної кількості сповіщень до сповіщень хостів відноситься понад 215 тисяч.

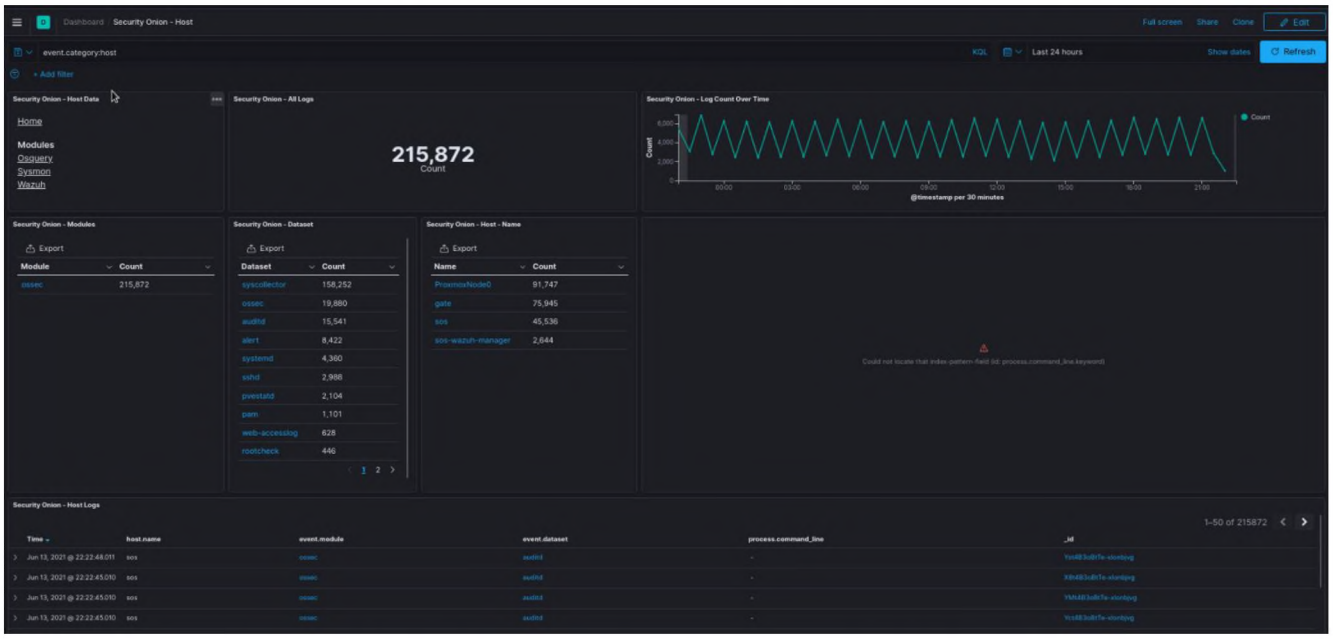


Рисунок 2.24 - сторінка сповіщень хостів в Kibana.

З загальної кількості сповіщень до сповіщень мережі відноситься понад 177 тисяч. (2.25)

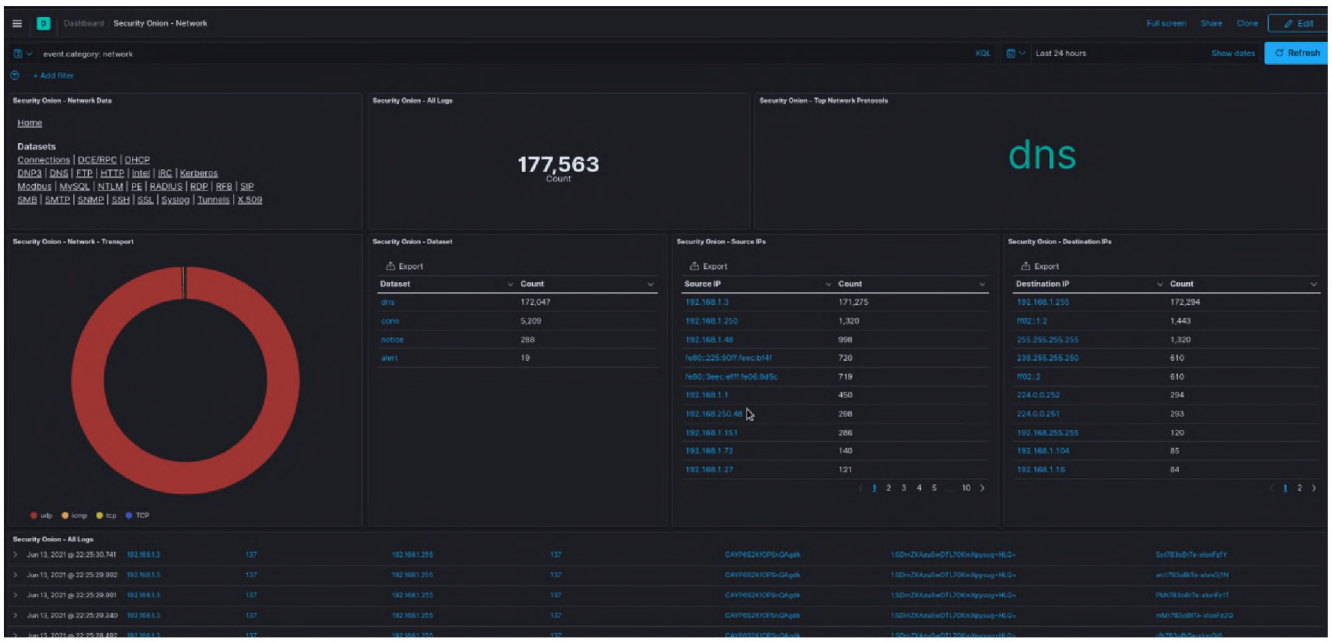


Рисунок 2.25 - сторінка сповіщень мережі в Kibana.

В процесі експлуатації системи виявлення аномалій було виявлено атаки типу підбору паролей, далі приведені рисунки з працюючої системою та реальними загрозами.

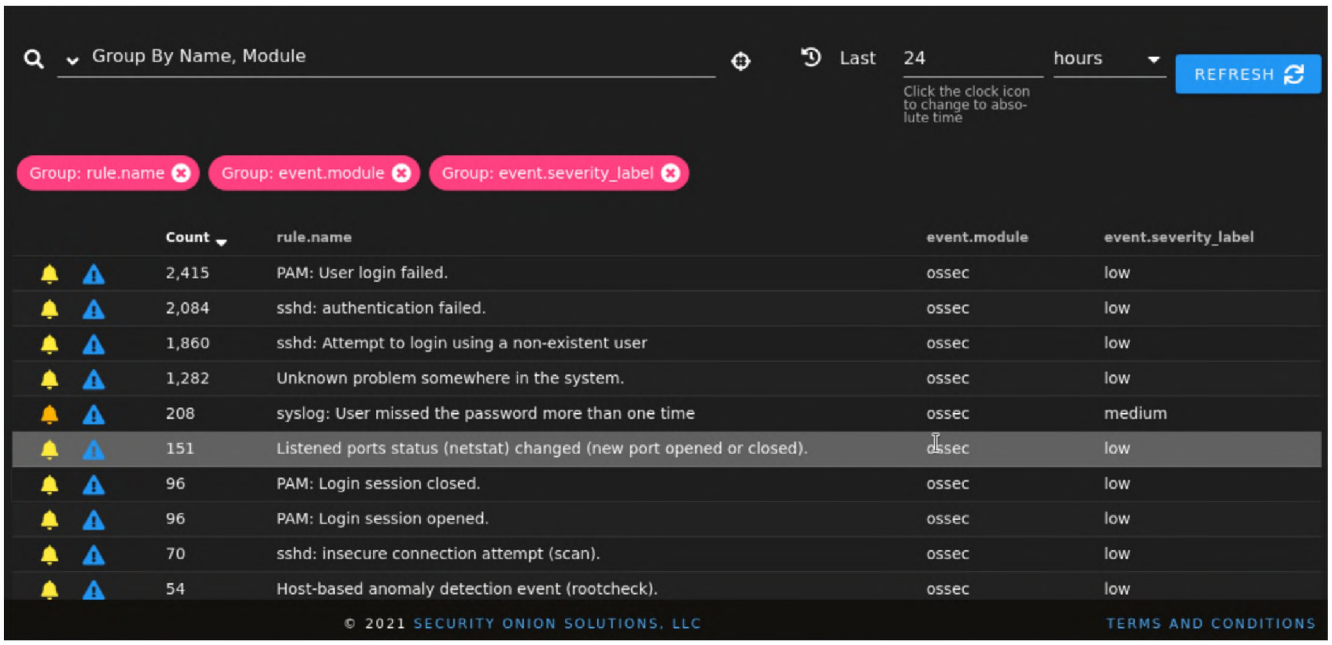


Рисунок 2.25 – загальний екран попереджень SOS.

Для аналізу попередження скористуємося функцією Hunt. В результаті опрацювання ми отримали графік розподілу попереджень за останні 24 години (2.26) та 30 днів (2.27).

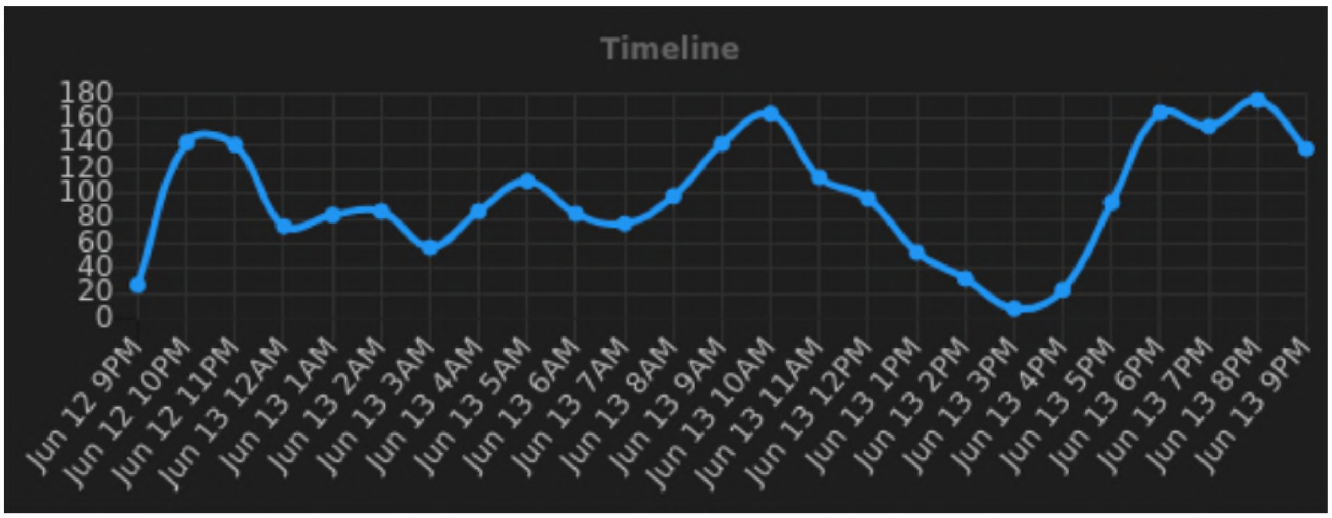


Рисунок 2.26 – графік розподілу попереджень за останні 24 години.

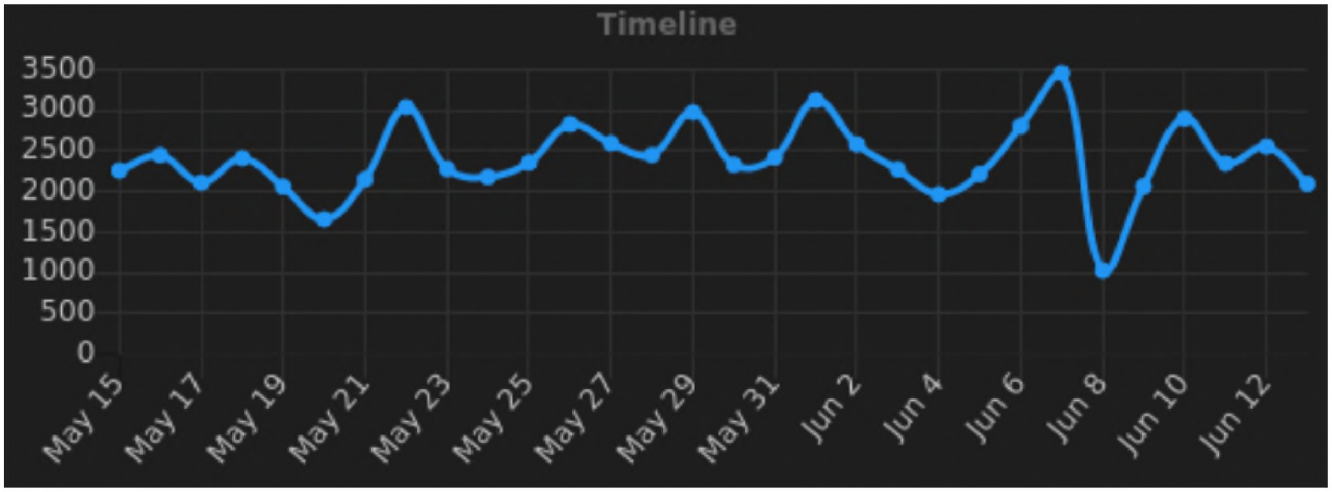


Рисунок 2.27 – графік розподілу попереджень за останні 30 днів.

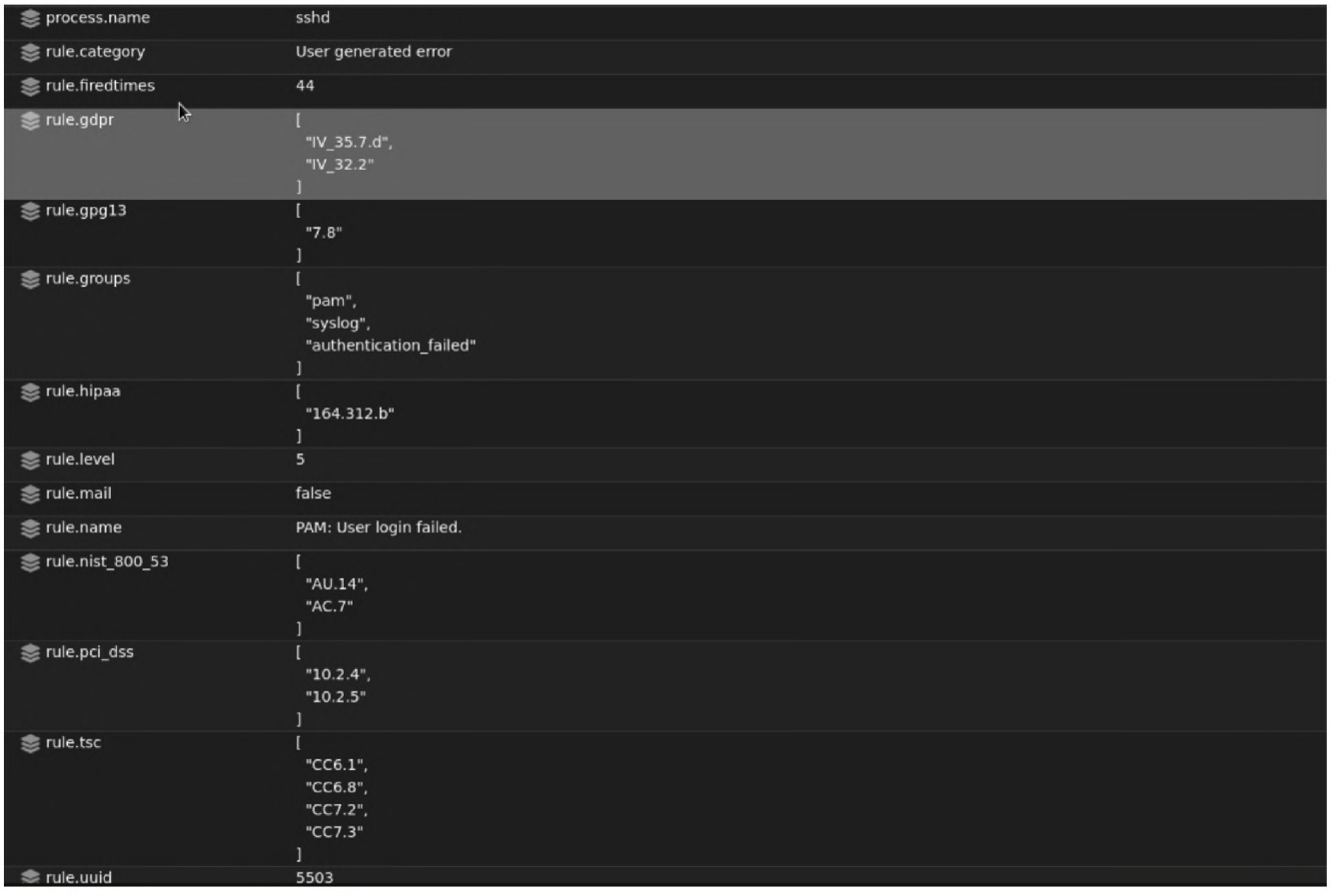
В результаті аналізу було отримано таблицю подій у часі (2.28), що відносяться до попереджень.

	Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.level	rule.category	process.name	user.name
›	2021-06-13 12:24:38.600 +00:00	81.71.47.65				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:20:08.539 +00:00	68.183.120.6				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:18:11.508 +00:00	181.30.129.31				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:16:55.487 +00:00	124.160.96.249				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:13:21.697 +00:00	81.71.47.65				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:11:07.662 +00:00	81.71.47.65				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:03:03.500 +00:00	106.55.37.174				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:01:57.484 +00:00	116.125.140.83				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:01:39.476 +00:00	181.30.129.31				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 12:01:04.465 +00:00	81.71.47.65				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 11:59:25.421 +00:00	106.55.37.174				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 11:58:54.406 +00:00	81.71.47.65				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 11:49:00.874 +00:00	116.125.140.83				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 11:48:23.861 +00:00	81.71.47.65				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 11:46:19.820 +00:00	81.71.47.65				PAM: User login failed.	5	User generated error	sshd	
›	2021-06-13 11:38:28.644 +00:00	42.193.96.159				PAM: User login failed.	5	User generated error	sshd	

Рисунок 2.28 – таблиця подій у часі.

При аналізі відповідних подій ми отримали інформацію про субєкт (ip-адреса) від дій якого сталося подія (2.29).

а)



б)

в)

Рисунок 2.29 – інформація про субєкт попередження

Також в результаті аналізу подій були отримані графіки розподілу в часі ресурсів в різноманітних метріках (2.30).

Рисунок 2.30 – сторінка Grafana графіків використання ресурсів сервісом SOS

2.14 Висновки до другого розділу

У другому розділі було розглянуто відомості про ОІД, проведено обстеження, розроблена модель порушника, загроз, обрано систему виявлення

аномального стану для реалізації, встановлено систему, проведено іспит, та аналіз її роботи.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Техніко-економічне обґрунтування дипломного проекту

Метою виконання економічного розділу є доведення доцільності впровадження запропонованої системи моніторингу відповідно до затрачених коштів.

Необхідність розробки полягає через великий вплив науково-технічної бібліотеки на працездатність навчального процесу вищого навчального закладу, оскільки при критичних атаках система може відмовити, та саме через це призупиниться не тільки робота бібліотеки, а і більшість навчальних процесів.

3.2 Визначення трудомісткості розробки політики безпеки

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}\ , \text{годин} \quad (3.1)$$

Де ttз – тривалість складання технічного завдання на розробку політики безпеки інформації; (становить 8 годин)

tв – тривалість розробки концепції безпеки інформації у організації; (становить 10 годин)

ta – тривалість процесу аналізу ризиків; (становить 4 години)

tвз – тривалість визначення вимог до заходів, методів та засобів захисту; (становить 4 години)

tозб – тривалість вибору основних рішень з забезпечення безпеки інформації; (становить 4 години)

tов – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації; (становить 12 годин)

tд – тривалість документального оформлення політики безпеки; (становить 5 годин)

Згідно формули (3.1) та наведених даних:

$$t = 8+10+4+4+4+12+5= 47 \text{ год.} \quad (3.1)$$

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч:

$$K_{рп}=З_{зп}+З_{мч}. \quad (3.2)$$

$$Крп = 7567 + 1873.89 = 9440.89 \text{ грн.} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$З_{зп} = t \times З_{іб}, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість розробки політики безпеки , годин; (становить 47 годин)

Зіб – середньо годинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину. (становить 161 грн.)

$$Ззп = 47 * 161 = 7567 \text{ грн.} \quad (3.3)$$

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t \times C_{мч}, \text{ грн,} \quad (3.4)$$

$$Змч = 47 * 39.87 = 1873.89 \quad (3.4)$$

де t – трудомісткість розробки політики безпеки інформації на ПК, годин; (становить 47 годин)

Смч – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \times t_{нал} \times C_e + \frac{Ф_{зал} \times H_a}{F_p} + \frac{K_{лпз} \times H_{апз}}{F_p}, \text{ грн,} \quad (3.5)$$

Де Р – встановлена потужність ПК, кВт; (становить 0.8)

tнал – кількість задіяних машин для розробки; (становить 1)

Се – тариф на електричну енергію, грн/кВт година; (становить 1.68)

Фзал – залишкова вартість ПК на поточний рік, грн.; (становить 140000)

На – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці; (становить 0.5)

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частка одиниці; (становить 0.4)

Клпз – вартість ліцензійного програмного забезпечення, грн.; (становить 1 гривню)

Fр – річний фонд робочого часу (становить 1920);

Смч= 0.8*1*1.68+((140000*0.5)/1920)+((1*0.4)/1920)= 39.87 грн. (3.5)

3.3 Розрахунок (капітальних) фінансових витрат

Капітальні витрати розраховуються за наступною формулою

$$K=K_{пр}+K_{зпз}+K_{пз}+K_{аз}+K_{навч}+K_{н}\ , \quad (3.6)$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультанті, тис. грн; (оскільки установа має своїх спеціалістів, цей показник не враховується)

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн; (оскільки все необхідне обладнання вже є у установи для реалізації, а додаткове ПЗ безкоштовне, цей показник не враховується)

Крп – вартість розробки політики безпеки інформації, тис. грн; (становить 9440.89 грн.)

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн; (становить 0 грн.)

Кнавч – витрати на навчання фахівців і обслуговуючого персоналу, тис. грн; (становить 0 грн.)

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. (становить 0)

$$К = 9440.89 \text{ грн} . \quad (3.6)$$

3.4 Розрахунок поточних (експлуатаційних) витрат

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки розраховуються за наступною формулою

$$C=C_{в}+C_{к}+C_{ак}\ , \text{ тис. грн.} \quad (3.7)$$

Де Св – витрати на оновлення системи; (становить 0)

Ск – витрати на керування системою, формула (3.8)

Сак – витрати викликані активністю користувачів системи; (становить0)

Витрати на керування системою розраховуються за наступною формулою

$$C_к = C_н + C_а + C_з + C_{єв} + C_{ел} + C_о + C_{тос}, \text{ грн.} \quad (3.8)$$

де Сн - витрати на навчання адміністративного персоналу; (становить 0)

Са - річний фонд амортизаційних відрахувань (становить 70000 грн.)

Сз - річний фонд заробітної плати інженерно-технічного персоналу, розраховується за наступною формулою:

$$C_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.9)$$

де Зосн – основна заробітна плата відповідно грн. на рік; (становить 60000 грн.)

Зосн = 5000 * 12 = 60000 грн.

Здод – додаткова заробітна плата відповідно грн. на рік; (становить 600 грн.)

Сз = 60000+6000 = 66000, грн. (3.9)

Сєв – (становить 14520 грн.)

Сєв =66000*22% = 14520

Сел – вартість електроенергії; (становить 1 кВт.)

Со – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування; (становить 0 грн., тому що на уряді є кваліфіковані працівники)

Стос - витрати на технічне й організаційне адміністрування та сервіс. (становить 0)

Ск = 70000+66000+14520+1= 150521 грн. (3.8)

С =0+150521+0 = 150521 грн. (3.7)

3.5 Оцінка величини збитку

Для розрахунку вартості величини збитку було застосовано наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки; (становить 4години)

tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу; (становить 4годин)

tви – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі; (становить 1година)

Зо – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць; (становить 5000 грн.)

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць; (становить 5000 грн.)

Чо – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб;(становить 1 особу)

Чс – чисельність співробітників атакованого вузла або сегмента мережі, осіб; (становить 20 осіб)

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік; (становить 0)

Пзч – вартість заміни встаткування або запасних частин, грн;(становить 5000 грн)

І – число атакованих вузлів або сегментів корпоративної мережі; (становить 8: репозиторій, сайт бібліотеки, сховище, архів документів в публічному доступі, електронний каталог, хмарний сервіс, ресурс для обробки документів, поточний медіа сервіс.)

N – середнє число атак на рік; (становить 20)

За наступною формулою було розраховано упущену вигоду:

$$U = П_п + П_в + V \ , \quad (3.10)$$

$$U = 2273 + 5682 + 0 = 7955 \quad (3.10)$$

Де Пп - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн, розраховуються за наступною формулою:

$$П_п = \frac{\Sigma З_с}{F} \times t_п \ , \quad (3.11)$$

$$Пп = (100000 / 176) * 4 = 2273 \quad (3.11)$$

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн, розраховується за наступною формулою:

$$П_в = П_{ви} + П_{пв} + П_{зч}\ , \quad (3.12)$$

$$Пв = 568+114+5000 = 5682 \quad (3.12)$$

V – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн, розраховуються за наступною формулою:

$$V = \frac{O}{Fг} \times (t_п + t_в + t_{ви})\ , \quad (3.13)$$

$$V = (0/2080)*(4+4+1) = 0 \quad (3.13)$$

Підрахувавши показник упущеної вигоди, розраховується показник збитку від атаки за наступною формулою:

$$B = \sum_i \times \sum_п \times U\ . \quad (3.14)$$

$$В=8*20*7955=1,272,800 \text{ грн.} \quad (3.14)$$

Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \times R - C\ , \quad (3.15)$$

Де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці - 0,25;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E=1,272,800*0.25-150521=167679 \quad (3.15)$$

3.6 Аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Коефіцієнт розраховується за наступною формулою:

$$ROSI = \frac{E}{K}$$, частка одиниці, (3.16)

Де Е – загальний ефект від впровадження системи;

К – Капітальні затрати.

ROSI = 167679 / 9441 = 17.76 (3.16)

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки. Коефіцієнт розраховується за наступною формулою:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}$$, років. (3.17)

To = 1 / 17 = 0.06 (3.17)

3.7 Висновки до третього розділу

У третьому розділі були проведені розрахунки та аналіз доцільності впровадження системи. Остаточні рішення розрахунки довели, що реалізація системи є доцільною оскільки при одноразовому вкладі коштів на суму 9441 гривня, було отримано коефіцієнт окупності рівний 17,76 (ROSI), завдяки цим даним унаслідок чого було підраховано термін тривалості окупності який дорівнює 0.06 одиниць та реалізує окупність впровадженої системи за місяць.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було проаналізовано сучасний рівень загроз інформаційних мереж від кібератак. Проаналізовано нормативно-правову базу відповідно до створення захисту інформації.

Було проведено обстеження науково-технічної бібліотеки НТУ “Дніпровська Політехніка” для виявлення слабких місць інформаційної мері. На базі обстеження було розроблено модель порушника, проаналізовано існуючі та потенційні загрози. Було проведено аналіз систем виявлення аномально стану мережі для подальшої реалізації.

Як результат було вибрано найбільш відповідну систему до певних вимог, та налаштовано для подальшої експлуатації та проведення подальших випробувань вже з реальними загрозами.

По завершенню проведень випробувань були проведені розрахунки що до доцільності впровадження системи виявлення аномального стану мережі. Було доведено, що впровадження є економічно вигідним для науково-технічної бібліотеки.

На підставі виконаної кваліфікаційної роботи було прийнято рішення, що до подальшого використовування системи виявлення аномального стану для науково-технічної бібліотеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12
2. Закон України «Про захист інформації в автоматизованих системах». URL: https://zakon.rada.gov.ua/laws/show/2594-15
3. Закон України «Про науково-технічну інформацію». URL: https://zakon.rada.gov.ua/laws/show/3322-12
4. Закон України «Про бібліотеки і бібліотечну справу». URL: https://zakon.rada.gov.ua/laws/show/32/95-%D0%B2%D1%80
5. ПКМУ № 611 «Про перелік відомостей, що не становлять комерційну таємницю». URL: https://zakon.rada.gov.ua/laws/show/611-93-%D0%BF
6. ПКМУ № 1126 « Про затвердження концепції технічного захисту інформації в Україні». URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF
7. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення». URL: https://tzi.com.ua/dstu-3396.0
8. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». URL: https://tzi.com.ua/dstu-3396.1-96
9. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу». URL: https://tzi.com.ua/nd-tz-1.1-002-99
11. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». URL: https://tzi.com.ua/nd-tz-1.4-001-2000
12. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». URL: https://tzi.ua/ua/nd_tz_2.5-004-99
13. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». URL: https://tzi.ua/ua/nd_tz_2.5-005-99
14. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання по створенню комплексної системи захисту інформації в автоматизованій системі». URL: https://tzi.ua/ua/nd_tz_3.7-001-99
15. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт по створенню комплексної системи захисту інформації в інформаційних телекомунікаційних системах». URL: https://tzi.ua/ua/nd_tz_3.7-003_-2005
16. Сайт науково-технічної бібліотеки НТУ “Дніпровська Політехніка”. URL: lib.nmu.org.ua
17. Вибір системи до впровадження. URL: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

18. Вибір системи до впровадження. URL: https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/
18. Вимоги до обладнання. URL:
https://docs.securityonion.net/en/2.3/hardware.html
19. Посилання до скрипта на доцільність відправки попереджень. URL: https://github.com/0xtf/testmynids.org
20. Встановлення агенту Osquery. URL: https://sos.nmu.org.ua/#/downloads

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	4	
6	А4	Спеціальна частина	52	
7	А4	Економічний розділ	6	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А.	1	
11	А4	Додаток Б.	1	
12	А4	Додаток В.	1	
13	А4	Додаток Г.	1	

ДОДАТОК Б. Перелік матеріалів на оптичному носії

1 Кваліфікаційна робота - Kiiko.R.Y 125 17 1.docx

2 Презентація до кваліфікаційної роботи - Kiiko.R.Y 125 17 1.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 125-17-1

Кійко Ростислава Євгеновича.

на тему: Підсистема виявлення аномального стану інформаційної системи бібліотеки НТУ “Дніпровська Політехніка”

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 79 сторінках та містить 30 рисунків, 11 таблиць, 20 джерел та 4 додатка.

Об'єкт розробки: науково-технічна бібліотека НТУ “Дніпровська Політехніка”

Мета роботи: підвищення захищеності інформаційної системи бібліотеки НТУ "Дніпровська Політехніка" через контроль її стану.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності бакалавра спеціальності 125 “Кібербезпека”. Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази в сфері забезпечення інформаційної безпеки, обстеження об’єкту інформаційної діяльності, вибір та налаштування системи виявлення аномального стану, робота в мережі з існуючими загрозами.

Практичне значення результатів кваліфікаційної роботи полягає у мінімізація успішних атак зловмисниками, за рахунок впровадження системи виявлення аномального стану мережі.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Кійко Р.Є проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма “Кібербезпека”.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

Кваліфікаційна робота заслуговує оцінки _____

Керівник кваліфікаційної роботи

Керівник спец. Розділу