МАГІСТЕРСЬКА РОБОТА

15.04 – МР. 1859 “С” 2021.П1.01.015 ПЗ

РЕШЕТНІКОВА ДАНИЇЛА ЮРІЙОВИЧА

2022 р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.056.57

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	Завідувач кафедри
Інформаційних технологій	Комп'ютерних систем і мереж
_____ / Глазунова О.Г., д.п.н, проф. /	_____ / Касаткін Д.Ю., к.п.н., доцент. /
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___» _____ 2022 р.	«___» _____ 2022 р.

МАГІСТЕРСЬКА РОБОТА

На тему: «Методи розпізнавання загроз та захист інформації в навчальному закладі»

Спеціальність: 123 «Комп’ютерна інженерія»

Освітня програма: Комп’ютерні системи та мережі

Керівник дипломного проекту: _____ / Лахно В.А. /
підпис ПІБ

Виконав: _____ / Решетніков Д.Ю. /
підпис ПІБ

КИЇВ-2022

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____ / Касаткін Д.Ю., к.п.н., доцент. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 2022 р.

ЗАВДАННЯ
ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Решетнікову Даниїлу Юрійовичу
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): 123 «Комп'ютерна інженерія»
Освітня програма: комп'ютерні системи та мережі

Тема магістерської роботи: «Методи розпізнавання загроз та захист інформації в навчальному закладі»
затверджена наказом ректора НУБіП України від "1" листопада 2021 № 1859 "С"
Термін подання завершеної роботи на кафедру _____
Вихідні дані до магістерської роботи: сервер зі встановленим програмним забезпеченням VmWare Workstation та Proxmox VE, система IPS з відкритим кодом «Suricata», платформа Splunk, маршрутизатор Asus RT-51U

Перелік питань, що підлягають дослідженню:
1. Аналіз предметної області для дослідження методів захисту інформації у навчальному закладі
2. Проектування системи захисту інформації
3. Побудова моделі захищеної мережі навчального закладу

Дата видачі завдання "1" листопада 2021 р.

Керівник магістерської роботи _____ / Лахно В.А. д.т.н., професор /
(підпис) (ПІБ, вчене звання і ступінь)

Завдання прийняв до виконання _____ / Решетніков Д.Ю. /
(підпис) (ПІБ)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі магістерської роботи		Виконано
2	Аналіз предметної області		Виконано
3	Проектування системи		Виконано
4	Реалізація системи		Виконано
5	Тестування розробленої системи		Виконано
6	Оформлення пояснювальної записки		Виконано
7	Оформлення графічного матеріалу		Виконано

Студент _____ / Решетніков Д.Ю. /
підпис ПІБ

Керівник проекту (роботи) _____ / Дахно В.А. /
підпис ПІБ

РЕФЕРАТ

Пояснювальна записка: 97с., 95 рис., 4 додатка, 42 використаних джерела.

МЕРЕЖА, НАВЧАЛЬНИЙ ЗАКЛАД, БЕЗПЕКА, ІНФОРМАЦІЯ, РОЗПІЗНАВАННЯ ЗАГРОЗ, PROXMOX, SURICATA, PI-HOLE, SPLUNK, XRDP, EVE-NG, СПИСКИ ДОСТУПУ

Мета роботи – створення моделі мережі навчального закладу, що включає в себе розгортання серверів та користувацьких віртуальних машин на них, налаштування можливості віддаленого доступу до них, налаштування емульованих мережевих пристроїв, створення та впровадження в роботу фільтру DNS-адрес та системи розпізнавання вторгнень.

Об’єкт – модель мережі з впровадженим захистом інформації.

Предмет – програмні додатки з відкритим кодом для виявлення кіберзагроз.

Робота складається з трьох розділів.

У першому розділі проведений аналіз предметної області, розглянуті тенденції кібербезпеки та вплив війни в Україні на це.

У другому розділі розглянуто методи захисту інформації, стандарти проектування захищених мереж.

У третьому розділі детально описаний процес створення та налаштування моделі мережі навчального закладу та розгортання систем захисту інформації в її межах.

В результаті виконання магістерської роботи проведено аналіз, дослідження та моделювання розроблюваної моделі захищеної мережі навчального закладу та розроблені рекомендації щодо її впровадження.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IRP — Платформа реагування на інциденти, Incident Response Platform

IaaS — Інфраструктура як послуга Infrastructure as a Service

PaaS — Платформа як послуга Platform as a Service

SaaS — Програмне забезпечення як послуга, Software as a Service

CNaaS — Хмарна мережа як послуга, Cloud Network as a Service

VPNaaS — VPN як послуга, VPN as a Service

FWaaS — Брандмауер як послуга, Firewall as a Service

VPN — Віртуальна приватна мережа, Virtual Private Network

MDR — Кероване виявлення і реагування, Managed Detection and Response

MSSP — Керовані постачальники послуг безпеки

ПЗ — Програмне забезпечення

ВМ — Віртуальна машина

ОС — Операційна система

PVE — Система віртуалізації Proxmox Virtual Environment

DNS — Служба доменних імен, Domain Name System

DRS — Системи балансування навантаження між фізичними серверами, Distributed Resource Scheduler

Wi-Fi — Технологія локальної бездротової мережі

NCPI — Індекс кіберсили держав світу, National Cyber Power Index

DHCP — Протокол динамічної конфігурації вузла, Dynamic Host Configuration Protocol

RAID — Надмірний масив незалежних дисків, Redundant Array of Independent Disks

IEEE — Інститут інженерів з електротехніки та електроніки, Institute of Electrical and Electronics Engineers

DDoS — Розподілена атака на відмову в обслуговуванні, Distributed Denial of Service

ARP — Протокол визначення адреси, Address Resolution Protocol

HDD — Жорсткий диск, Hard Disk Drive

WEB — Система доступу до пов'язаних між собою документів на різних комп'ютерах, підключених до Інтернету.

VLAN — Віртуальна локальна мережа, Virtual Local Area Network

SSD — Твердотілий накопичувач, Solid-state drive

PCIe — комп'ютерна шина передачі даних, PCI Express

CNAPP — Платформи захисту хмарних додатків, Cloud Native Application Protection Platforms

CSNS — Хмарна служба безпеки мережі, Cloud Service Network Security

CSPM — Управління безпекою хмарних ресурсів, Cloud Security Posture Management

CWPP — Платформа захисту хмарних робочих навантажень, Cloud Workload Protection Platform

UPS — Джерело безперебійного живлення, Uninterruptible Power Supply

IOT — Інтернет речей, пристрої що під’єднуються до мережі Інтернет, Internet of Things

TCO — Сукупна вартість усіх витрат на володіння, Total Cost of Ownership

OSI — Мережева модель взаємодії відкритих системThe Open Systems Interconnection model

ВСТУП

Тема захисту інформації завжди була важливою, коли справа стосувалася державних таємниць, бізнесу, та приватних секретів. Ще в роки Римської імперії секретні військові накази імператорів шифрувалися задля безпеки військ, що могли потрапити у пастку при розкритті інформації в наказі. З моменту створення та розвитку електронно-обчислювальної техніки безпека інформації набула нового відтінку – тепер слід було винайти механізми шифрування електронних даних. Паралельно з розвитком мікропроцесорів розвивалися і алгоритми шифрування, політики безпеки компаній та правові основи кібербезпеки. Створювались та впроваджувались плани реагування на інциденти (IRP), щоб IT-команди знали, як реагувати, коли трапляється порушення безпеки.

Для України питання захисту інформації особливо гостро постало у 2014 році через події анексії Криму військами російської федерації та початку бойових дій у Луганській та Донецькій областях. Починаючи з цього часу наша держава постійно атакується як фізично, так і в цифровому просторі. За останні 8 років загалом кількість кібератак на державні ресурси України та приватні компанії, зареєстровані в Україні зросла більш ніж у 35 разів. Починаючи з 24 лютого 2022 року – повномасштабного вторгнення рф на терени України важливість серйозного та комплексного підходу до питань кіберзахисту лише вчергове показало свою важливість. Безпека інформації - одна з невід’ємних складових перемоги та розбудови сильної, захищеної та процвітаючої Української держави, і безпека інформації в навчальному закладі – один з її аспектів, оскільки ступінь захищеності мережі навчального закладу безпосередньо впливає на якість навчального процесу, що в свою чергу має вплив на загальний рівень освіти та культури суспільства. Як показує статистика, бідні країни з низьким рівнем життя мають і низький рівень освіченості суспільства, в той час як розвинуті країни мають високий рівень розвитку системи освіти та широкі можливості для навчання.

Таким чином, економічний та освітній рівні держави тісно пов’язані між собою, і позитивно впливаючи на один з них можна позитивно вплинути на інший аспект життя суспільства.

Тема захисту інформації у навчальному закладі також актуальна тому що говорячи про молодшу суспільну групу – дітей та підлітків варто зазначити, що це ті, хто найчастіше завантажує собі нові додатки на смартфони та ноутбуки/персональні комп’ютери. Частіше за все цими додатками є ігри, що далеко не завжди проходять перевірку в онлайн-магазинах додатків, не кажучи вже про ті, які завантажуються з інтернету/торентів та ін. Встановлений такий додаток потенційно несе загрозу та може бути розповсюджений через локальну мережу. В навчальних закладах зазвичай слабкий рівень безпекових налаштувань, через що мережі шкіл та університетів можуть бути одним з місць розповсюдження вірусів.

В даній дипломній роботі стоїть задача засобами віртуалізації змоделювати мережу навчального закладу та створити систему захисту, що допомогла б вирішити дані проблеми та при цьому не вимагала великих вкладень, через часто недостатній рівень інвестування державою ресурсів у навчальні заклади. Ідеальними для цього є системи з відкритим кодом, які не вимагають вкладень та часто мають широку підтримку від користувачів, що значно спрощує впровадження таких систем на практиці.

1 АНАЛІТИЧНИЙ ОГЛЯД

1.1 Напрями розвитку кібербезпеки у 2021-2022 роках

Ландшафт кіберзагроз та методи кібербезпеки доволі швидко змінюються, і це стало ще більш очевидно з початком пандемії COVID-19, особливо в корпоративних бізнес-операціях та IT-архітектурі компаній. Зловмисники почали активно користуватися цими змінами, спрямовуючи свої атаки на вразливі місця у сфері віддаленого доступу, хмарних обчислень та інших рішень, прийнятих в межах нових політик безпеки. Зростають також і такі загрози, як багатовекторні атаки,зараження вірусами-вимагачами комп'ютерів кінцевих користувачів, атаки на ланцюги поставок. А складні атаки, такі як використання вразливості Log4j, впливають на мільйони компаній, в тому числі Amazon, Tesla і Cisco. Вище наведені приклади еволюції ландшафту кіберзагроз мають значний вплив на тенденції розвитку кібербезпеки, оскільки організації мусять адаптуватися до новітніх загроз. Деякі з провідних загроз кібербезпеки 2022 року подані нижче.

Програми-вимагачі стали однією з найпоширеніших і найпомітніших загроз кібербезпеки останніх років. За даними Cybersecurity Ventures, прогнозується, що збитки від програм-вимагачів складуть 11,5 мільярдів доларів США. Поточний обсяг загрози призводить до появи нової жертви кожні 14 секунд. Реалізація полягає у зараженні комп'ютера жертви шкідливим програмним забезпеченням, що призначене для шифрування файлів у системі та вимагання викупу в обмін на ключ дешифрування, необхідний для відновлення доступу до цих файлів. В останні роки загроза вірусів-вимагачів зростає та еволюціонує, оскільки суб'єкти кіберзагроз вдосконалюють свої інструменти та методи. Сучасні атаки вимагачів є цілеспрямованими і вимагають багатомільйонні викупи. Ці атаки також еволюціонували і включають в себе різні способи вимагання, такі як крадіжка даних перед їх шифруванням і загроза розподіленої атаки на відмову в обслуговуванні (DDoS), щоб надати зловмиснику додаткові важелі впливу на жертву, щоб змусити її задовольнити вимогу викупу.

Фішинг та компрометація ділової електронної пошти залишаються найпопулярнішими низько-технологічними методами, які використовують кіберзлочинці для отримання доступу до мереж. Фішингові електронні листи виглядають як звичайні, щоденні електронні листи від компаній, керівників та довірених осіб. При переході за шкідливими посиланнями або наданні інформації на фальшивих цільових сторінках на пристрої завантажується шкідливе програмне забезпечення, що дозволяє кіберзлочинцям отримати доступ до критично важливих мереж. З широким розповсюдженням хмарних сервісів, таких як Gmail та Office 365, хакери стають все більш витонченими у своїх навичках самозванства та соціальної інженерії. Хмарні сервіси не можуть адекватно захистити ваші конфіденційні дані. Вжиття додаткових заходів безпеки електронної пошти з шифруванням та аналізом загроз - це розумний спосіб захистити співробітників від витончених атак електронною поштою [1].

До наступної категорії кіберзагроз, що набирають популярність, належать злами систем ланцюгів постачання. Так, злом SolarWinds у 2020 році був першим з багатьох таких нещодавніх атак. Часто для їх реалізації використовувались довірчі відносини, що існують між організаціями. Метод реалізації такої атаки полягає у наступному: кожна компанія має набір довірених клієнтів, постачальників та інших партнерів. Зловмисники використовують дані довірчі відносини, та завдяки наявному доступу до систем партнера, проводять атаку на IT-активи іншої організації або здійснюють фішингову атаку. За даними Ponemon Institute, 75% опитаних IT-фахівців визнали, що ризик проникнення через третю сторону є небезпечним і зростає. Зокрема, за даними Soha Systems, 63% всіх витоків даних можуть бути прямо або опосередковано пов'язані з доступом третіх осіб.

Злом SolarWinds та подібні атаки базувалися на тому, що всі компанії використовують у своїх мережах довірене стороннє програмне забезпечення. Шкідливий код, що вбудовувався в програмне забезпечення або оновлення наявного програмного забезпечення, був встановлений і запущений без додаткових перевірок автентичності, забезпечуючи внутрішній доступ до мережі організації.

Використання Інтернету речей (IoT) зростає з кожним днем (за даними Statista.com, очікується, що до кінця 2022 року кількість пристроїв, підключених до Інтернету речей, досягне майже 31 мільярда). IoT включає в себе все - роутери, веб-камери, побутову техніку, смарт-годинники, медичні прилади, виробниче обладнання, автомобілі і навіть системи домашньої безпеки. Більше підключених пристроїв означає більший ризик. Потрапивши під контроль хакерів, пристрої Інтернету речей можуть бути використані для перевантаження мереж, отримання доступу до конфіденційних даних або блокування важливого обладнання з метою отримання фінансової вигоди.

Все частіше суб'єкти кіберзагроз вдаються до багатовекторних атак. Ще десятиріччя назад програми-вимагачі були зосереджені виключно на шифруванні даних, а тепер включають в себе крадіжку даних, DDoS та інші загрози. Основним викликом у проведенні більшості кібератак є отримання доступу до цінних даних організації.

Наведені приклади атак на IT-ресурси компаній мають вплив на визначення трендів у протидії інформаційним загрозам. Нижче представлені деякі з них.

1.1.1. Консолідація безпеки

Історично склалося так, що архітектура корпоративної безпеки будувалася з численних автономних рішень, призначених для усунення конкретних ризиків безпеки. В результаті такого підходу є складна, роз'єднана архітектура безпеки, в якій аналітики перевантажені сповіщеннями з різних систем і не можуть ефективно контролювати і управляти безліччю рішень і інформаційних панелей. Крім того, складна архітектура може пропускати прогалини в безпеці та працювати неефективно через дублювання технологій безпеки.

Компанії, що помітили такі ризики в своїх мережах, починають рухатися в напрямку консолідації безпеки, розгортаючи платформи безпеки, створені одним постачальником. Ці об’єднані платформи безпеки пропонують простоту керування багатьма компонентами, поліпшену видимість, більшу ефективність і більш низьку

сукупну вартість володіння (TCO), ніж архітектура з розрізнених автономних рішень.

1.1.2. Mesh-архітектура

На жаль, не завжди можна захистити всю IT-систему компанії рішеннями від одного постачальника. Складність і прогалини в безпеці, створені архітектурою безпеки, надихнули Gartner визначити як один з головних стратегічних трендів 2022 року mesh-архітектуру кібербезпеки (CSMA). Метою CSMA є створення засобів для ефективної спільної роботи рішень безпеки від різних постачальників для досягнення певних цілей безпеки.

Для цього Gartner визначив чотири базові рівні CSMA, які описують ключові цілі безпеки, серед яких:

а) Консолідоване управління політикою і станом (Consolidated Policy and Posture Management)

б) Розподілена структура ідентичності (Distributed Identity Fabric)

в) Консолідовані інформаційні панелі

г) Аналітика та розвідка безпеки

Впроваджуючи рішення, сумісні з CSMA, організація може подолати проблеми, пов'язаних з архітектурами безпеки, що складаються з точкових рішень, і краще досягти основних цілей безпеки, коли неможливо обійтись рішенням від одного постачальника.

1.1.3. Безпека в першу чергу для розробників

Кількість нових виявлених вразливостей в програмному забезпеченні зростає з кожним роком. Одним з основних чинників цього є те, що основна увага приділяється створенню функціонального додатку та дотриманню термінів випуску, а питання безпеки часто вирішуються на етапі тестування життєвого циклу розробки програмного забезпечення (ЖЦРПЗ), якщо взагалі вирішуються.

Вразливе програмне забезпечення має численні негативні наслідки для його користувачів і виробника. Одним із шляхів вирішення даної проблеми є додавання

вимог безпеки до процесу планування, інтеграція сканування вразливостей та інші рішення для забезпечення безпеки в автоматизованих конвеєрах CI/CD. Таким чином, організації можуть зменшити вартість та вплив вразливостей безпеки з мінімальним впливом на терміни розробки та дати випуску.

1.1.4. Хмарна платформа захисту додатків

Впровадження хмарної інфраструктури створює нові виклики для безпеки організацій і робить необхідним розгортання хмарно-орієнтованих рішень для забезпечення безпеки. Ефективний захист хмарних середовищ вимагає рішень Cloud Service Network Security (CSNS), Cloud Security Posture Management (CSPM) і Cloud Workload Protection Platform (CWPP).

Платформи захисту хмарних додатків (CNAPP) об'єднують всі ці можливості хмарної безпеки в єдине хмарне рішення. Інтегруючи хмарну безпеку в єдине цілісне рішення, яке охоплює весь життєвий цикл додатків, організації можуть закрити прогалини в хмарній безпеці і видимості та спростити архітектуру хмарної безпеки.

1.1.5. Збільшення кількості послуг

Індустрія кібербезпеки стикається зі значним дефіцитом навичок, мільйони позицій залишаються незаповненими по всьому світу. Труднощі із залученням та утриманням кваліфікованого персоналу на критично важливих посадах призвели до того, що корпоративні служби безпеки часто недоукомплектовані та не мають ключових можливостей та навичок у сфері безпеки. В останні роки компанії все частіше використовують послуги як засіб вирішення проблеми нестачі кадрів. Кероване виявлення і реагування (MDR), керовані постачальники послуг безпеки (MSSP), хмарна мережа як послуга (CNaaS), VPN як послуга (VPNaaS) і брандмауер як послуга (FWaaS) є прикладами деяких з доступних послуг.

На додаток до усунення прогалин у навичках, ці керовані послуги пропонують організаціям інші переваги. Дані рішення професійно конфігуруються і управляються та можуть запропонувати більшу масштабованість і нижчу загальну

вартість володіння, ніж підтримка тих же можливостей ресурсами компанії. Крім того, керовані послуги часто дозволяють організаціям розгортати готову програму безпеки швидше, ніж це можливо зробити власними силами.

1.1.6. Доступ з найменшими привілеями

Надмірні привілеї є поширеною проблемою безпеки для організацій. Працівникам надаються дозволи на рівні адміністратора, коли вони не потрібні для їхньої ролі. Підрядники, постачальники та інші сторонні партнери мають законні потреби в доступі до певних корпоративних ресурсів, і їм надається необмежений доступ і потенційно привілейовані облікові записи. Такі надмірні дозволи сприяють виникненню та загостренню інцидентів безпеки та призвели до розробки моделі безпеки з нульовою довірою. Модель нульової довіри реалізує принцип найменших привілеїв, надаючи користувачеві, пристрою або додатку лише ті дозволи, які необхідні для виконання його ролі. Кожен запит на доступ оцінюється відповідно до цих обмежень доступу в кожному конкретному випадку. Таким чином отримується більша видимість того, як користувачі використовують їх мережу та ресурси, а також можливість виявляти та блокувати потенційні атаки та управляти їх впливом на організацію.

1.1.7. Гібридні центри обробки даних

Як локальна, так і хмарна інфраструктура пропонує значні переваги для організації. При локальному розгортанні організація має більший контроль над своїми даними та додатками. З іншого боку, хмарна інфраструктура пропонує більшу гнучкість і масштабованість. Гібридні центри обробки даних охоплюють локальну та хмарну інфраструктуру і дозволяють переміщувати дані та додатки між ними. Впровадження гібридних центрів обробки даних дозволяє організації повною мірою використовувати переваги як локального, так і хмарного середовищ та адаптуватися до потреб бізнесу. Однак для ефективного і безпечного впровадження гібридного центру обробки даних необхідна комплексна, послідовна видимість і безпека як в локальному, так і в хмарному середовищі [2].

1.2 Найпоширеніші загрози кібербезпеці у 2022 році

В останні роки загострення соціально-політичних заворушень призвели до різкого зростання кількості і тяжкості кіберзлочинів. Очевидним стає те, що чим далі, тим загрози безпеці стають більш витонченими, і відповідно, більш дорогими: експерти прогнозують, що глобальні витрати на кіберзлочинність досягнуть 10,5 трильйона доларів США до 2025 року, що у 3,5 разів більше, ніж у 2015 році. За даними IT Governance, через кібератаки та витоки даних за період з січня по квітень 2022 році було скомпрометовано більше 14,3 мільйона облікових записів користувачів. Ці інциденти безпеки включають кібератаки, програми-вимагачі, витоки даних, фінансової інформації, зловмисні дії працівників компаній та інші інциденти.

Деякі з найвідоміших інцидентів безпеки в 2022 році включають злом Crypto.com у січні 2022 року - кібератака на криптовалютні гаманці майже 500 користувачів. Зловмисники викрали $18 млн в Bitcoin і $15 млн в Ethereum. У березні 2022 року злом Microsoft торкнувся Bing, Cortana та інших продуктів. Хакерам вдалося викрасти матеріали Microsoft, але компанія зупинила атаку до того, як постраждали дані клієнтів. Атака стороннього підрядника Червоного Хреста призвела до компрометації 500 000 записів, включаючи "дуже вразливі" секретні документи. Проактивний захист є ключем до уникнення кібератаки, тож нижчі наведені топ-10 загроз кібербезпеки у 2022 році.

1.2.1. Соціальна інженерія

Соціальна інженерія залишається однією з найнебезпечніших хакерських технік, яку використовують кіберзлочинці, в основному тому, що вона покладається на людські помилки, а не на технічні вразливості. Легше обдурити людину, ніж зламати систему безпеки. І зрозуміло, що хакери це знають: згідно зі звітом Verizon Data Breach Investigations, 85% всіх витоків даних пов'язані з людською взаємодією. У 2022 році ми бачимо, як атаки соціальної інженерії, такі

як фішинг, еволюціонують, включаючи нові тенденції, технології та тактики. Наприклад, кількість атак, пов'язаних з криптовалютами, зросла майже на 200% в період з жовтня 2020 року по квітень 2021 року, і залишається значною загрозою, оскільки біткоїн та інші валюти, засновані на блокчейні, продовжують зростати в популярності та ціні.

1.2.2. Вплив третіх сторін

Кіберзлочинці можуть обійти системи безпеки, зламуючи менш захищені мережі, що належать третім особам, які мають привілейований доступ до основної мети хакера. Один з основних прикладів стороннього зламу стався на початку 2021 року, коли хакери здійснили витік персональних даних з понад 214 мільйонів акаунтів у Facebook, Instagram та Linkedin. Хакери змогли отримати доступ до даних, зламавши стороннього підрядника під назвою Socialarks, який працював у всіх трьох компаніях і мав привілейований доступ до їхніх мереж. У 2022 році порушення з боку третіх осіб лишається актуальною загрозою, оскільки компанії все частіше користуються аутсорсом для завершення роботи, яку раніше виконували штатні співробітники.

Згідно зі звітом про тенденції робочої сили за 2021 рік, понад 50% компаній більш охоче наймають фрілансерів в результаті переходу на віддалену роботу, спричинену COVID-19. Фірма з кібербезпеки CyberArk повідомляє, що 96% організацій надають цим зовнішнім сторонам доступ до критично важливих систем, забезпечуючи потенційно незахищений шлях доступу до своїх даних для використання хакерами.

1.2.3. Помилки конфігурації

Навіть професійні системи безпеки, швидше за все, містять принаймні одну помилку у встановленні та налаштуванні програмного забезпечення. У серії з 268 випробувань, проведених компанією Rapid7, що займається розробкою програмного забезпечення для кібербезпеки, 80% тестів на зовнішнє проникнення зіткнулися з помилковою конфігурацією, яку можна було б використати. У тестах,

де зловмисник мав внутрішній доступ до системи (тобто випробування, що імітують доступ через третю сторону або проникнення у фізичний офіс), кількість помилок конфігурації, які можна використати, зросла до 96%. Ponemon Institute повідомляє, що половина IT-спеціалістів визнають, що не знають, наскільки добре працюють встановлені ними інструменти кібербезпеки, а це означає, що щонайменше половина IT-спеціалістів вже не проводять регулярне внутрішнє тестування та технічне обслуговування.

У 2022 році на тлі продовження комбінованого впливу пандемії COVID-19, соціально-політичних потрясінь і триваючого фінансового стресу, прогнозовано збільшується кількість необережних помилок, які співробітники допускають на роботі, створюючи більше можливостей для використання кіберзлочинцями. Так, наприклад, згідно зі звітом компанії Lyra Health, 81% працівників зіткнулися з проблемами психічного здоров'я в результаті пандемії, а 65% працівників стверджують, що їхнє психічне здоров'я безпосередньо вплинуло на продуктивність їхньої роботи.

1.2.4. Низький рівень кібергігієни

"Кібергігієна" – поняття, що описує регулярні звички і практики щодо використання технологій, таких як уникнення незахищених мереж WiFi та впровадження запобіжних заходів, таких як VPN або багатофакторна автентифікація. Згідно з дослідженнями, майже 60% організацій покладаються на людську пам'ять для управління паролями, а 42% організацій управляють паролями за допомогою стікерів. Більше половини (54%) IT-фахівців не вимагають використання двофакторної автентифікації для доступу до облікових записів компанії, і лише 37% фізичних осіб використовують двофакторну автентифікацію для особистих облікових записів. Статистика: 75% кібератак у 2020 році використовували вразливості, які були виявлені щонайменше два роки тому. Менше половини (45%) опитаних користувачів кажуть, що змінили б свій пароль після витоку даних, і лише 34% кажуть, що регулярно змінюють свої паролі.

Завдяки зростанню віддаленої роботи у 2022 році, системи, що захищені слабкими паролями тепер доступні з незахищених домашніх мереж, а працівники входять в систему з особистих пристроїв, які мають набагато більше шансів бути втраченими або викраденими. Компанії і приватні особи, які не вдосконалюють свої кібер-практики, наражаються на набагато більший ризик, ніж раніше. Дивно, але IT-спеціалісти часто мають навіть гірші звички щодо кібергігієни, ніж населення в цілому: 50% IT-працівників стверджують, що вони повторно використовують паролі для облікових записів на робочому місці, у порівнянні з 39% громадян загалом.

1.2.5. Хмарні вразливості

Вважається, що безпека IT систем з кожним роком росте, однак в хмарній інфраструктурі відбуваються зворотні процеси. IBM повідомляє, що за останні п'ять років вразливості хмарних технологій зросли на 150%. Verizon's DBIR виявив, що понад 90% з 29 000 порушень, проаналізованих у звіті, були спричинені порушеннями веб-додатків. За даними Gartner, хмарна безпека в даний час є найбільш швидкозростаючим сегментом ринку кібербезпеки, який збільшився на 41% з $595 млн в 2020 році до $841 млн в 2021 році. Хоча спочатку експерти прогнозували масове повернення в офіс, зростання кількості нових варіантів COVID і проривних випадків роблять цей сценарій все більш малоймовірним - а це означає, що підвищена загроза порушень хмарної безпеки навряд чи ослабне в найближчому часі.

Нові розробки в області хмарної безпеки включають в себе прийняття архітектури хмарної безпеки "Zero Trust" ("Нульова довіра"). Системи Zero Trust розроблені таким чином, щоб функціонувати так, ніби мережа вже була скомпрометована, виконуючи необхідні перевірки на кожному кроці і при кожному вході в систему, замість того, щоб надавати постійний доступ до розпізнаних пристроїв або пристроїв в межах периметра мережі. Цей стиль безпеки набув популярності у 2021 році і отримує широке впровадження у нинішньому році.

1.2.6. Вразливості мобільних пристроїв

Ще однією закономірністю, спричиненою пандемією COVID-19, стало зростання використання мобільних пристроїв. Мало того, що віддалені користувачі більше покладаються на мобільні пристрої, експерти з питань пандемії також заохочували широкомасштабне впровадження мобільних гаманців та технологій безконтактних платежів з метою обмеження передачі мікробів.

Вразливості мобільних пристроїв посилилися через масовий перехід на віддалену роботу, що призвело до зростання кількості компаній, які впроваджують політику "принеси свій власний пристрій" (bring-your-own-device, BYOD). Згідно зі звітом Check Point Software про мобільну безпеку, протягом 2021 року 46% компаній зіткнулися з інцидентом безпеки, пов'язаним зі зловмисним мобільним додатком, завантаженим співробітником.

Кіберзлочинці також почали націлюватися на системи управління мобільними пристроями, які, за іронією долі, призначені для того, щоб дозволити компаніям управляти корпоративними пристроями таким чином, щоб забезпечити безпеку корпоративних даних. Оскільки системи управління мобільними пристроями підключені до всієї мережі мобільних пристроїв, хакери можуть використовувати їх для одночасної атаки на девайс кожного співробітника компанії.

1.2.7. Вразливості інтернету речей

Так чи інакше, але велику роль у формуванні сучасного ландшафту загроз відіграв викликаний пандемією перехід на віддалену роботу. Так, в США понад чверть працюючого населення перенесли свою роботу додому, де 70% будинків мають принаймні один "розумний" пристрій. Не дивно, що в результаті цього різко зросла кількість атак на смарт-пристрої або пристрої "Інтернету речей" (IoT). З січня по червень 2021 року було зафіксовано понад 1,5 мільярда зламів пристроїв IoT.

У поєднанні з низьким рівнем кібергігієни більшої половини людей, підключення до Інтернету речей відкриває світ вразливостей для хакерів.

Середньостатистичний розумний пристрій піддається атаці протягом п'яти хвилин після підключення до Інтернету, і за оцінками експертів, розумний будинок з широким спектром пристроїв Інтернету речей може стати мішенню для 12 000 спроб злому протягом одного тижня. Дослідники прогнозують, що кількість розумних пристроїв подвоїться в період між 2021 і 2025 роками, створюючи ще більш широку мережу точок доступу, які можуть бути використані для злому персональних і корпоративних систем. Очікується, що кількість мобільних IoT-з'єднань досягне 3,5 мільярда в 2023 році, а експерти прогнозують, що до 2025 року більше чверті всіх кібератак на бізнес будуть засновані на IoT.

1.2.8. Програми-вимагачі

Хоча атаки з використанням програм-вимагачів аж ніяк не є новою загрозою, за останні роки вони значно подорожчали: у період з 2018 по 2020 рік середня сума викупу зросла з $5 000 до $200 000. Атаки вірусів-здирників також коштують компаніям у вигляді недоотриманого доходу, поки хакери утримують доступ до системи з метою отримання викупу. (Середня тривалість простою системи після атаки вірусу-здирника становить 21 день).

В опитуванні 1 263 фахівців з кібербезпеки, проведеному в 2021 році, 66% заявили, що їхні компанії зазнали значних втрат доходу в результаті атаки з використанням програм-вимагачів. Кожен третій заявив, що їхня компанія втратила найвище керівництво через звільнення або відставку, а 29% заявили, що їхні компанії були змушені звільнити працівників після атаки з використанням програм-вимагачів. Статистика: середня вартість відновлення після атаки вірусу-здирника зросла більш ніж удвічі в період з 2020 по 2021 рік.

1.2.9. Неефективне управління даними

Управління даними - це більше, ніж просто підтримання в порядку систем зберігання та організації. Для порівняння, обсяг даних, створених споживачами, подвоюється кожні чотири роки, але більше половини цих нових даних ніколи не використовуються і не аналізуються. Нагромадження надлишкових даних

призводить до плутанини, що робить їх вразливими до кібератак. Порушення, спричинені помилками в обробці даних, можуть коштувати так само дорого, як і високотехнологічні атаки на засоби забезпечення кібербезпеки. У 2018 році компанія Aetna була зобов'язана виплатити 17 мільйонів доларів штрафу після того, як вона відправила конфіденційну медичну інформацію в конверті неправильного типу.

Щоб відсортувати правильні дані від непотрібних, команди все більше покладаються на автоматизацію, яка має свій набір ризиків. Автоматизовані програми схожі на павутину - невелика подія на одній стороні павутини може відчуватися по всій структурі. І хоча сама обробка даних покладається на штучний інтелект, правила та налаштування, яким ШІ має слідувати, все ще створюються людьми і чутливі до людських помилок.

1.2.10. Неадекватні процедури після атаки

Дірки в безпеці повинні бути усунені одразу після кібератаки. В опитуванні 1 263 компаній, які стали мішенню для кібератак у 2021 році, 80% жертв, які внесли викуп, заявили, що незабаром після цього вони зазнали ще однієї атаки. Фактично, 60% кібератак можна було б запобігти, якби було застосовано доступне виправлення, а 39% організацій стверджують, що вони знали про свою вразливість до того, як сталася кібератака.

Одним з рішень, що набуває все більшої популярності, є впровадження моделі підписки на програмне забезпечення для управління виправленнями. Продукти "Patching-as-a-Service" забезпечують безперервні оновлення та виправлення, збільшуючи швидкість та ефективність виправлень. Автоматизована установка патчів також знижує ймовірність появи вразливостей, створених через людський фактор [3].

1.3 Вплив вторгнення рф в Україну на кібербезпеку

Компанія ESET, що спеціалізуються на інформаційній безпеці опублікували звіт, згідно якого загальна кількість виявлених зразків загроз у січні-квітні 2022 року зросла на 20% порівняно з аналогічним періодом 2021 року. У звіті компанії вказується, що зокрема, зросла кількість шпигунських програм та загроз, що поширюються через електронну пошту.

1.3.1 Звіт компанії ESET

Значний вплив на дану ситуацію поширення загроз у світі мала війна в Україні. Зокрема, ця тема активно використовувалася у спам-розсилках та на шкідливих веб-сайтах маскуючись під допомогу постраждалим. У період з січня по квітень 2022 року кількість загроз, що поширюються через електронну пошту, раптово зросла на 37%. Це найбільший приріст цього типу загроз починаючи з 2020 року. Таку динаміку спеціалісти пов'язують з відновленням роботи ботнету Emotet, який масово розсилає користувачам спам-повідомлення зі шкідливими вкладенням. Крім звичних тем електронних листів, таких як платежі, замовлення та доставки, з початку року зростає кількість шкідливих повідомлень на тему подорожей.

Крім того, з початку повномасштабного вторгнення в Україну на інфраструктуру країни неодноразово проводились кібератаки. Зокрема, починаючи з 23 лютого, під час атак на українські організації було використано низку шкідливих програм для знищення даних, а також унікальну загрозу Industroyer, націлену на енергетичний сектор.

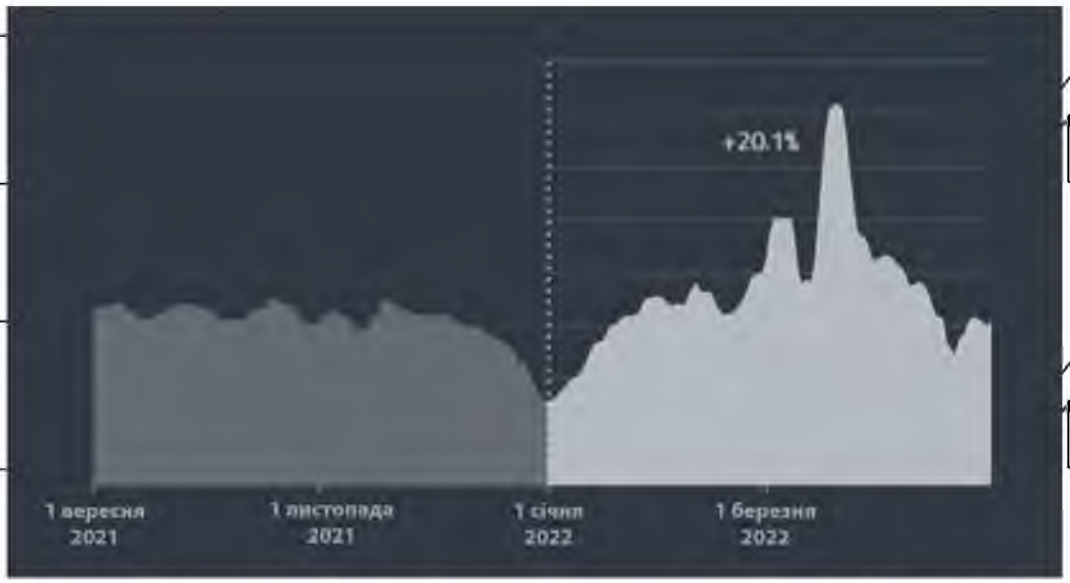


Рисунок 1.1 – Графік зафіксованих кібератак

На противагу зростаючому рівню фішингових атак, вперше за два роки безперервного зростання атак на протокол RDP був спад даної активності. Кількість атак з метою підбору пароля на протокол віддаленого робочого столу (RDP) знизилася в 2022 році на 41%. При цьому, 60% RDP-атак з початку 2022 року походили з Росії.

За термін с січня по квітень 2022 року кількість загроз викрадення інформації зросла на 12% у порівнянні з попереднім роком. Найбільше зростання відбулося серед атак з використанням шпигунських програм та шкідливого банківського ПЗ. Зокрема, кількість програм зі шпигунським кодом за цей період зросла приблизно на 18%.

Зросла також і кількість мобільних шпигунських застосунків. Активність таких програм, які можуть отримувати доступ до різних функцій смартфона, включаючи аудіо- та відеозапис, збільшилась на 170%. Даний показник свідчить про те, що зловмисники шукають способи заробітку на особистих або навіть корпоративних даних на Android-пристроях. В цей же час на операційній системі macOS майже половина просканованих додатків були потенційно небажаними додатками.

Відразу після вторгнення Росії в Україну шахраї вирішили скористатися добродійністю людей з усього світу у підтримці українців задля виманювання

грошей у користувачів. 24 лютого фахівці ESET зафіксували значне збільшення спам-повідомлень і перші шахрайські домени, які використовують тему війни для наживи. У середньому телеметрія компанії ESET щодня виявляє 4,8 млн веб-загроз і 370 тис. шкідливих URL-адрес по всьому світу. При цьому кількість заблокованих фішингових URL-адрес зросла майже на 30%. Найвищий показник виявлення був зафіксований 07 березня, що втричі перевищило середньодобовий показник з початку поточного року. Крім того, за даними ESET, близько третини фішингових URL-адрес, що були виявлені за період з січня по квітень 2022 року, були замасковані під фінансові організації. Зловмисники також використовували в якості приманки підроблені сторінки входу в Facebook і WhatsApp.

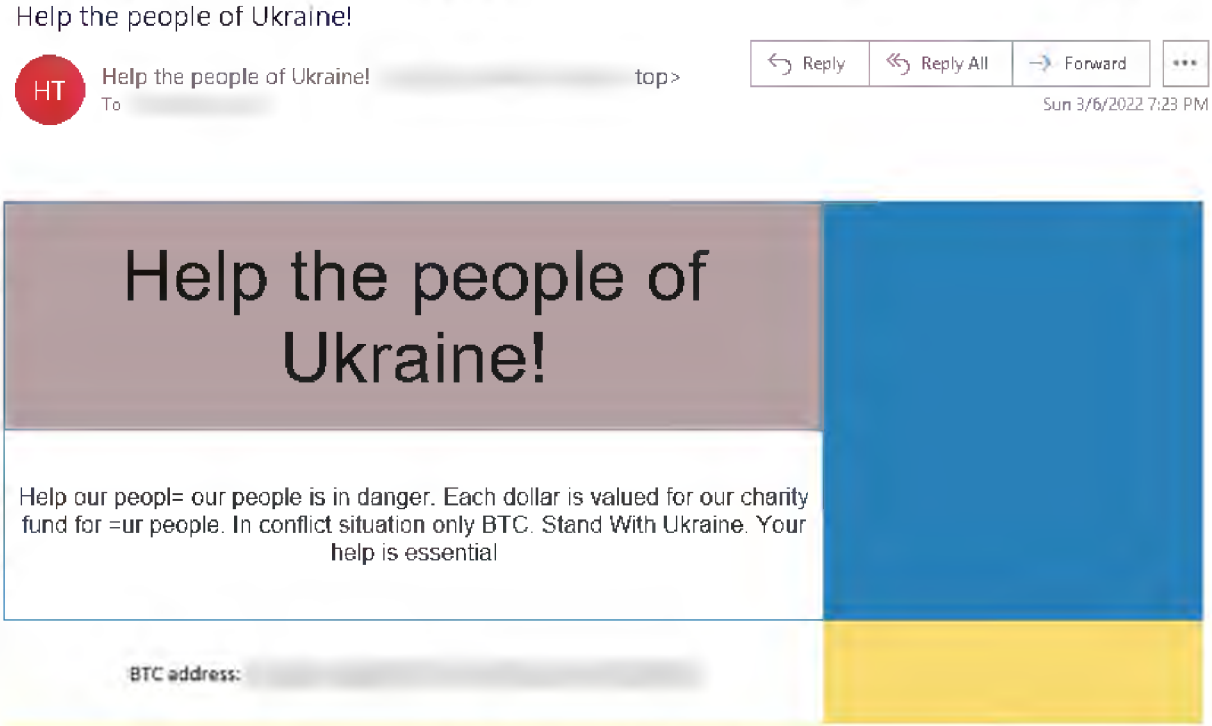


Рисунок 1.2 – Шахрайське повідомлення

Щоб убезпечити мережу компанії та особисті дані спеціалісти рекомендують використовувати надійні паролі та двофакторну автентифікацію, дбати про безпеку свого мобільного пристрою, а також забезпечити надійний фізичний захист обладнання компанії.

1.3.2 Індекс кіберсили держав світу

Гарвардський Центр науки і міжнародних відносин Белфера оприлюднив оновлений Індекс кіберсили держав світу (NCPI) за 2022 рік, що є розвитком попереднього звіту за 2020 рік, в якому 30 найсильніших країн ранжуються відповідно до їх спроможності досягти восьми ключових пунктів, що демонструють силу у кіберпросторі.

До пунктів, що оцінюються належать такі:

а) накопичення та захист цінної інформації;

б) контроль та маніпулювання інформаційним середовищем;

в) участь у розвитку міжнародних кібернетичних норм та технічних стандартах у сфері кібербезпеки;

г) знищення або виведення з ладу інфраструктури супротивника;

д) збір даних зовнішньої розвідки для національної безпеки;

е) зростання компетентності національних технологій кібербезпеки та комерції;

є) посилення та вдосконалення кіберзахисту;

ж) спостереження та моніторинг за внутрішніми загрозами.

Під накопиченням та захистом цінної інформації мається на увазі проведення державою кібероперацій з метою накопичення багатства – цінної інформації. Це включає в себе крадіжку за допомогою кіберзасобів, включаючи програми-вимагачі, шантаж з використанням інформації, отриманої через злом даних та атаки на цифрову інфраструктуру фінансових установ та інше.

Контроль та маніпулювання інформаційним середовищем відображає використання державою електронних засобів для контролю інформації та зміни наративів як всередині країни, так і за її межами. Ця форма включає в себе поширення внутрішньої пропаганди, створення та посилення дезінформації за кордоном, використання кіберзасобів для націлювання на групи, що знаходяться за межами її юрисдикції, та підриву їхньої діяльності. Останнє включає в себе видалення екстремістських матеріалів із соціальних мереж та спростування іноземної пропаганди.

Участь у розвитку міжнародних кібернетичних норм та технічних стандартах у сфері кібербезпеки має на увазі те, чи бере держава активну участь у міжнародних правових, політичних та технічних дебатах навколо норм кібербезпеки. Це включає в себе підписання договорів у сфері кібербезпеки, участь у робочих групах, приєднання до кіберпартнерств та альянсів для боротьби з кіберзлочинністю та обміну технічним досвідом і можливостями.

«Знищення або виведення з ладу інфраструктури супротивника» - під даним критерієм мається на увазі використання державою руйнівних кібертехнологій, тактику і процедури для стримування, розмивання або погіршення здатності супротивника вести бойові дії в кібернетичній або фізичній військовій площині. Сюди входять кібератаки на об'єкти критичної інфраструктури і атаки типу "відмова в обслуговуванні" на урядові комунікаційні мережі. Це також включає кібератаки для демонстрації намірів і спроможності стримувати супротивника від його можливих намірів.

Пункт «збір даних зовнішньої розвідки для національної безпеки» вказує на те, що держава здобуває інформацію, що є державною таємницю іншої країни за допомогою засобів кібервтручання. Це має на меті збір інформації про дипломатичну діяльність, військове планування, моніторинг договорів та інші ситуації, в яких держави прагнуть покращити свою ситуативну обізнаність та розуміння планів та цілей іншої держави. Це включає в себе хакерські атаки з порушенням доступу до секретних матеріалів, таких як військові плани, кадрові записи, доступ до комунікацій високопоставлених державних діячів.

Зростання компетентності національних технологій кібербезпеки та комерції – про те як держава намагається розвивати свою внутрішню технологічну галузь. Це може відбуватися як легальними, так і нелегальними шляхами. Незаконні засоби включають ведення промислового шпигунства проти іноземних компаній і держав з метою викрадення потрібних технологій. Легальні засоби включають інвестиції в дослідження і розробки в галузі кібербезпеки та пріоритетний розвиток кадрів у сфері кібербезпеки.

Під виразом «Посилення та вдосконалення кіберзахисту» мається на увазі те, що держава визначила пріоритетом стратегію посилення захисту урядових та національних активів і систем, а також покращення національної кібергігієни та відмовостійкості. Це включає активний захист державних активів, просування кібербезпеки та кібергігієни в ключових галузях промисловості та населення в цілому, а також підвищення національної обізнаності про кіберзагрози.

Спостереження та моніторинг за внутрішніми загрозами має на меті вжиття державою заходів для надання собі правових дозволів та можливостей для моніторингу, виявлення та збору розвідувальної інформації про внутрішні загрози. Це може варіюватися від зусиль зі стеження за своїми громадянами, моніторингу інтернет-трафіку, обходу шифрування та виявлення діяльності іноземних спецслужб, злочинних організацій і терористичних груп [4].

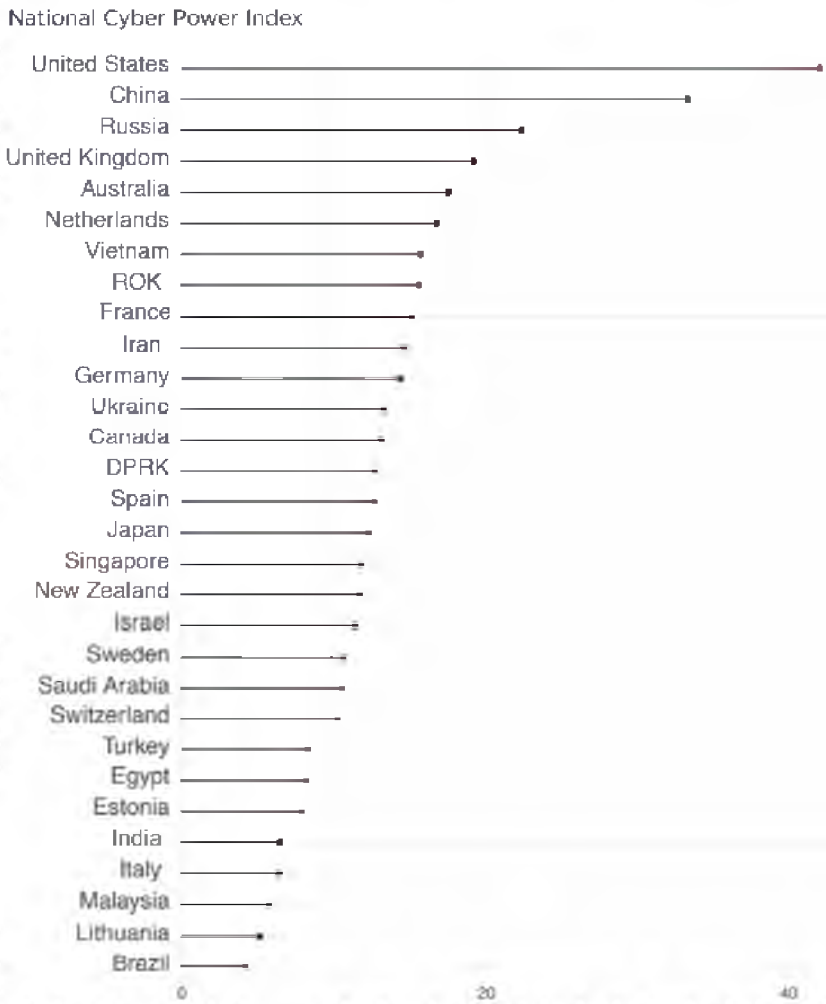


Рисунок 1.3 – Рейтинг кіберсили держав світу

Згідно даного рейтингу, перші 3 місця належать США, Китаю та росії, відповідно. Україна в ньому посідає 12 місце, що значно краще ніж було у 2020 році – тоді вона посідала 20 місце, а в рейтингу захисту державних ресурсів Україна знаходиться аж на 2 місці. На посилення позиції України тут вплинув перегляд державою політики у сфері кібербезпеки та інвестування в обладнання та спеціалістів.

Формула розрахунку індексу держав виглядає так:

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{8}\sum_{x=1}^{8} Capability_x \times Intent_x$$

де capability – можливості держави, intent – прагнення держави в їх розвитку та використанні.

Рисунок 1.4 – Сильні та слабкі сторони України у сфері захисту

Також можна переглянути характеристику кожної з 30 держав окремо, де показані сильні та слабкі сторони кіберрозвитку країни.

Слід зазначити, що в питанні захисту даних Україна має гарні показники, займаючи 2 стрічну в рейтингу після Австралії. На жаль, в інших сферах поки не вдалося досягти подібних результатів, але те що Україна за 2 роки піднялася в

рейтингу на 8 позицій говорить про здатність до подальшого розвитку не тільки сфери захисту даних, але й проведення успішних кібератак на території супротивника, ще більше впровадження технологій у виробництво та участь у міжнародних стандартах та нормах.

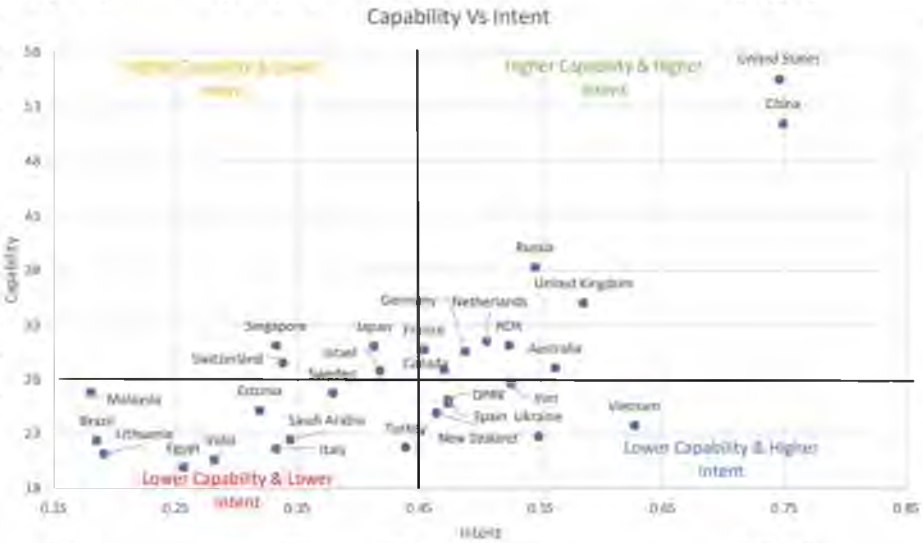


Рисунок 1.5 – Графік можливостей та прагнень держав

Окремо слід відмітити рейтинг прагнень держав до використання інформаційних ресурсів, де Україна ввійшла в топ-10, зайнявши 9 місце в рейтингу, поруч з Нідерландами та Іспанією.

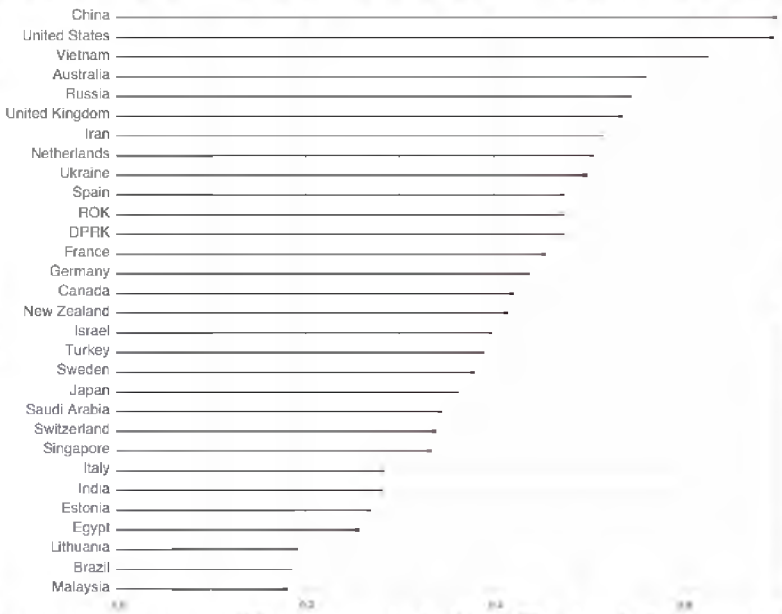


Рисунок 1.6 – Показник прагнень держави до використання кіберресурсів

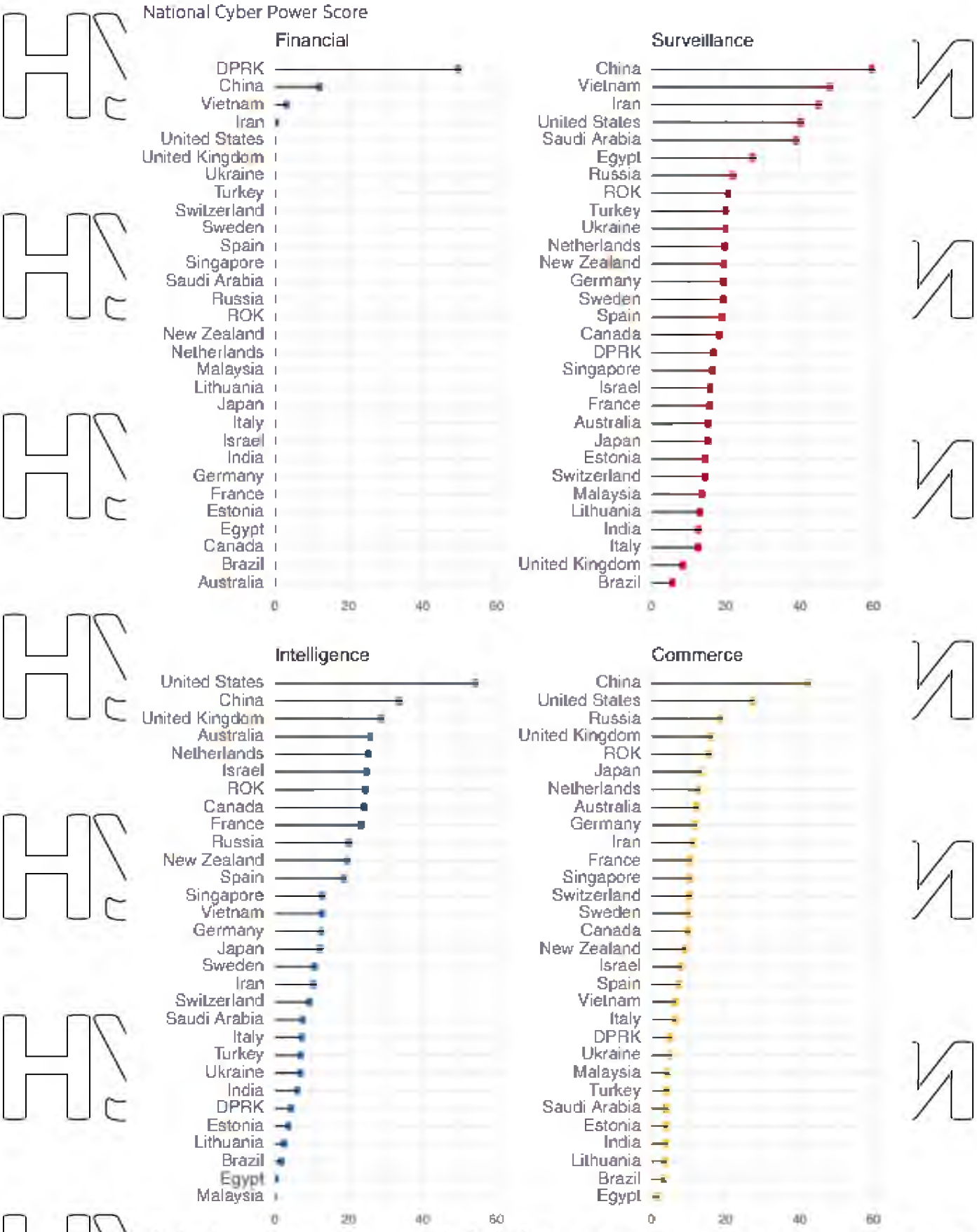


Рисунок 1.7 – Рейтинг по показникам: накопичення цінної інформації, спостереження, інтелектуальні вкладення, розвиток технологічного сектору

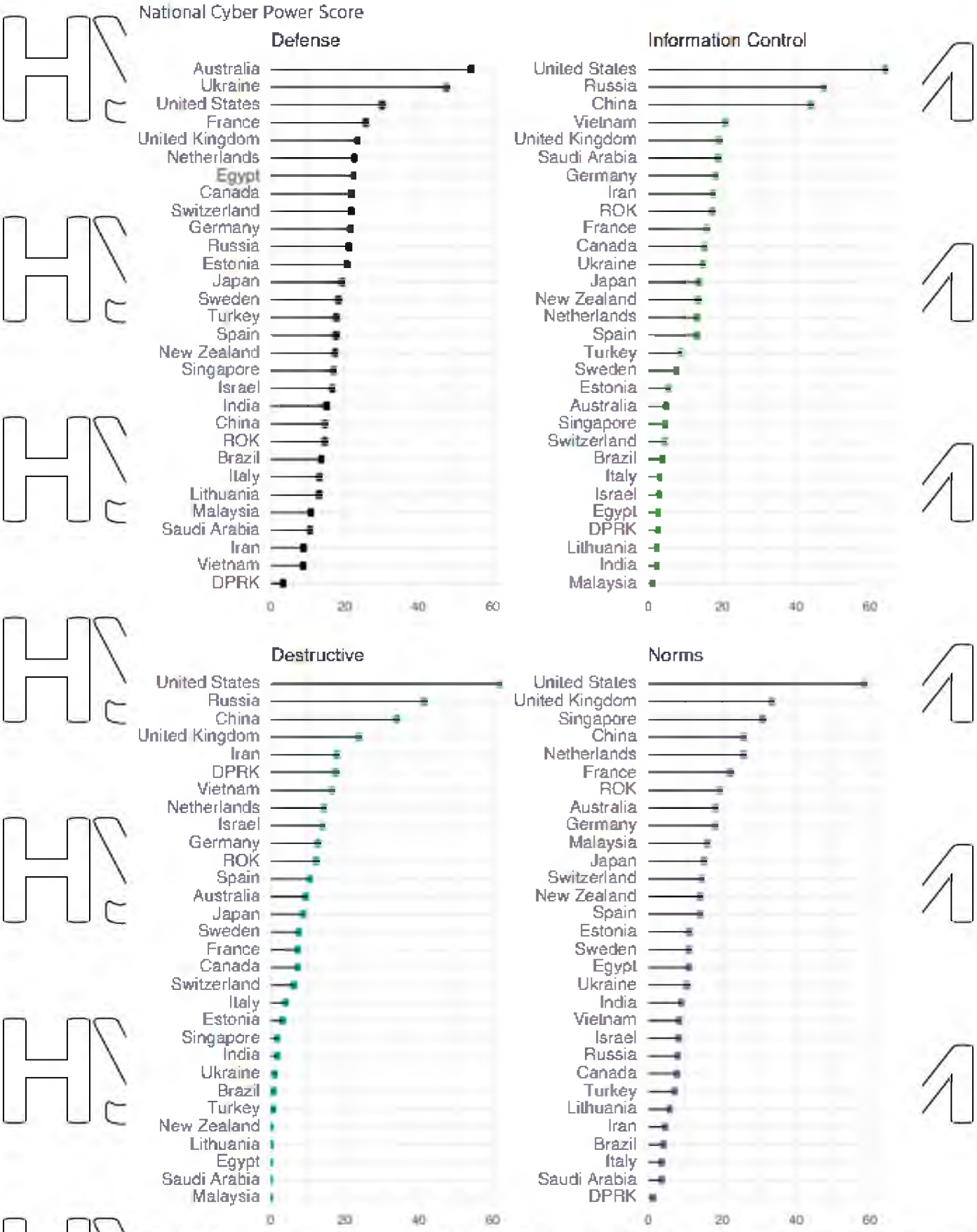


Рисунок 1.8 – Рейтинг по показникам: захист, контроль інформації, виведення з ладу інфраструктури супротивника, участь у кібернормах

2 ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У НАВЧАЛЬНОМУ ЗАКЛАДІ

2.1 Основні методи та моделі в кібербезпеці

Фахівці практично в будь якій сфері використовують моделі поведінки та реагування на інциденти для роботи. Медичні працівники використовують моделі для опису спостереження та диференціації захворювань, а фахівці з психічного здоров'я впродовж десятиліть розробляють різні моделі поведінки людей. Спеціалісти з кібербезпеки також використовують моделі для забезпечення ясності системи, визначення того, як розмістити засоби контролю безпеки і, що найголовніше, профілювання того, як здійснюються кібератаки.

Не менш важливими є методи розпізнавання загроз, які дають змогу зрозуміти, в якому напрями має рухатись компанія для забезпечення захисту даних. Нижче наведені основні з них:

а) розвідка загроз;

б) аналіз поведінки зловмисників і користувачів;

в) пастки для зловмисників;

г) полювання на загрози.

Кожен метод виявлення загроз не буде дієвим, якщо не будуть застосовуватись комплексні моделі захисту. Найпопулярнішими з них є:

а) модель «льодяника»;

б) модель «Цибулини» або «Піраміди»;

в) модель зрілості промислової кібербезпеки

При розгляді типових додатків для виявлення вторгнень, таких як Snort, інструмент управління інформацією і подіями безпеки (SIEM), додаток Splunk, або розвідки кіберзагроз (CTI), такий як AlienVault OTX, можна побачити посилання на один або кілька життєвих циклів хакерів.

Це моделі для злому. Насправді, можна знайти посилання на ці моделі в тисячах додатків. Наприклад, впровадження штучного інтелекту (ШІ) часто

базується на цих моделях. Наступні три основні моделі кібербезпеки, які використовуються для розслідування вторгнень є ключовими для розуміння принципів роботи кіберрозвідки, яка авторитетно визначена в документі Серджіо Кальтаджіроне "Інтелектуальний аналіз загроз промислового контролю" (Industrial Control Threat Intelligence):

а) ланцюг кіберзахисту від Lockheed Martin

б) діамантова модель аналізу вторгнень

в) модель MITRE ATT&CK

2.2 Методи розпізнавання загроз

2.2.1 Розвідка загроз

Метод розвідки загроз необхідний для того, щоб компанії могли зупинити можливі загрози. Для виявлення невідомих загроз може використовуватися програмне забезпечення, яке використовує дані сигнатур, зібрані в результаті попередніх атак.

Така програма також збирає розвідувальні дані або докази, які ідентифікують небезпеки шляхом порівняння подібності між поточними і минулими даними. Ефективним способом ознайомлення з розпізнаними ризиками є застосування інтелектуальних підходів для виявлення загроз.

Загрози, які використовують ще неопубліковані прогалини в безпеці, однак, можуть бути нерозпізнані системою захисту. Розвідка загроз часто спирається на дані і знання, отримані в результаті попередніх атак, що ускладнює виявлення нових небезпек. Розвідка про загрози прагне зрозуміти наступне:

а) методи, якими користуються зловмисники;

б) вразливості мережі, систем і додатків компанії;

в) ідентифікація зловмисників, які прагнуть скомпрометувати мережі.

Ця інформація допомагає підвищити готовність до інформаційних загроз та консолідувати зусилля щодо їх подолання, одночасно інформуючи керівників компаній і зацікавлені сторони про потенційні ризики та наслідки, якщо зловмисники досягнуть успіху [5].

2.2.2 Аналіз поведінки зловмисників і користувачів

Аналіз поведінки є одним з методів виявлення загроз, оскільки він використовує довідкові дані для виявлення відхилень або затримок, які потенційно можуть призвести до злому. Програмне забезпечення для виявлення загроз відстежує активність користувачів та аналізує дані, щоб виявити підозрілу поведінку користувачів системи, що можуть бути діями кіберзловмисника.

Тривалість доступу та тип даних, які шукає зловмисник, часто збігаються з діями, зафіксованими програмним забезпеченням для виявлення загроз. Реакція безпеки буде негайно ініційована, коли програмне забезпечення для виявлення загроз визначить, що користувач намагається отримати інформацію з небезпечного сайту або поза встановленим часом.

Детектори загроз збирають воєдино фрагменти інформації, щоб зрозуміти складну поведінку зловмисника. Організація може використовувати це для виявлення активності зловмисника.

2.2.3 Пастки для зловмисників

Пастка для зловмисника – це надійний метод виявлення небезпеки для захисту ваших даних. Цей метод може зупинити кіберзловмисника від доступу до системи безпеки даних вашої компанії для отримання необхідної інформації. Експерти радять компаніям використовувати пастки для виявлення будь-яких небезпечних загроз.

Пастка для зловмисників встановлюється таким чином, щоб обдурити зловмисника, використовуючи приманку (аналогією може бути бажаного горщика з медом). Приманка може здатися зловмиснику справжньою, і він потрапляє в пастку, використовуючи цю ефективну техніку виявлення загроз. Використання

фальшивих даних може спровокувати виявлення сигналу, який автоматично розпочне розслідування тіньової діяльності у вашій мережі.

2.2.4 Полювання на загрози

Полювання на загрози - це відкритий проактивний метод до виявлення загроз, коли аналітики безпеки активно шукають загрози, що можуть бути реалізовані, або ознаки того, що зловмисники вже отримали доступ до ключових систем. Досліджуючи мережу організації, кінцеві точки та технології безпеки, мисливці за загрозами намагаються виявити зловмисників, які успішно оминули сучасні засоби кіберзахисту. Здатність захистити корпоративні дані при використанні даного методу залежить від отриманої інформації. Полювання на загрози дозволяє експертам з кібербезпеки шукати вхідні небезпеки, які ще не були виявлені засобами захисту.

Крім того, цей метод виявлення загроз є більш сучасним. Через це лише проникливі та кваліфіковані фахівці з кібербезпеки можуть планувати та готуватися до такого роду виявлення загроз [6].

2.3 Моделі захисту інформаційних систем

2.3.1 «Льодяникова» модель захисту системи

Льодяникова модель - це модель захисту системи, що подається як аналогія до звичайного льодяника. Зазвичай льодяник має в середині наповнення, а навколо - шар скоринки, в основному з цукрового ароматизованого сиропу. Людина лиже і лиже льодяник, і врешті-решт скоринка зникає, і вже можна насолодитися наповненням.

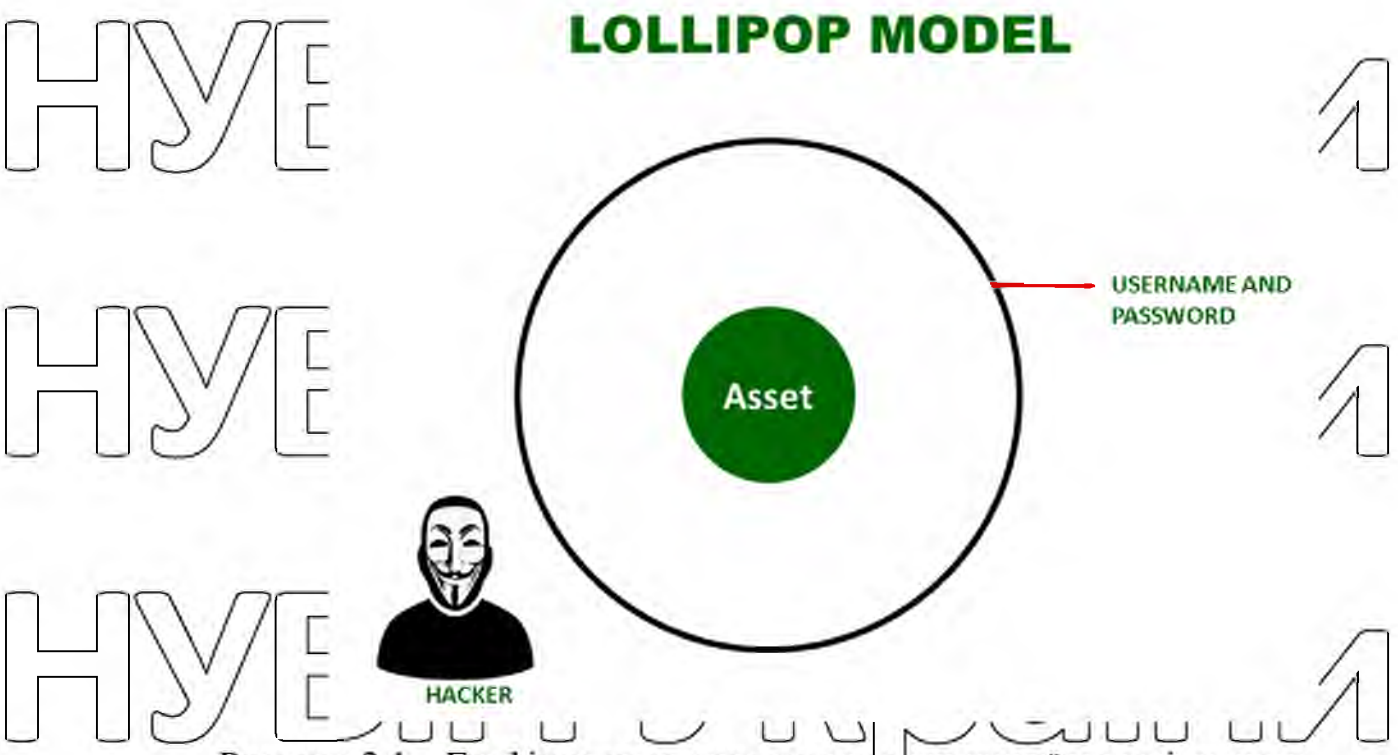


Рисунок 2.1 – Графічне представлення льодяникової моделі захисту

Якщо порівняти цю аналогію льодяника з моделлю, як показано на рисунку вище, хакеру потрібно лише зламати один шар захисту, щоб отримати доступ до даних, в даному випадку, наприклад, до імені користувача та паролю від облікового запису. Як тільки це буде зроблено, хакер отримає доступ до даних користувача. Таким чином, льодяникова модель є доволі слабкою моделлю для мережевої безпеки.

2.3.2 Модель «цибулини» або «піраміди»

«Цибулина модель» - це модель захисту, пов'язана з аналогією до цибулі. Цибуля - це овоч, який складається з багатьох шарів. Тільки знімаючи кожен шар, ми можемо дістатися до центру цибулини. До того ж, знімаючи ці шари, очі людини починають сльозитися. Якщо зіставити цю аналогію цибулини з моделлю, як показано на рисунку нижче, то хакеру необхідно зламати всі шари захисту, щоб отримати доступ до даних. Порушення кожного рівня, тобто міжмережевого екрану, IDS/IPS, аутентифікації, авторизації та криптографії, в даному випадку, повинно викликати сльози на його очах.

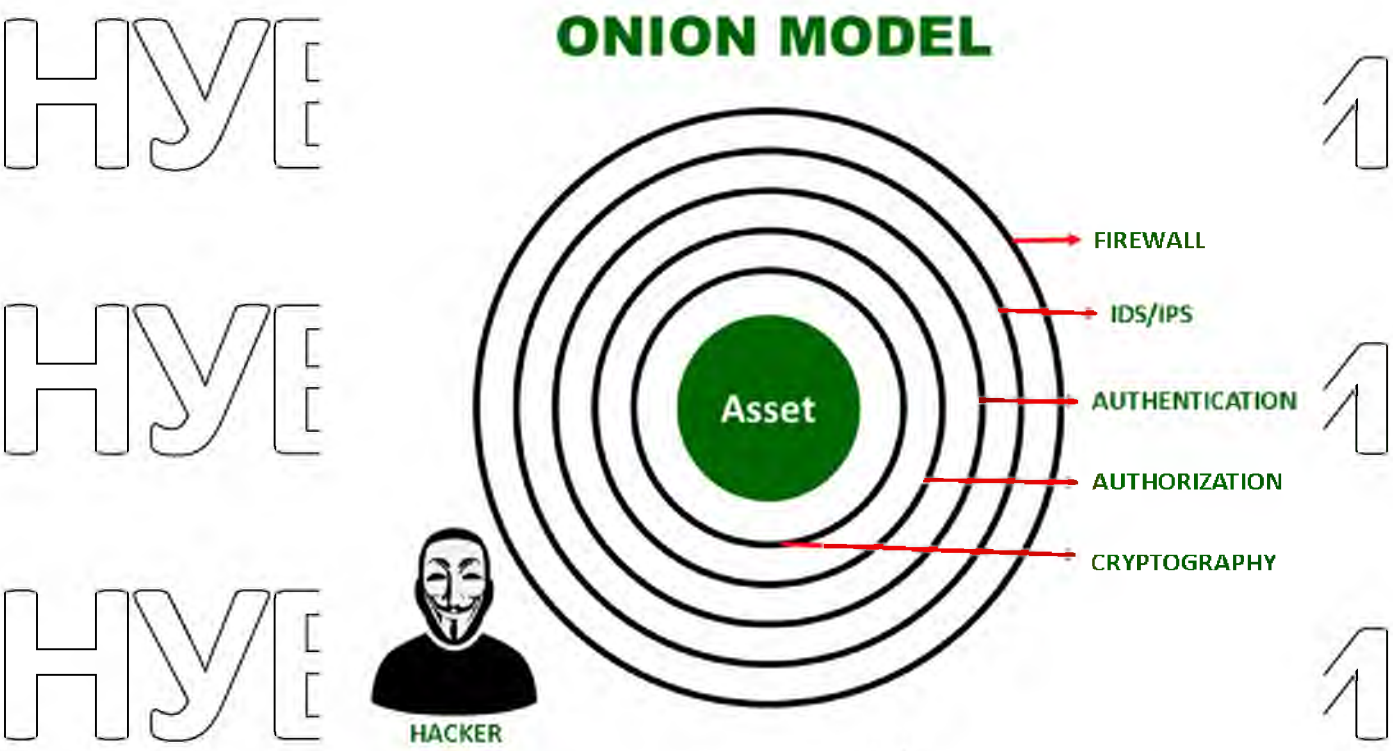


Рисунок 2.2 – Графічне представлення «цибулиної» моделі захисту

Простими словами, злам кожного рівня повинен бути складним і надзвичайно важким для хакера. Тому модель "цибулини" вважається досить хорошою моделлю для мережевої безпеки.

Модель «піраміди» практично ідентична до «цибулиної», де чим більше рівнів має піраміда захисту, тим більш захищеною є система.

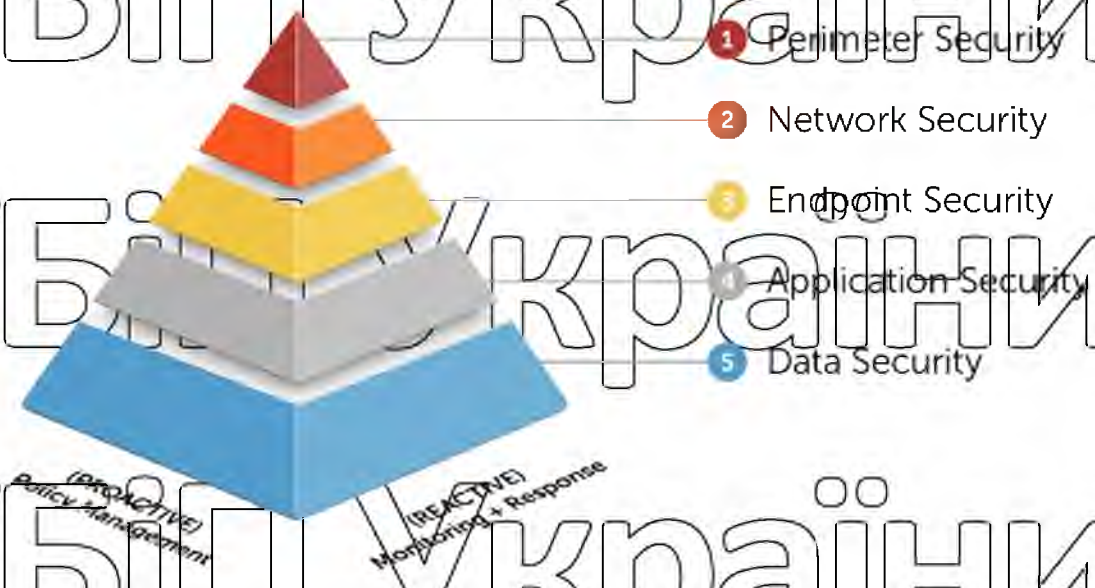


Рисунок 2.3 – Модель захисту «Піраміда»

Так само проводячи аналогію зі справжніми пірамідами, чим вона нижча – тим легше залізти на вершину, а чим вища – тим важче піднятися. Такі діаграми можуть мати різне розташування елементів безпеки, але незмінно одне – чим більше рівнів захисту даних – тим краще.

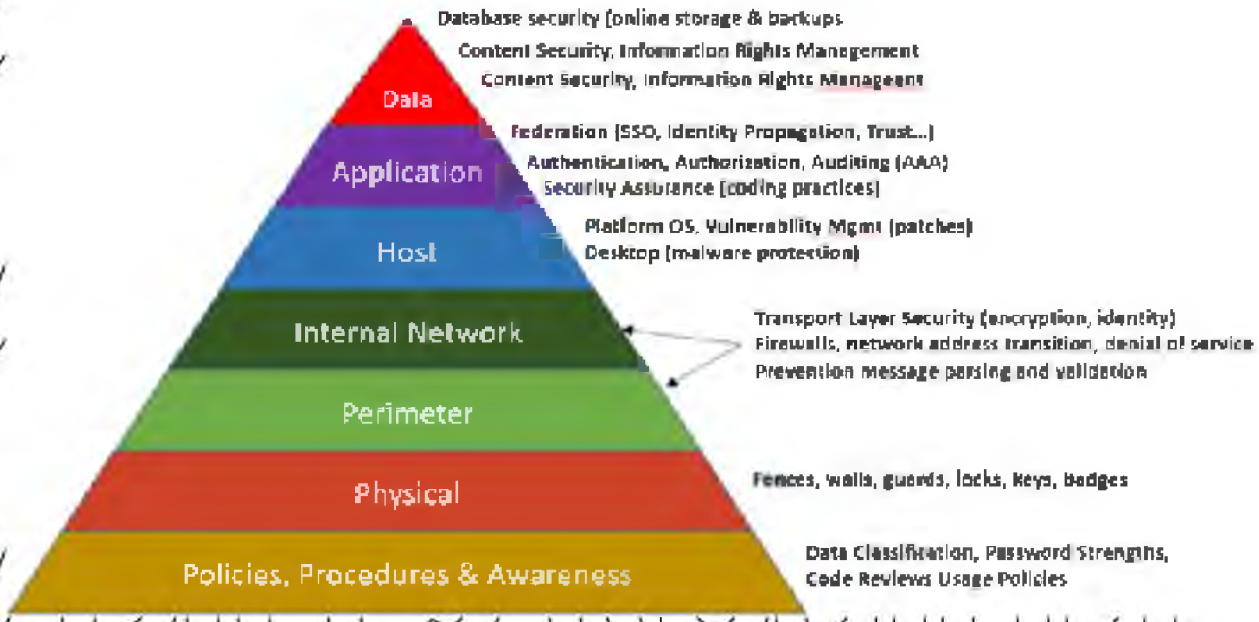


Рисунок 2.4 – Детальний розгляд моделі «піраміда»

2.3.3 Модель зрілості промислової кібербезпеки

Дана модель була розроблена компанією ARC, що спеціалізується на кібербезпеці та допомагає менеджерам в компаніях зрозуміти виклики кібербезпеки без необхідності ставати експертами з кібербезпеки. Вона дозволяє менеджерам збалансувати інвестиції в кібербезпеку з їхньою готовністю прийняти кіберризики та економічними перевагами додаткових рівнів безпеки. Ця модель також надає зручний спосіб пояснити відмінності між пасивним та активним кіберзахистом. Модель ARC розбиває кібербезпеку на набір кроків, які поступово зменшують кіберризики. Кожен крок спрямований на вирішення конкретної, легко зрозумілої проблеми безпеки, такої як захист окремих пристроїв, захист підприємств від зовнішніх атак, стримування шкідливого програмного забезпечення, яке все ще може потрапити в систему управління, моніторинг систем

на предмет підозрілої активності, а також активне управління складними загрозами та кіберінцидентами.

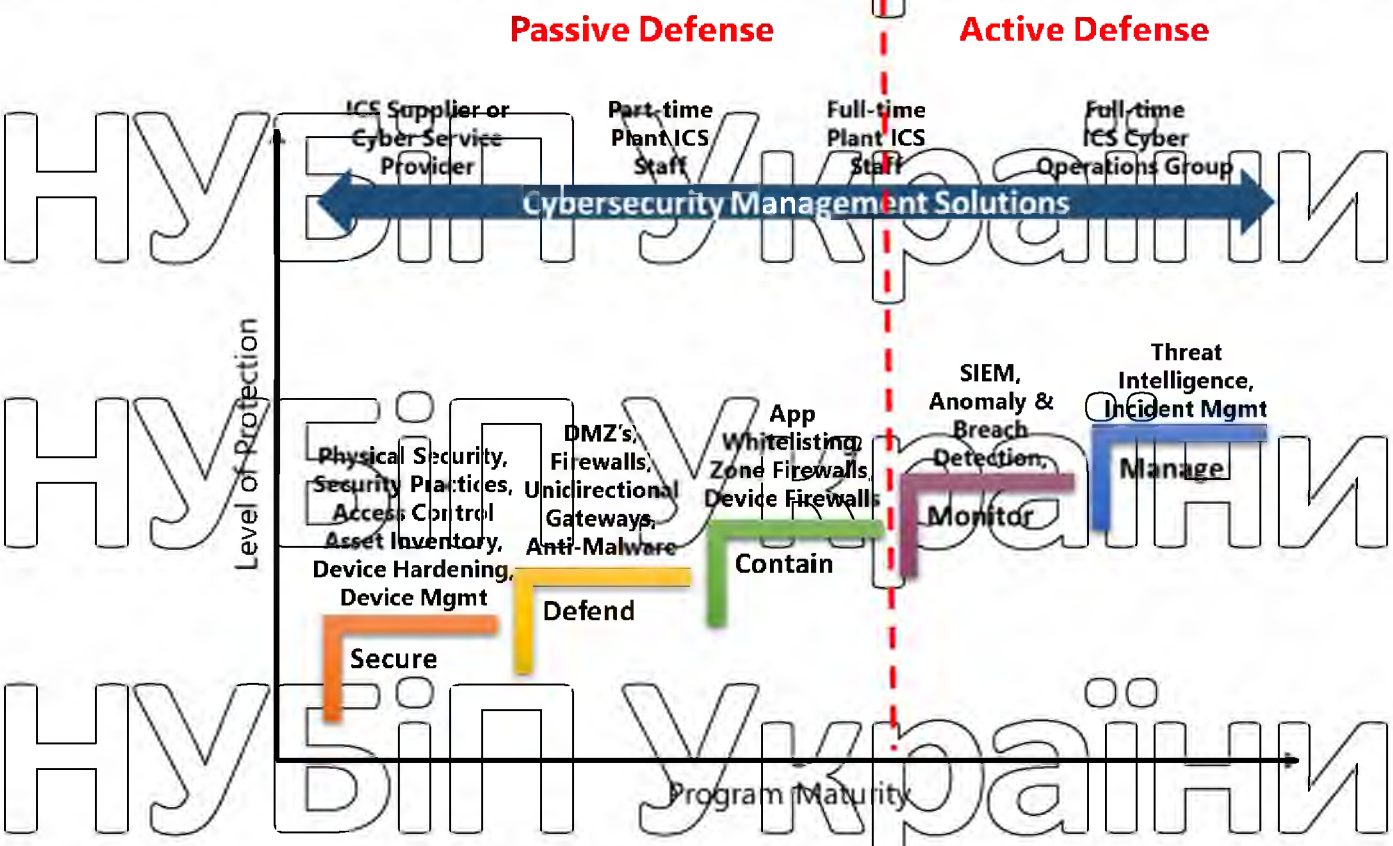


Рисунок 2.5– представлення моделі зрілості промислової кібербезпеки

Кожен крок має відповідний набір дій та технологій, які можуть бути використані для досягнення поставлених цілей. Модель також показує людські ресурси та інструменти, необхідні для підтримки та ефективного використання інвестицій в технології.

Рекомендації з кібербезпеки від постачальників систем автоматизації та експертів з безпеки охоплюють весь спектр. Однак дослідження ARC показує, що більшість компаній оснастили свої об'єкти тільки пасивними захисними технологіями. Багатьом організаціям також не вистачає ресурсів для підтримки і використання більш складних засобів захисту вище цього рівня. Це може бути достатнім для компаній, які можуть терпіти збої в роботі. Але оператори критичної інфраструктури не можуть приймати на себе зайві ризики. Вони мають бути обачними і переконатися, що їхні програми включають активний захист усіх

об'єктів, заснований на підході, що базується на розвідці. Це забезпечить швидкий аналіз першопричин та належне реагування на кіберзагрози, що мінімізує середній час відновлення після будь-яких інцидентів.

Відмінність активного та пасивного захисту полягає у тому, що ефективна програма активного захисту кібербезпеки вимагає постійного моніторингу з боку людей, які можуть розпізнавати та реагувати на складні кібератаки. Розвідка надає їм контекст і відповідні рекомендації щодо дій для кожної загрози. Це часто вимагає від організацій додаткових інвестицій в технології, людей і процеси [].

2.4 Моделі розслідування вторгнень

2.4.1 Ланцюг кіберзахисту від Lockheed Martin

Ця перевірена часом модель існує найдовше, і фахівці з кібербезпеки та розробники програмного забезпечення часто посилаються на неї. Вперше вона була опублікована в 2011 році, модель, показана нижче, описує сім кроків, які зловмисник робить під час вторгнення: розвідка, озброєння, доставка, експлуатація, встановлення, командування та управління, дії по досягненню цілей.

Це ефективна модель, оскільки вона авторитетно описує типові кроки зловмисника. Крім того, ця модель увібрала в себе анекдотичну мудрість тисяч експертів у цій галузі і стандартизувала значну частину лексики, що використовується в цій галузі.

Ланцюг кіберзахисту від Lockheed Martin є досить лінійним у своєму підході, що може бути перевагою. Фахівці з кібербезпеки часто опиняються в ситуації невизначеності і можливість більш конкретно вивчити певний крок часто вітається. Однак ця лінійність може бути і проблемою, оскільки вона може призвести до того, що фахівці з кібербезпеки будуть спрощувати ситуації або робити швидкі висновки.

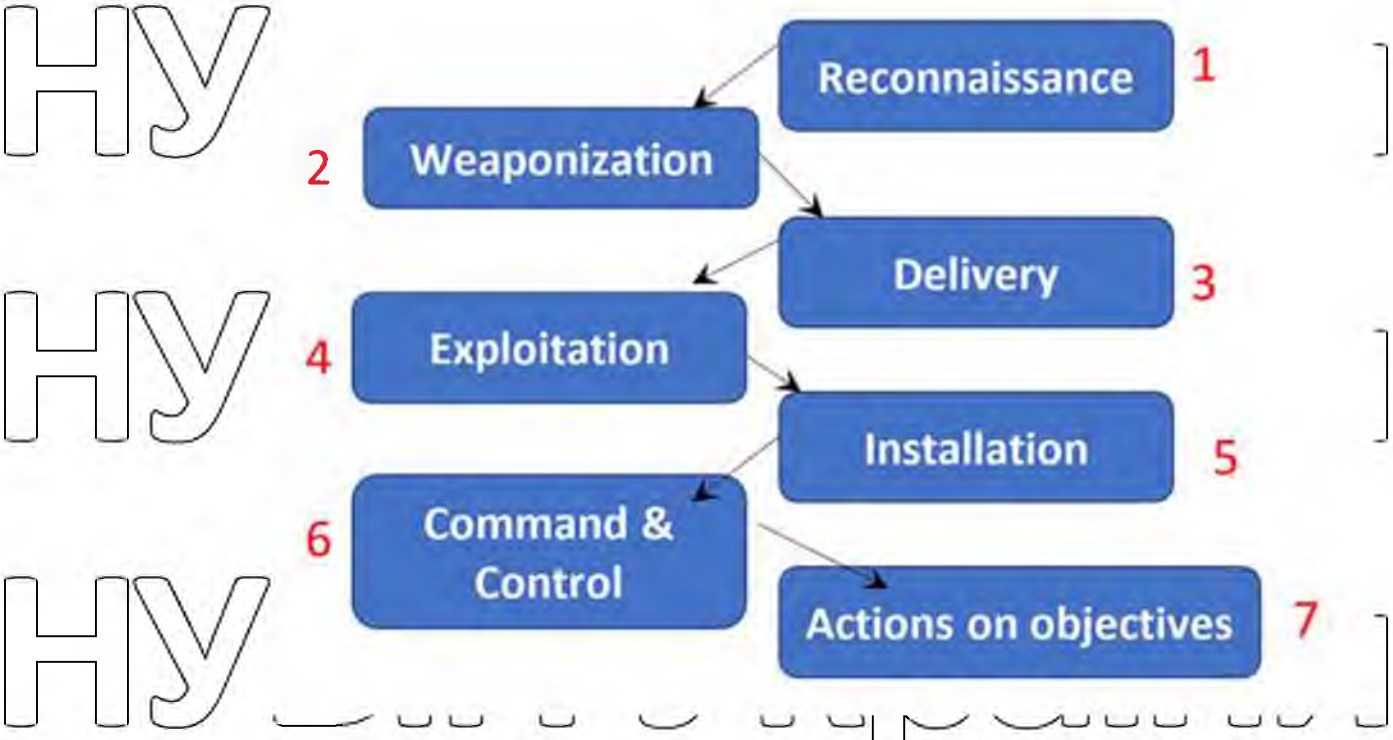


Рисунок 2.6 – Ланцюг кіберзахисту компанії Lockheed-Martin

2.4.2 Діамантова модель аналізу вторгнень

Фахівці у сфері кіберзахисту Серджіо Кальтаджироне, Ендрю Пендергаст і Крістофер Бец вважають, що лінійні моделі аналізу вторгнень мають кілька недоліків. Вони хотіли зосередитись на конкретній поведінці хакерів і створити модель, яка б дозволила фахівцям з кібербезпеки визначити взаємозв'язок між мотивацією зловмисника, жертвою і технологією, яка використовується для здійснення атаки. Вони вперше сформулювали діамантову модель в 2006 році і пізніше опублікували її в 2013 році. У цій моделі кожна подія, наприклад, вторгнення, представлена діамантом.

Як і діамант, подія має чотири квадранти, і кожен квадрант описує основні характеристики:

а) Противник: Особа або група осіб, що атакує вас

б) Інфраструктура: IP-адреси, доменні імена або адреси електронної пошти

в) Можливості: Що може зробити противник (наприклад, шкідливе програмне забезпечення, експлойти, маніпулювання інфраструктурою)

г) Жертва: Може включати людей, сервіси, мережеві активи або інформацію

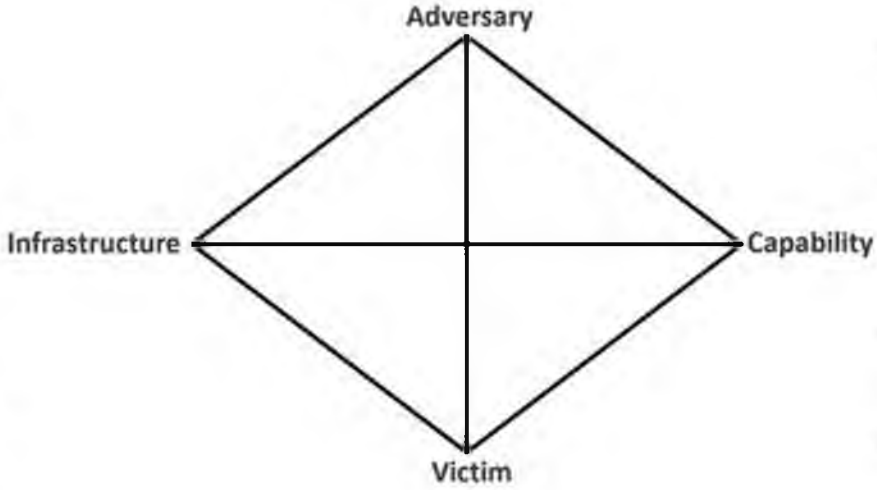


Рисунок 2.7 – Діамантова модель аналізу вторгнень

Ідея цієї моделі полягає в тому, щоб дуже детально розглянути відносини між супротивником (хакером) і жертвою. Найголовніше, що творці Діамантової моделі хотіли отримати способи ідентифікації активності «при розвороті», в момент атаки, коли хакер змінює тактику вторгнення в систему. Коли хакер розвертається, він визначає шляхи атаки на певне середовище, яке найменш захищене. Повороти можуть створювати багато шуму - і діамантова модель може дозволити людям і машинам ідентифікувати та оцінювати цей шум для визначення подальших намірів.

Виявити поворотні точки хакерських атак важко, але можливо - якщо зосередитись на взаємозв'язках між супротивником, інфраструктурою, можливостями і жертвою.

Основна перевага діамантової моделі полягає в тому, що вона дозволяє людям - і програмам штучного інтелекту - визначати, коли хакер переорієнтовується. Вона також дозволяє аналітику з кібербезпеки робити те, що називається аналітичним поворотом, коли аналітик визначає взаємозв'язок між методами атаки. Акцент робиться не стільки на самих компонентах, скільки на взаємозв'язку між цими компонентами.

Використовуючи діамантову модель, можна зв'язати воєдино кілька подій - або діамантів - і створити групу активності. Це дозволяє відстежувати кроки атаки протягом усієї кампанії злому системи.

Одним з результатів застосування діамантової моделі є те, що вона допомогла перетворити діяльність з виявлення вторгнень з мистецтва на науку - де цій діяльності можна навчатись і надалі відтворювати. Також ця модель дозволила розробникам програмного забезпечення застосувати штучний інтелект до діяльності з виявлення вторгнень.

2.4.3 Поєднання ланцюга кіберзахисту та діамантової моделі

Розробники діамантової моделі зіставили її з кібернетичним ланцюгом кібератак, назвавши їх такими, що значно доповнюють одна одну. Поєднання цих двох моделей можна зобразити у вигляді атак, як показано нижче

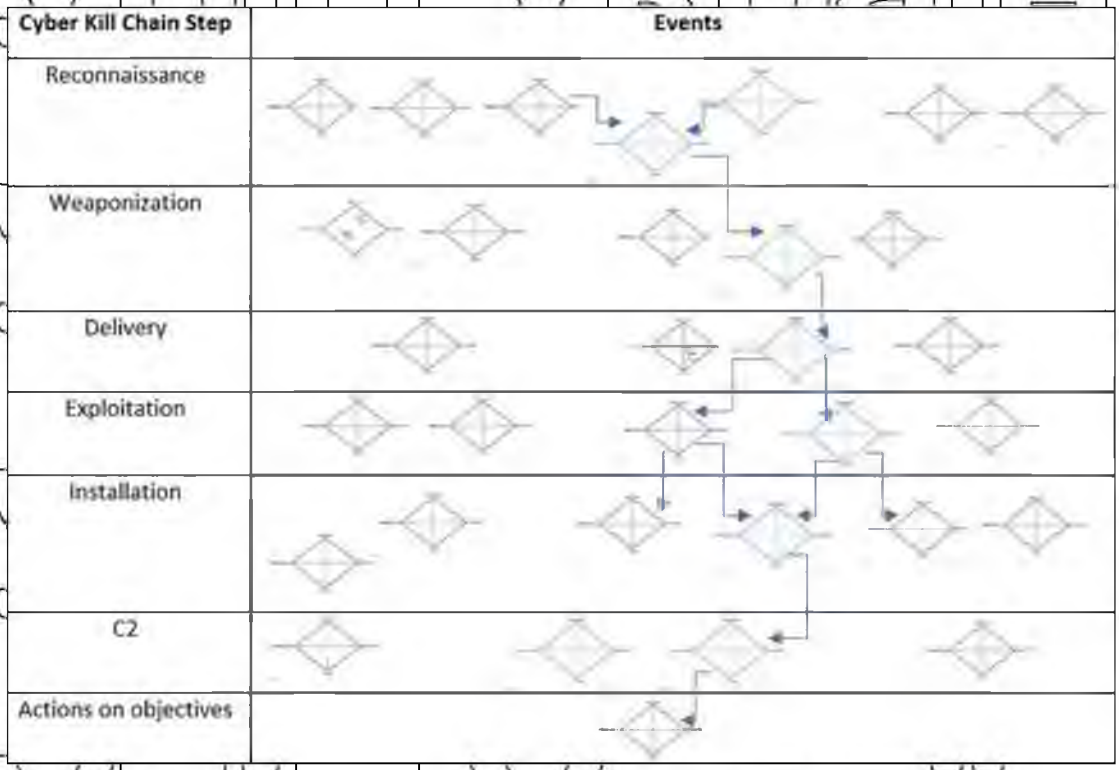


Рисунок 2.8 – Поєднання ланцюга кіберзахисту та діамантової моделі

За допомогою даної діаграми на прикладі конкретної атаки можна переглядати серії невдалих подій - і поворотних точок через поєднання ланцюга кіберзахисту та діамантової моделі. Графік атаки дозволяє аналітику з кібербезпеки ідентифікувати не лише кожен крок ланцюга кібератак, але й окремі ключові моменти, які хакер виконує в рамках цих кроків. Результатом є набагато більш

багате і нюансоване розуміння аналізу вторгнень, і цей підхід ліг в основу більшості інструментів виявлення вторгнень і SIEM, які існують на сьогоднішній день.

На графіку атаки вище показано кілька ключових точок: перша в області розвідки і друга в розділі установки. Схоже, що зловмисник розглядав кілька різних тактик, але вибрав область, яка могла включати певну вразливість (застарілі патчі), використання встановленого інструменту (PowerShell) або певного середовища розробки (Python). Творці діамантової моделі стверджують, що застосування їхнього підходу до лінійної моделі, такої як ланцюга кіберзахисту, дозволяє як програмному забезпеченню, так і захисникам отримати краще розуміння вторгнення.

2.4.4 Модель MITRE ATT&CK

Модель Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) стала надзвичайно популярною за останні п'ять років і зустрічається в програмному забезпеченні практично усюди. Багато додатків посилаються на неї як на фактичний стандарт для визначення етапів життєвого циклу атаки.

Згідно з моделлю MITRE, хакери здійснюють наступні кроки: початковий доступ, виконання, збереження, ескалація привілеїв, ухилення від захисту, обліковий доступ, виявлення, бічний рух, збереження, командування і контроль. Зазвичай MITRE розглядає кроки хакерів у більш широкому контексті.

Як можна бачити, навігатор MITRE ATT&CK Navigator робить більше, ніж просто перераховує кілька кроків. Він прив'язує конкретні тактики і процедури до кожного кроку. За допомогою MITRE ATT&CK Navigator можна зіставити конкретні тактики і процедури з реальними групами загроз, визначивши загальні методи і процедури, які зловмисники можуть використовувати, коли вони націлені на компанію.

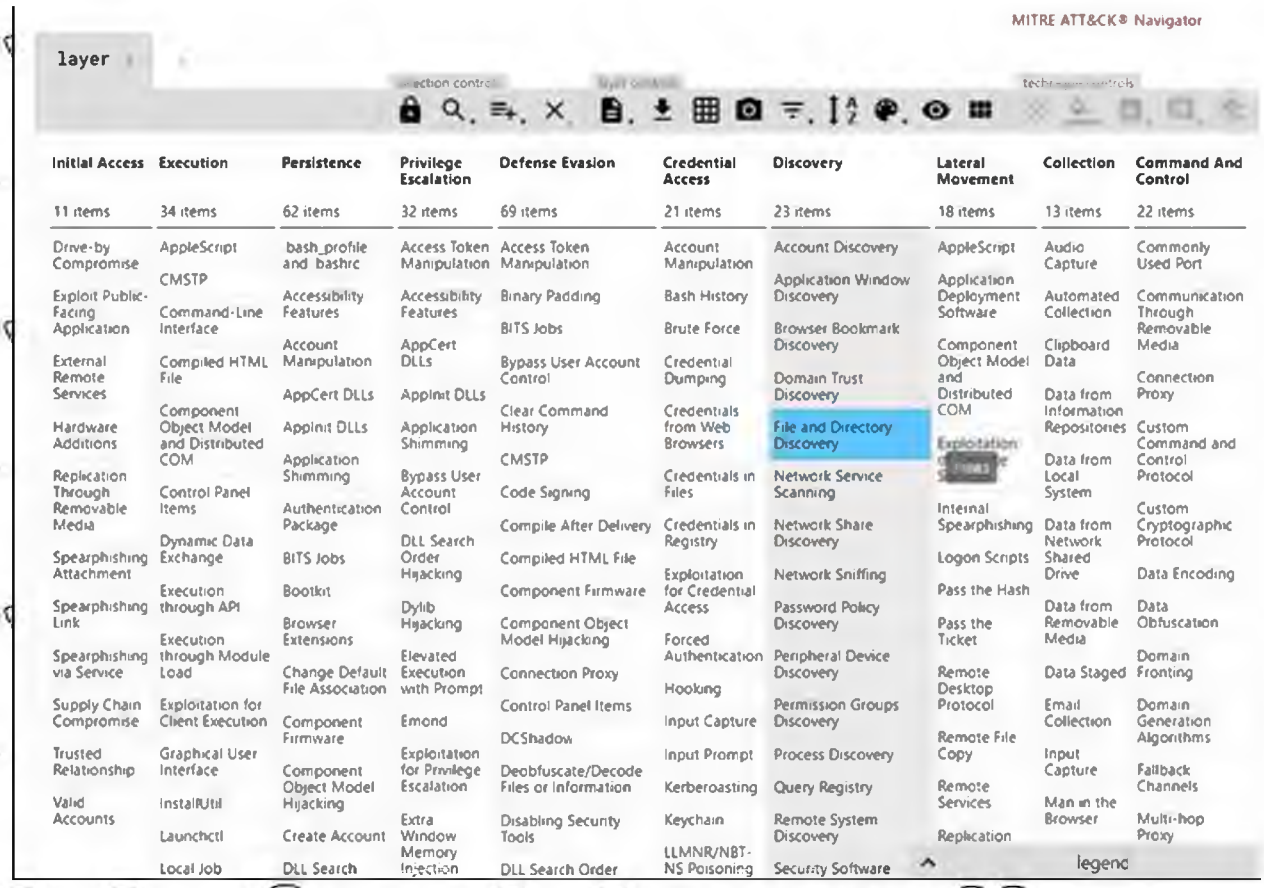


Рисунок 2.9 – Навігатор MITRE ATT&CK Navigator

В даному випадку виділено виявлення файлів і каталогів як можливу процедуру, до якої може вдатися зловмисник. Таким чином, можна почати прогнозувати, як саме зловмисник буде це робити, забезпечуючи цінну стратегію запобігання. Цікаво спостерігати, як MITRE не лише зіставив ідею життєвого циклу атаки з поширеними технологіями, які використовують потенційні жертви, але також MITRE вносить незначні зміни до структури атаки в різний час [4].

2.5 Моделі, що застосовуються у навчальних закладах

На практиці, для проактивного захисту інформації найчастіше компанії не здатні інвестувати достатньо ресурсів, або не бачать в цьому потреби. Стосується це не лише обладнання, але і кваліфікованих кадрів. Виражається дана проблема в

тому, що ті фахівці з кібербезпеки, що працюють в такій компанії, не мають змоги захистити мережу перевіреними рішеннями відповідно до вимог часу, та змушені постійно шукати діючі методи захисту даних без необхідності великих вкладень. Через що, часто захист корпоративних мереж займає місце між моделями «льодяника» та «цибулини», маючи більше ніж один рівень захисту, але менше, ніж цього вимагають реалії. Часто мережі навчальних закладів також потерпають від недостатнього інвестування.

Такі мережі, зазвичай, не мають налаштувань відмово стійкості компонентів, що є дуже важливим для стабільної роботи. Через високу вартість фаєрволів, систем запобігання вторгненню, систем аналізу трафіку, зазвичай їх роботу виконують маршрутизатори з налаштованими ACL-списками фільтрації трафіку. Однак маршрутизатори часто нездатні глибоко аналізувати трафік, через що є захист від запитів з відомих небезпечних доменів, однак відсутній захист від вірусів. Також на маршрутизаторах налаштовують блокування портів, що не використовуються та адрес, з яких надходить надмірна кількість трафіку, що може свідчити про початок атаки «відмова в обслуговуванні» [8].

На рівні ядра мережі також часто відсутнє резервування комутаторів 3 рівня, через що трафік з різних мереж проходить через один комутатор та при його відмові не можна буде не лише обмінюватися даними з мережею Інтернет, а і отримати доступ до локальних ресурсів (корпоративної пошти, файлового сервера, внутрішніх веб-ресурсів).

Мережеві пристрої рівня доступу найменш потерпають від проблем нестачі вкладень, однак також відчувають його вплив. Так, в 2022 переважна частина комп'ютерів користувачів випускаються з мережевими адаптерами, що підтримують швидкість 1 Гбіт/с, однак часто комутатори, до яких вони під'єднуються мають на LAN-портах швидкість 100 Мбіт/с, що не відповідає сучасним вимогам [9].

Wi-Fi мережі в навчальних закладах часто використовують застарілі протоколи передачі даних g/n та вже втрачаючий актуальність протокол ac, через що швидкість доступу до інформації лишає бажати кращого, а користувачі

починають користуватися мобільним інтернетом та вмикають точки роздачі Wi-Fi, тим самим забиваючи доступні канали та ще більше зменшуючи швидкість передачі даних по бездротовій мережі і радіус дії точок доступу.

Що ж стосується мережевого сховища, то часто воно будується на базі не призначених до цього серверів, що не тільки не можуть надати необхідну продуктивність при читанні/запису інформації, але і не мають резервування дискового контролера, що створює небезпеки втрати інформації.

2.6 Шляхи поліпшення захисту інформації у навчальному закладі

Модель «цибулини» показує, що чим більше шарів захисту мають дані, тим зловмиснику складніше викрасти дані з неї. Через що експерти рекомендують будувати мережу з декількома рівнями апаратного та програмного захисту.

Окрім маршрутизаторів в мережі обов'язково мають бути фаєрволи, система розпізнавання вторгнень та глибокого аналізу трафіку, а також локальний захист кожного пристрою від атак на 2 та 3 рівнях моделі OSI [10].

Дуже важливою частиною захищеної мережі є резервування пристроїв. Це запобігає не лише втраті доступу до ресурсів при виході з ладу певного мережевого пристрою, але і при атаці на відмову обслуговування [11]. Також важливим є підключення ключових пристроїв мережі (маршрутизаторів, фаєрволів та інших систем захисту, комутаторів ядра та серверів) до джерел безперебійного живлення та дизельних/бензинових генераторів, що здатні живити мережу струмом навіть при відключенні централізованого електропостачання [12].

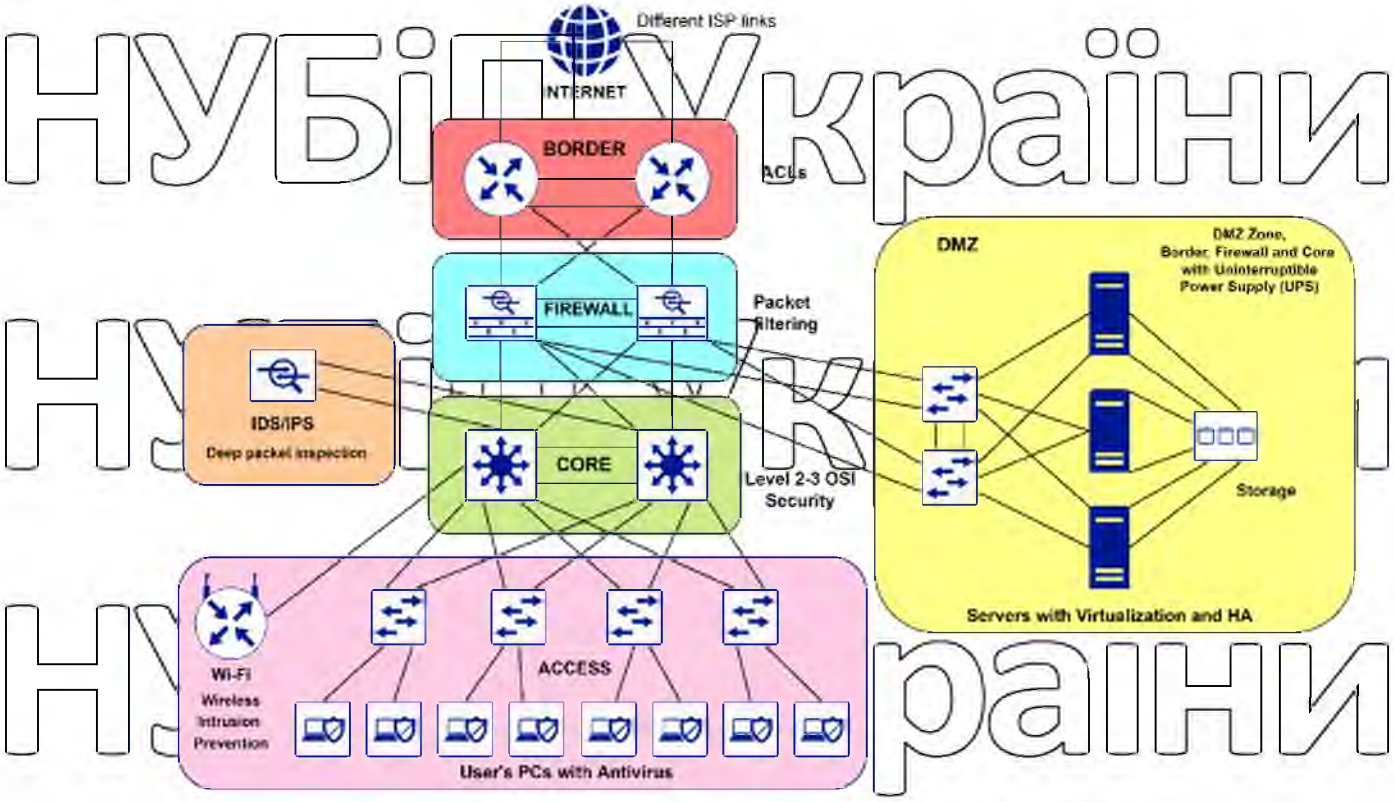


Рисунок 2.10 – Захищена локальна мережа

Не менш важливим є підключення маршрутизаторів до різних провайдерів або одного провайдера, але з різними точками підключення. При відмові одного з лінків, мережа все ще матиме змогу функціонувати через другий канал підключення [13].

3 ПОБУДОВА МОДЕЛІ ЗАХИЩЕНОЇ МЕРЕЖІ В НАВЧАЛЬНОМУ ЗАКЛАДІ

3.1 Створення середовища для моделювання мережі

Для моделювання мережі навчального закладу треба спершу створити середовище для цього. В якості бази була обрана платформа VmWare Workstation, встановлена на комп'ютер під керуванням ОС Windows 10. Сам комп'ютер побудований на базі серверного процесора Intel Xeon E5 1650 та має встановлену пам'ять ОЗП об'ємом 32 Гб, що достатньо для операцій зі створення віртуальних машин та моделювання роботи систем.

Після встановлення VmWare Worksation слід створити віртуальні машини, на яких буде розгорнена система для моделювання. Загалом було створено 3 віртуальні машини, з них 2 – під керуванням ОС Proxmox VE, що виступає гіпервізором для розгортання на ньому інших віртуальних машин. На третю ВМ було встановлено Ubuntu Server та додаток для моделювання мереж EVE-NG. Для створення віртуальної машини обираємо кастомізоване створення в налаштуваннях.

Рисунок 3.1 – Створення віртуальної машини

Далі слід обрати образ операційної системи для встановлення, вказати об'єм оперативної пам'яті, кількість ядер процесора та об'єм диску для ВМ.

Рисунок 3.2 – Параметри віртуальної машини

Далі в налаштуваннях створеної віртуальної машини слід змінити налаштування мережі на «міст», щоб віртуальна машина мала свою адресу в мережі.

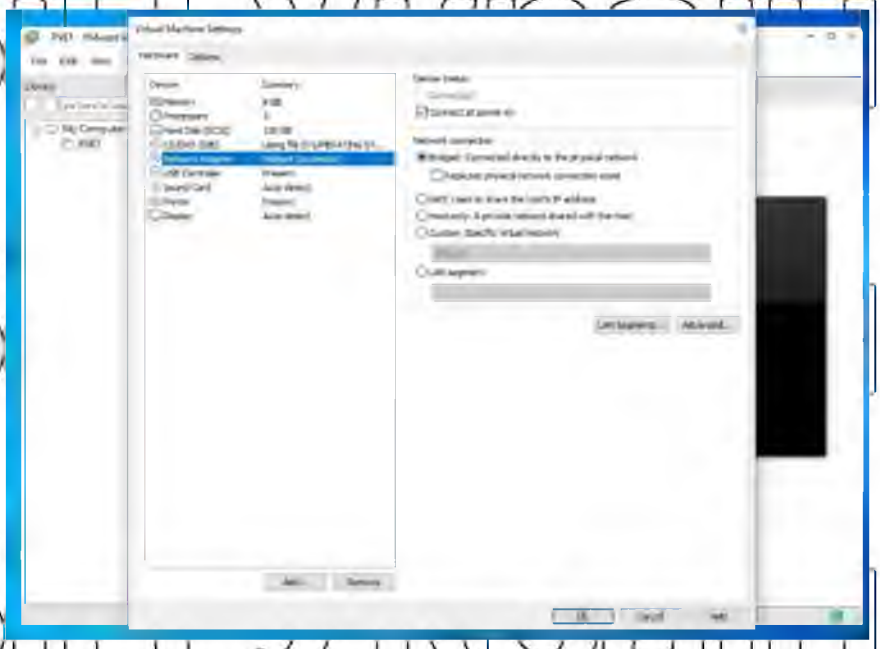


Рисунок 3.3 – Зміна мережевих налаштувань

Окрім цього, слід в налаштуваннях процесора вказати підтримку віртуалізації, для можливості створення віртуальних машин у віртуальній машині.

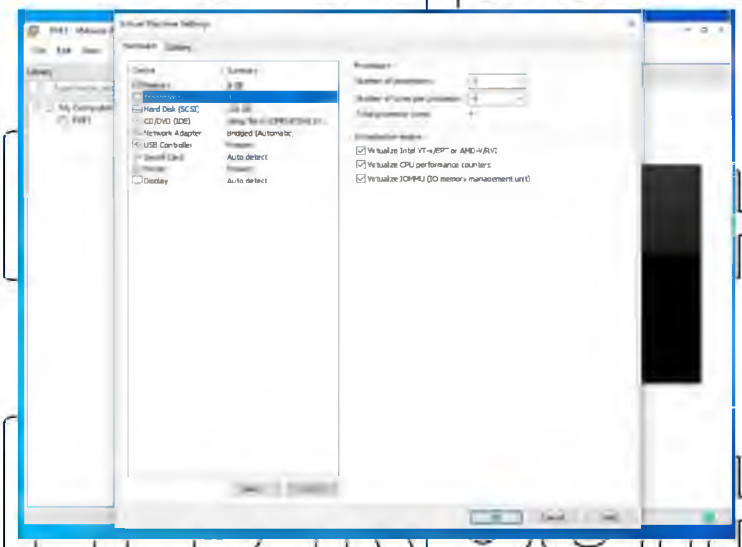


Рисунок 3.4 – Зміна налаштувань процесора

3.1.1 Створення двох ВМ під керуванням ОС Proxmox VE

Після здійснення даних маніпуляцій запускаємо віртуальну машину, де проводимо налаштування її операційної системи. В якості ОС була обрана система віртуалізації з відкритим кодом Proxmox Virtual Environment [14].

Рисунок 3.5 – Вибір диску, на який буде встановлена ОС

Під час встановлення гіпервізора Proxmox VE слід обрати, на який диск буде встановлена система, часовий пояс та ввести дані користувача.

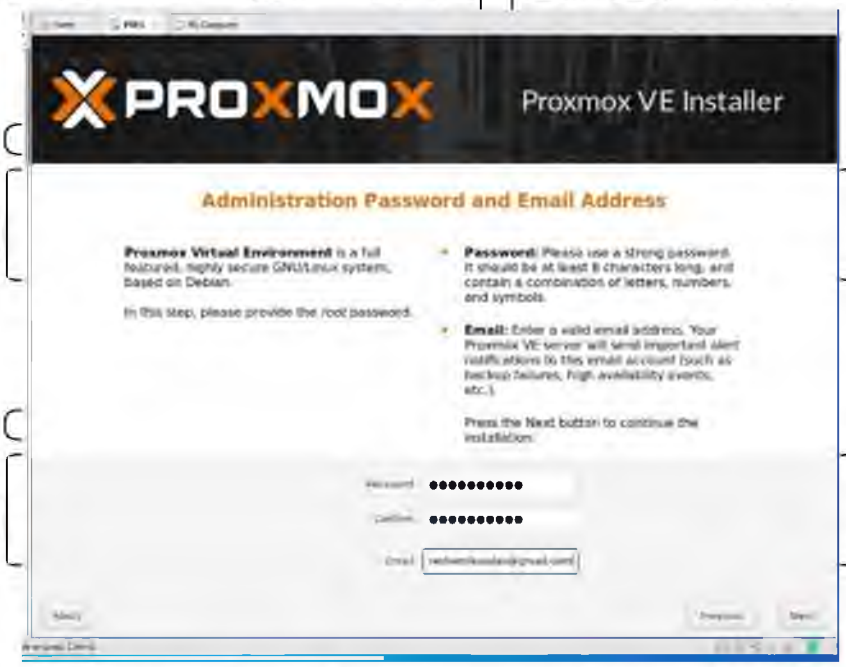


Рисунок 3.6 – Введення пароля користувача

Особливо важливим кроком є мережеві налаштування, оскільки через обрану IP-адресу далі треба буде підключатися до сервера.

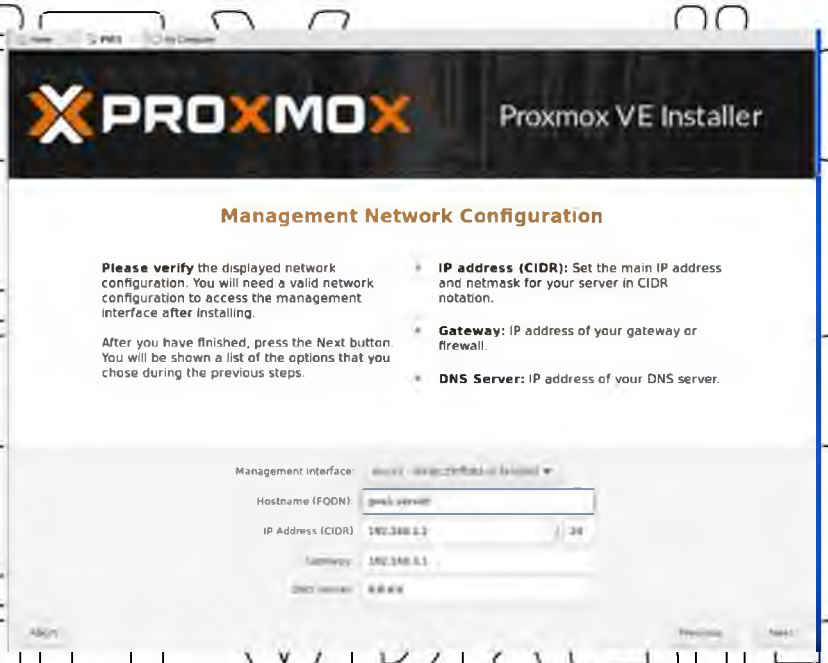


Рисунок 3.7 – Введення IP-адреси для ВМ

На останньому етапі встановлення ОС перед користувачем з'являється вікно з основними налаштуваннями, які було здійснено.

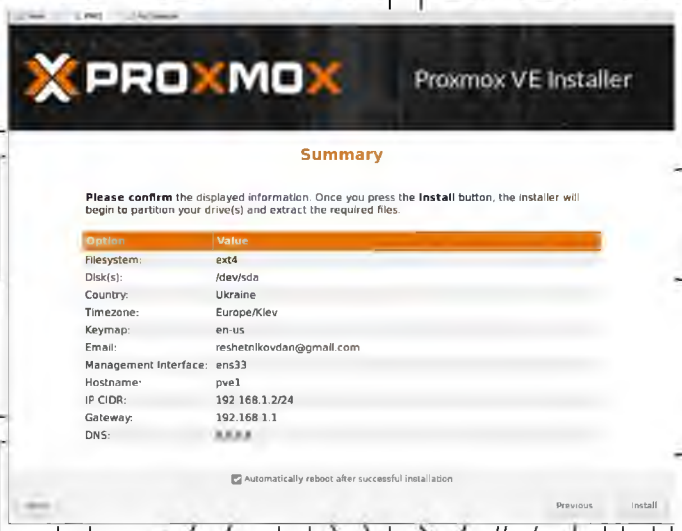


Рисунок 3.8 – Основні параметри ОС Proxmox VE

Після цього буде запущено процес встановлення ОС на диск, за результатами якого віртуальну машину буде перезавантажено.

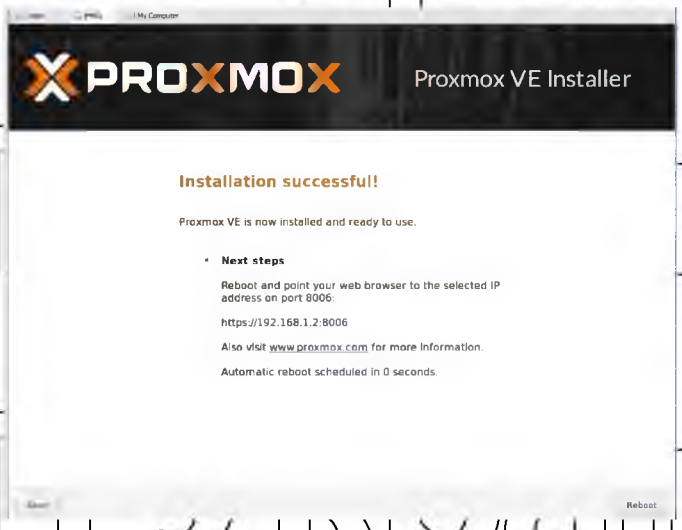


Рисунок 3.9 – Вікно успішного встановлення ОС

Після перезавантаження перед користувачем з'явиться відповідне вікно з IP-адресою, на яку треба перейти з браузера на іншому пристрої для подальшого керування сервером.

Рисунок 3.10 – Запуск віртуальної машини зі встановленим гіпервізором Proxmox

Після встановлення гіпервізора Proxmox слід ввести IP-адресу сервера у пошуковій стрічці браузера. Відкриється вікно авторизації.

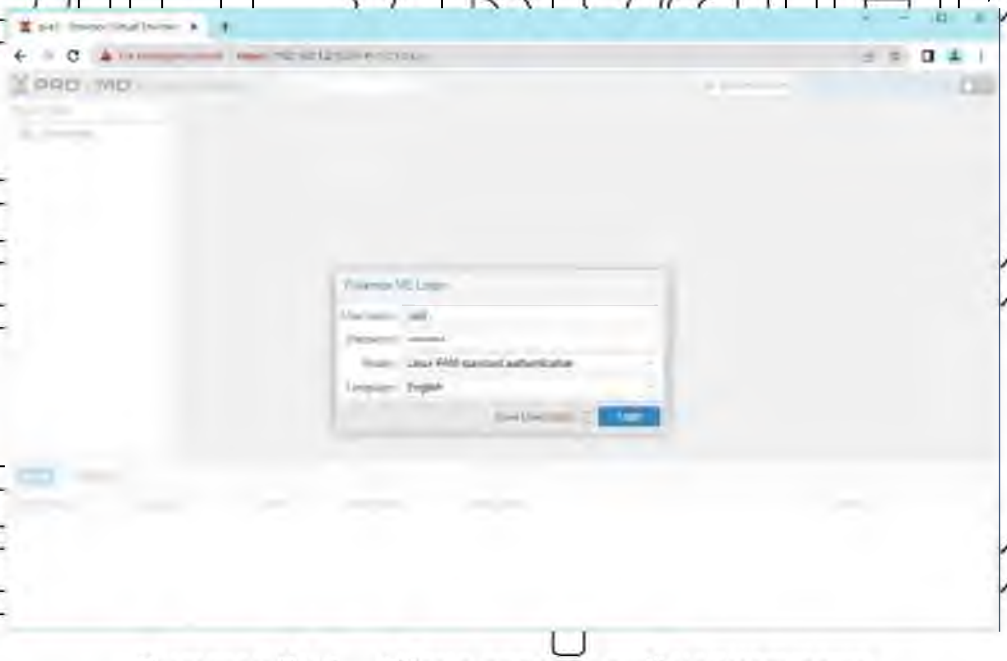


Рисунок 3.11 – Вікно авторизації користувача

Після авторизації перед користувачем з'являється вікно, де показаний стан ресурсів сервера.

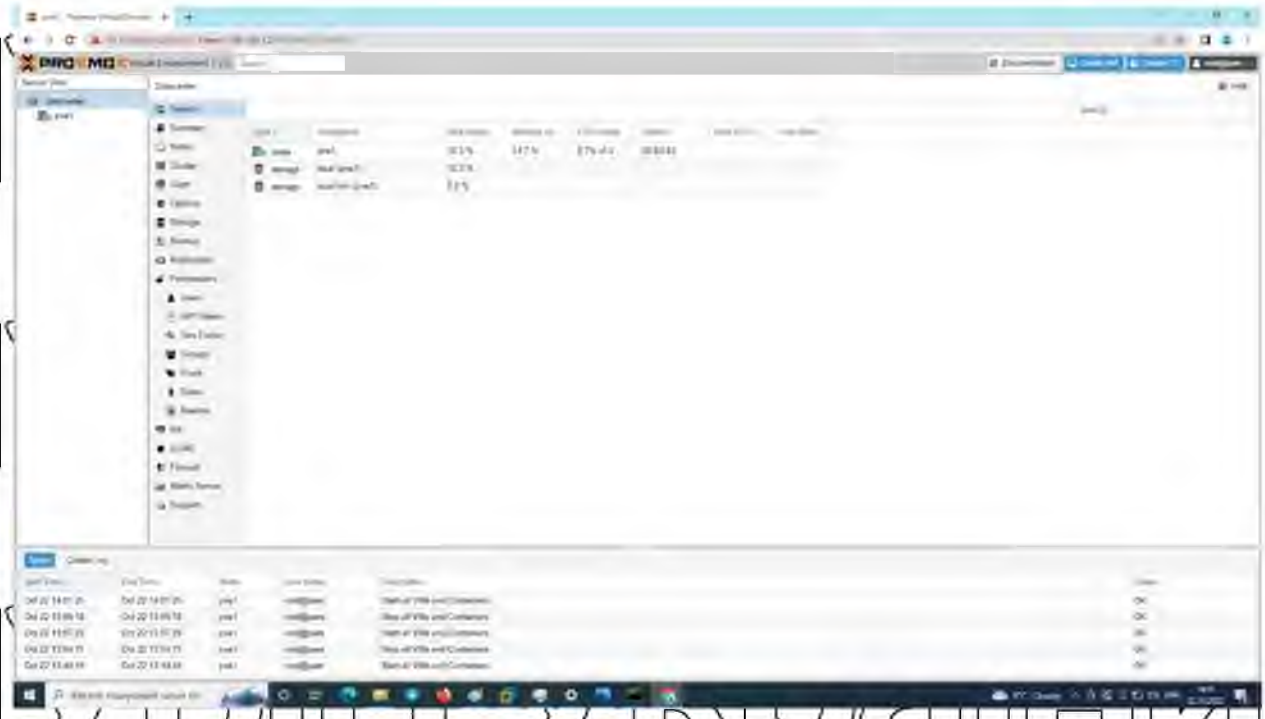


Рисунок 3.12 – Наявні ресурси сервера

На цьому робота з сервером PVE1 тимчасово припиняється. За там же шаблоном створюємо другу віртуальну машину PVE2, де виконуємо аналогічні налаштування. Єдиною відмінністю є різні мережеві налаштування. Серверу PVE2 присвоюємо іншу IP-адресу.

Рисунок 3.13 – Мережеві налаштування сервера PVE2

Всі інші параметри залишаються незмінними. Їх можна переглянути у вкладці «Summary» після встановлення гіпервізора Proxmox VE.

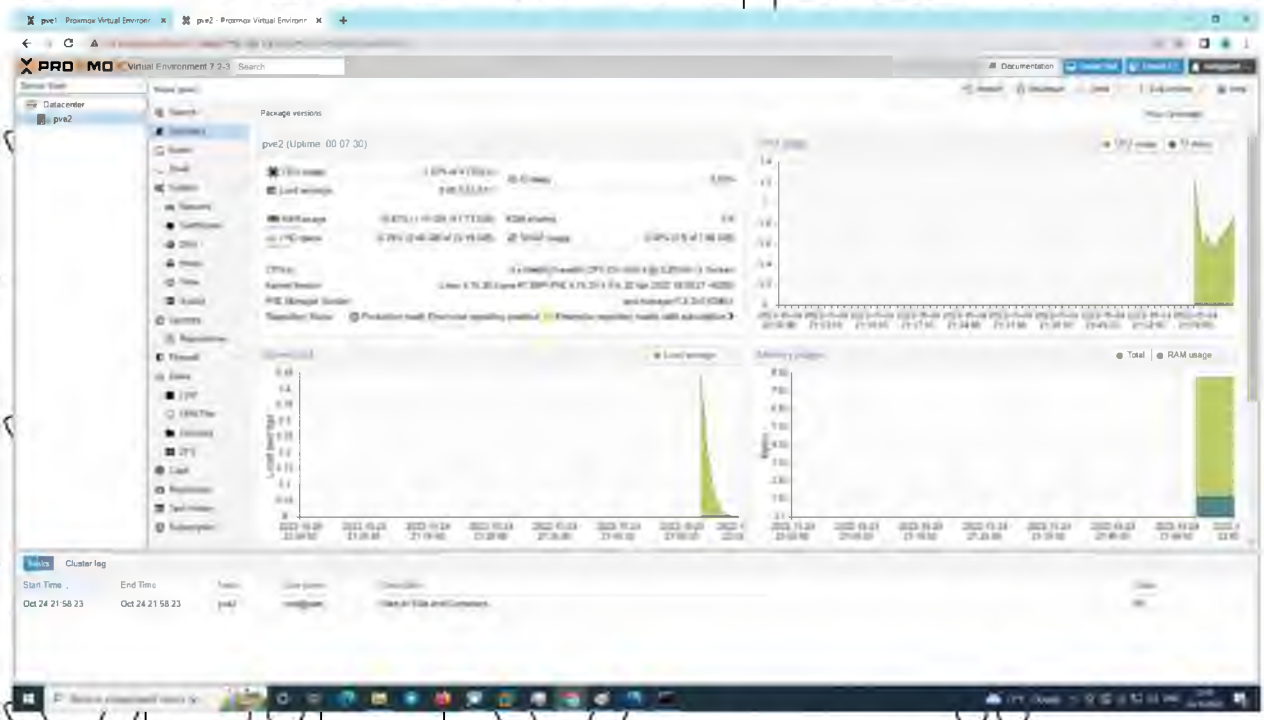


Рисунок 3.14 – Параметри сервера PVE2

3.1.2 Створення ВМ для додатку EVE-NG

Для моделювання самих мережевих пристроїв використовується додаток EVE-NG, який необхідно встановити на систему під керуванням Ubuntu Linux. EVE-NG — це перше без клієнтське програмне забезпечення для емуляції мережевих пристроїв від багатьох постачальників [15].

Процес створення віртуальної машини для подальшого встановлення додатку для моделювання безпосередньо мережі EVE-NG практично не відрізняється від попереднього створення віртуальних машин за винятком надання меншої кількості ресурсів даній машині. Тут було обрано надати віртуальній машині 2 ядра процесора та 4 Гб оперативної пам'яті, 50 Гб дискового простору. Мережеві налаштування – аналогічні до інших віртуальних машин – встановлення віртуального інтерфейсу у режим роботи типу «міст».

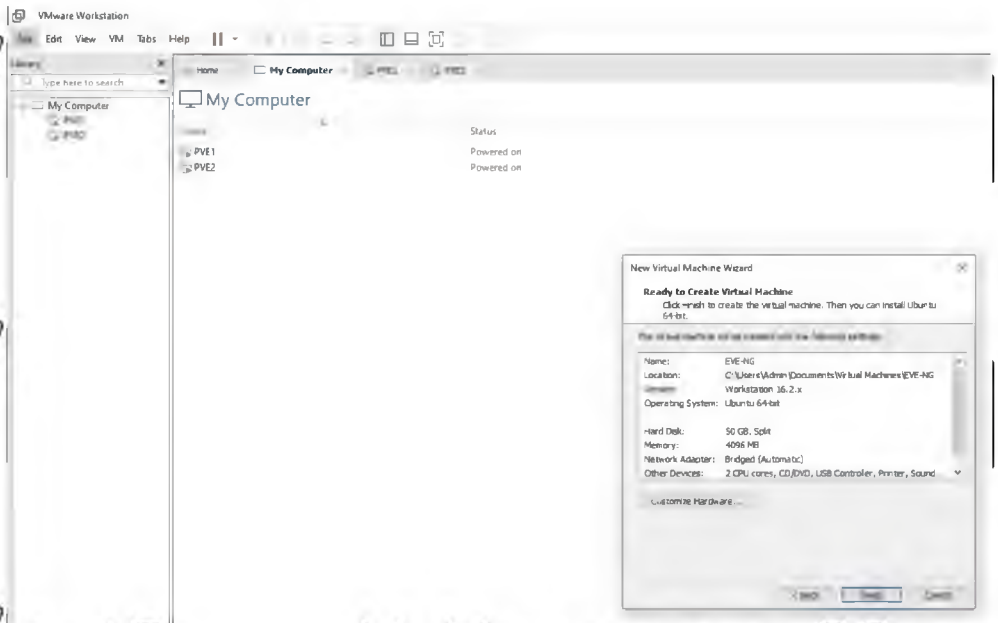


Рисунок 3.15 – Характеристики ВМ для додатку EVE-NG

Також замість створення нового віртуального диску було обрано попередньо створений віртуального диску з вже встановленою системою, що можна завантажити з сайту EVE-NG.

Рисунок 3.16 – Додавання іншого віртуального диску до ВМ

Сама операційна системи вже була встановлена на віртуальному диску. В якості ОС виступає Ubuntu Server. Сам процес налаштування ОС також схожий зі встановленням Proxmox VE, однак дещо відрізняється.

Після першого запуску нової створеної віртуальної машини перед користувачем з'являється меню налаштувань ОС.

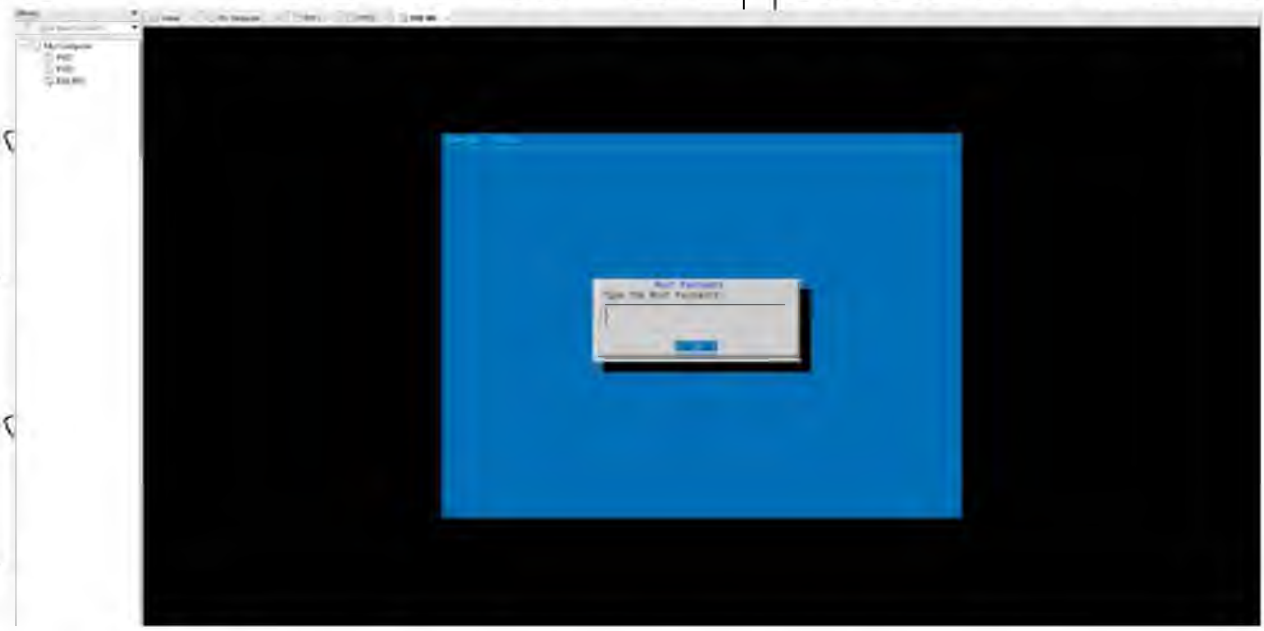


Рисунок 3.17 – Введення паролю супер-користувача

Окрім авторизаційних даних слід також ввести дані мережі – тип адреси (динамічна чи статична), а також адреси маршрутизатора та DNS-серверів.

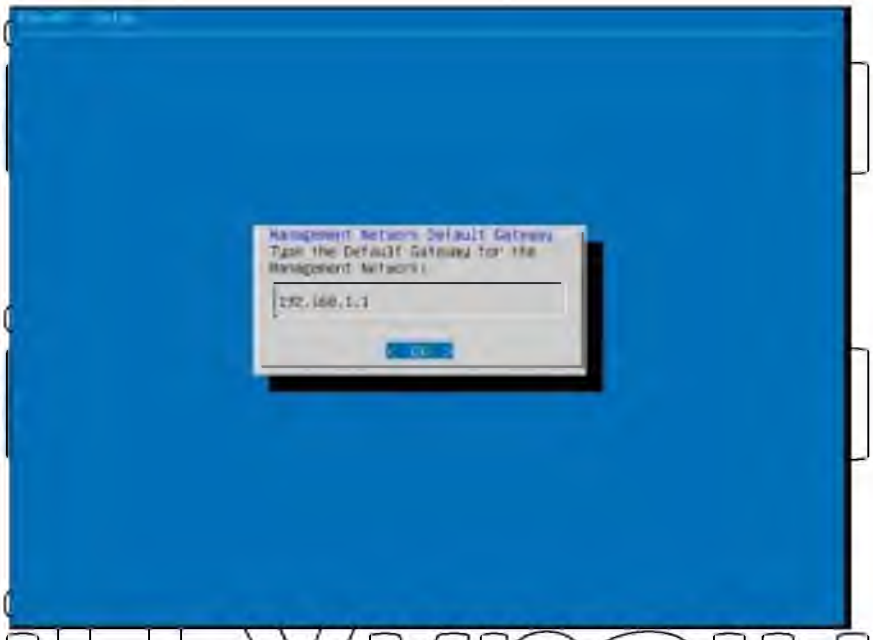


Рисунок 3.18 – Введення IP-адреси маршрутизатора

Після введення всіх налаштувань віртуальна машина перезавантажиться та перед користувачем відкриється вікно з IP-адресою, на яку треба переходити через браузер для подальшої роботи з платформою EVE-NG.

Рисунок 3.19 – Підключення до платформи EVE-NG

Після успішної авторизації перед користувачем відкривається вікно файлового менеджера. Тут створюємо новий файл лабораторної роботи і відкриваємо його.

Тут крім емульованих ПК з командним рядком нічого додати не виходить, інші об ‘єкти неактивні. Додаємо емульовані ПК та перевіряємо працездатність системи, присвоюємо їм IP-адреси та застосовуємо команду ping для перевірки правильності налаштувань. Пакети надходять до адресатів і успішно повертаються назад, отже зв’язок налаштовано правильно.

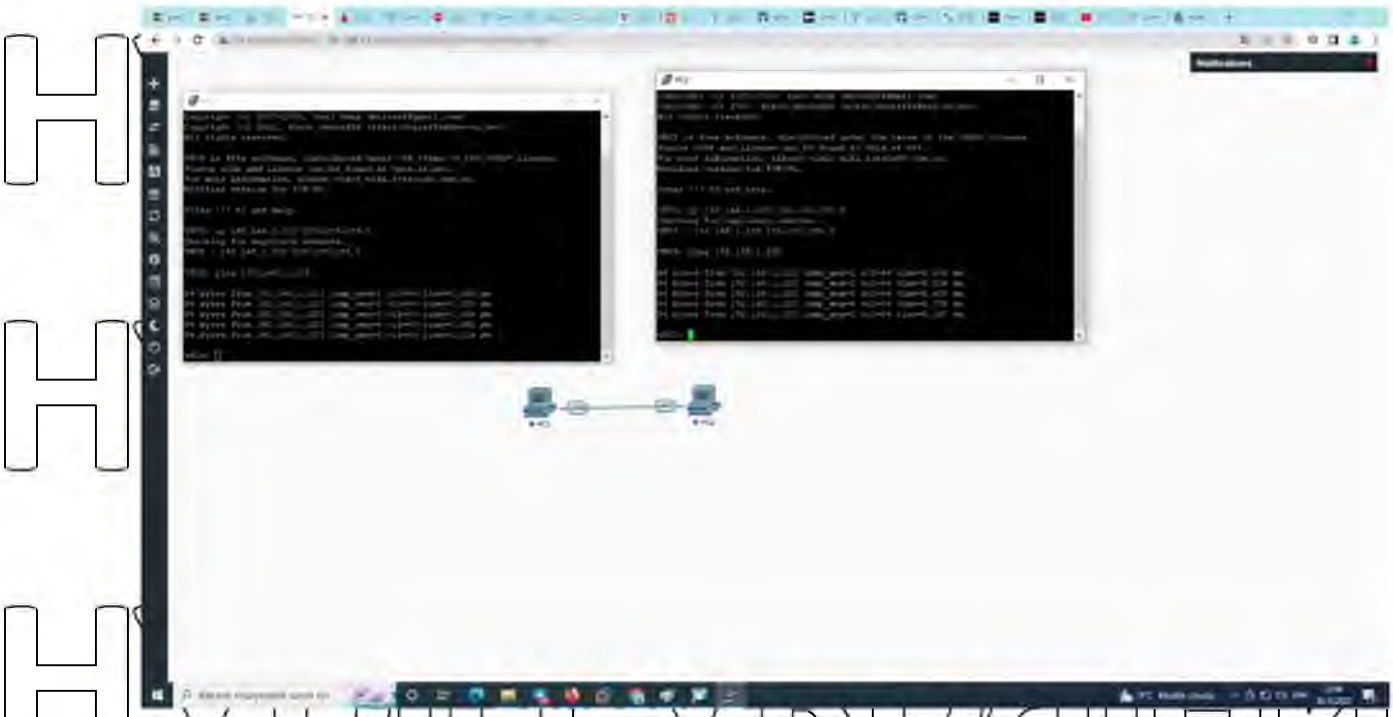


Рисунок 3.20 – Додавання об’єктів на поле роботи

Для того, щоб мати можливість на поле роботи додавати інші об’єкти слід образи їхніх операційних систем завантажити у відповідні теки на віртуальній машині. Аби зробити це слід завантажити FTP-клієнт, через який можна буде здійснювати доступ до файлової системи віртуальної машини [16].

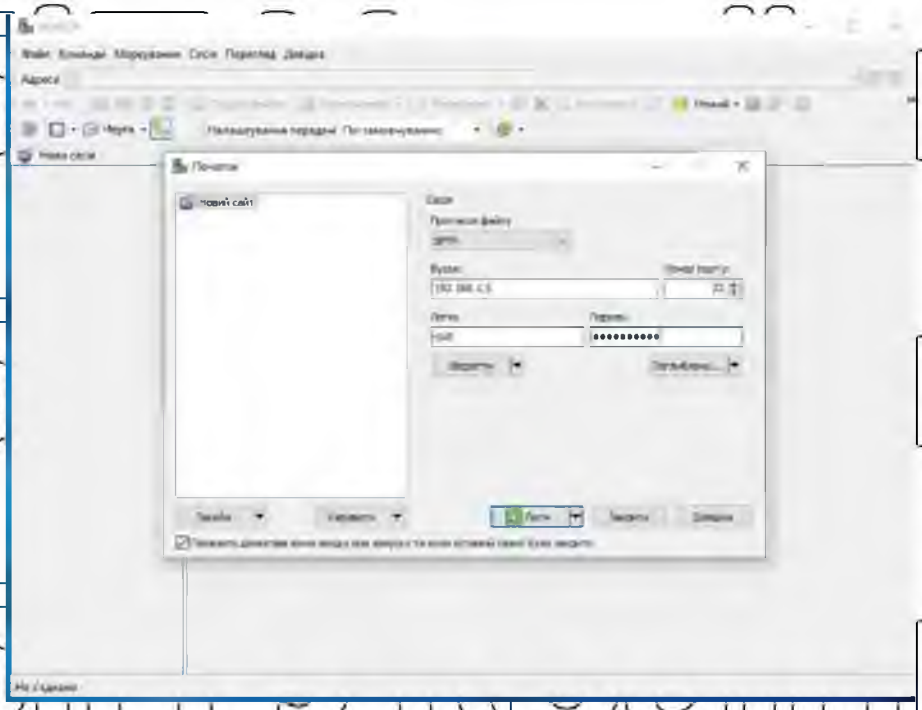


Рисунок 3.21 – Підключення до файлової системи ВМ

Після отримання доступу слід перейти у відповідні папки для IOS/IOL образів, та завантажити образи операційних систем пристроїв.

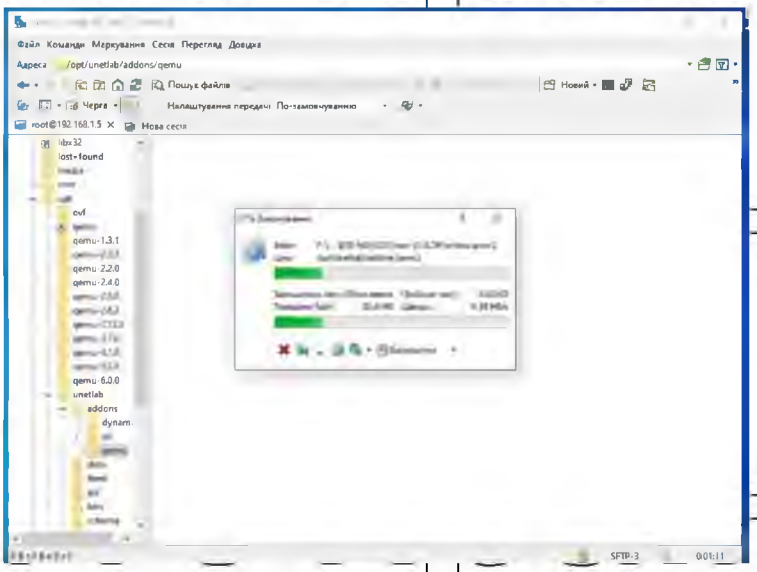


Рисунок 3.22 – Завантаження образів пристроїв

Після завантаження образів пристроїв слід додати скрипт для їх активації та запустити файл на його виконання, а результат зберегти у новий файл.

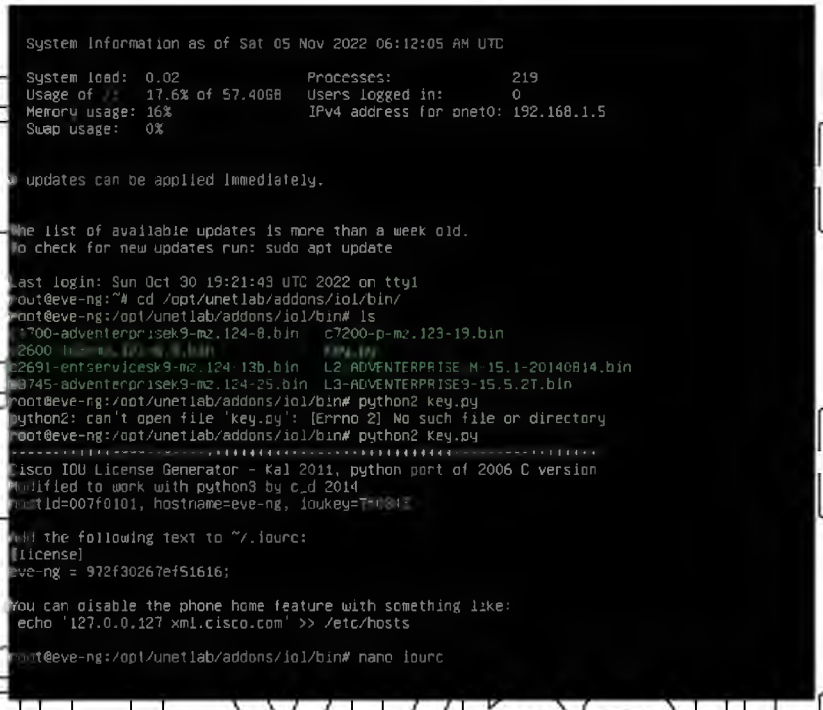


Рисунок 3.23 – Активація образів пристроїв

Окрім вищеназваних дій слід зробити файли образів пристроїв виконуваними. Після цього слід перейти у веб-сторінку системи EVE-NG, та відкрити файл з роботою.

Рисунок 3.24 – Додавання пристроїв до роботи

Після вибору необхідного пристрою тепер можна переглянути та змінити його характеристики. На цьому налаштування віртуальної машини для моделювання мережі завершено, саме моделювання буде розглянуто далі.

Рисунок 3.25 – Зміна параметрів пристроїв

3.2 Побудова моделі мережевого комплексу навчального закладу

3.2.1 Створення віртуальних машин

На сьогоднішній день для організацій, що не володіють великими фінансовими можливостями є популярним рішення віддалених робочих столів. В даному випадку немає потреби закуповувати потужні робочі комп'ютери для кожного користувача, а можна обійтись купівлею декількох потужних серверів та необхідної кількості тонких клієнтів – ПК зі слабкими характеристиками, основною задачею яких є підключення до віртуальних машин на сервері. Це дозволяє економити і ресурси енергоспоживання, оскільки доволі рідко всі машини будуть мати навантаження у 100%, а отже і потужності сервера можуть бути меншими, ніж при відповідній потужності та кількості звичайних стаціонарних ПК.

В даному випадку для роботи студентів були створені віртуальні машини на базі ОС Kali Linux, що дозволяє проводити навчання з кібербезпеки.

Першим кроком до створення віртуальних машин на базі гіпервізора Proxmox VE є завантаження на дисковий простір гіпервізора образу операційної системи для встановлення. Для цього слід перейти у вікно сховища сервера, вказати шлях до завантаження, та натиснути ОК. В результаті завантаження в переліку доступних образів для створення віртуальних машин з'явиться образ завантаженої системи.

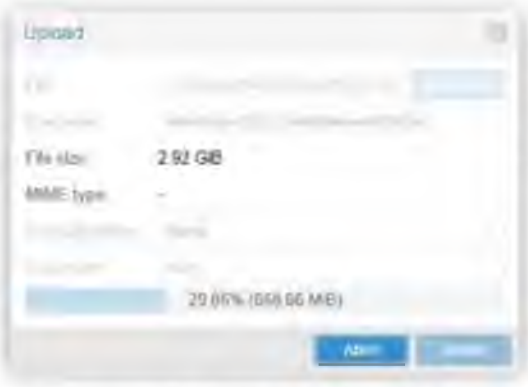


Рисунок 3.26 – Завантаження образу ОС

Після успішного завантаження файл з’явиться у списку доступних образів. Для того, щоб створити віртуальну машину слід перейти у вікно загальної інформації про сервер, де натиснути на кнопку створення ВМ.

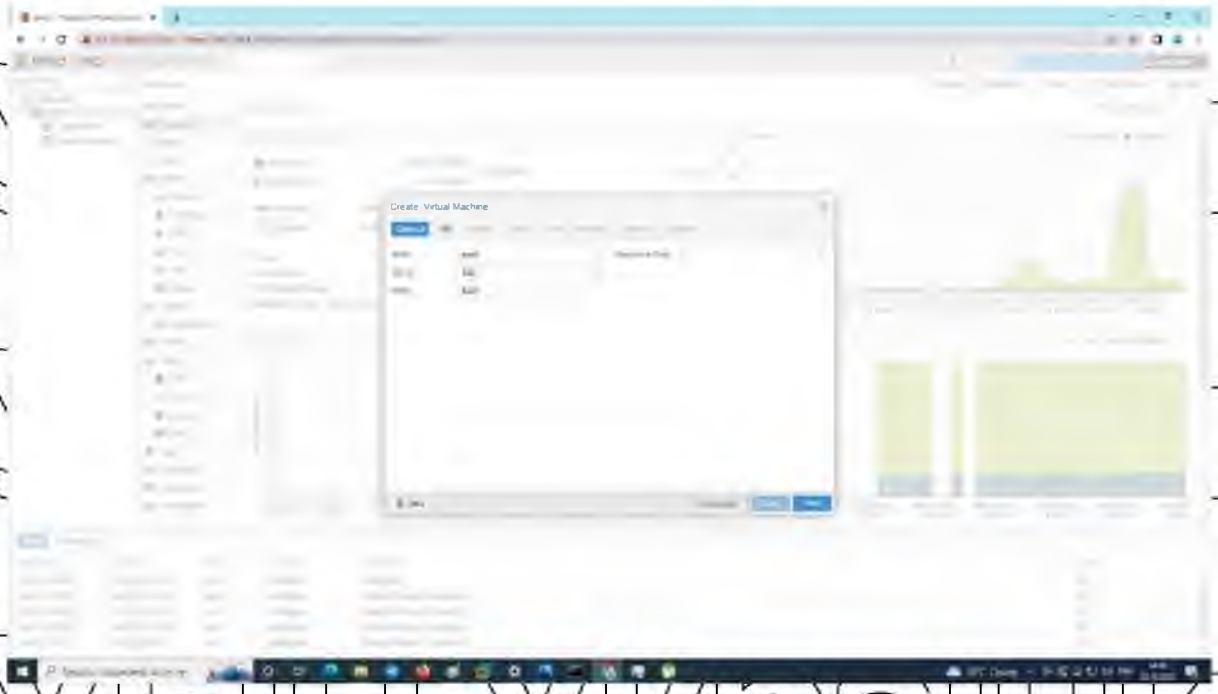


Рисунок 3.27 – Створення ВМ на базі Proxmox VE

Далі система запитує ті ж самі параметри, що і VmWare Workstation: тип операційної системи, розмір ОЗП та диску, кількість ядер процесора, образ диску до завантаження, та тип мережі. В кінці налаштувань виводиться вікно з загальними характеристиками.

Рисунок 3.28 – Параметри віртуальної машини

Після цього запуститься процес створення віртуальної машини, результатом якого стане вікно нової віртуальної машини. Слід запустити її, і перед користувачем виникає вікно, де слід обрати тип встановлення ОС.

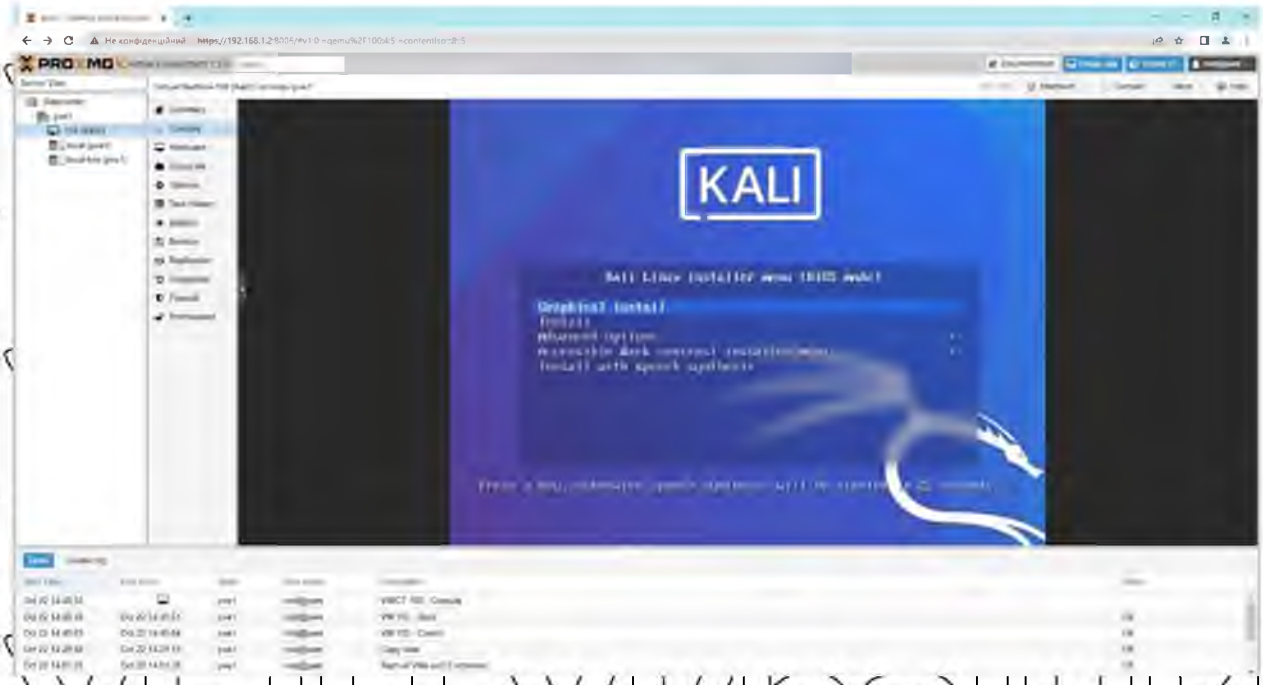


Рисунок 3.29 – Вибір типу встановлення системи

Далі треба буде вказати дані, аналогічні, як при встановленні операційних систем на віртуальні машин до цього – мову, часовий пояс, дані користувача, диск та кількість програм, які необхідні встановити на ОС. Після успішного встановлення віртуальну машину буде перезавантажено.

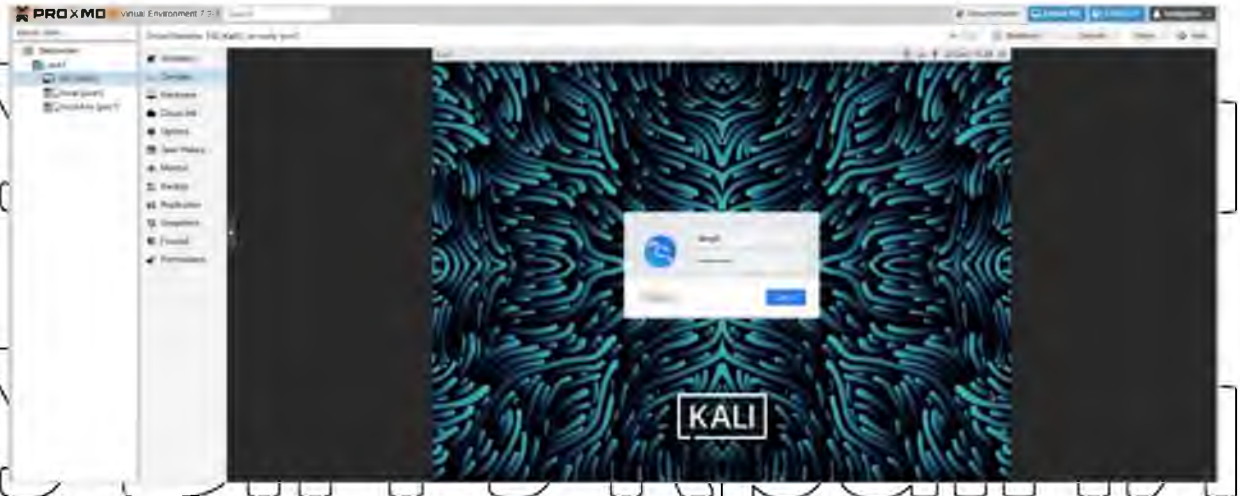


Рисунок 3.30 – Перший вхід в систему

Далі відкриваємо командний рядок у створеній ВМ під управлінням Kali Linux та встановлюємо пароль для супер-користувача root і завантажуємо пакет для віддаленого підключення до віртуальної машини xrdp [17].

Рисунок 3.31 – Встановлення пакету xrdp

Наступним етапом слід встановити статичну IP-адресу та переглянути зміни. Для цього слід перейти в мережеві налаштування.

Рисунок 3.32 – Встановлення та перегляд статичної IP-адреси

Після цього запускаємо процес xrpd для можливості підключення до віртуальної машини

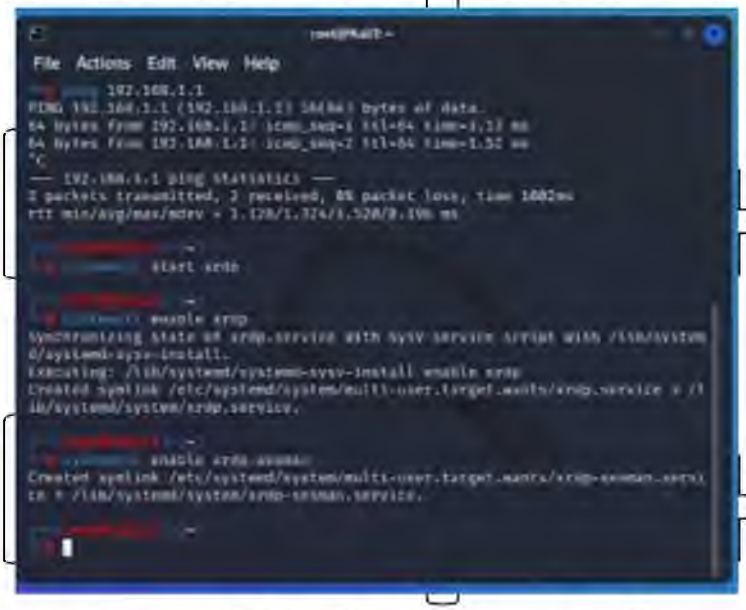


Рисунок 3.33 – Запуск процесу xrdp

Запускаємо з комп'ютера клієнт Remote Desktop Protocol, вводимо IP-адресу віртуальної машини та підключаємось до неї

Рисунок 3.34 – Підключення до Kali Linux через RDP

На цьому стандартне налаштування користувацької віртуальної машини завершено. Далі слід її вимкнути та клонувати, не забувши на кожній новій ВМ змінити мережеві налаштування.

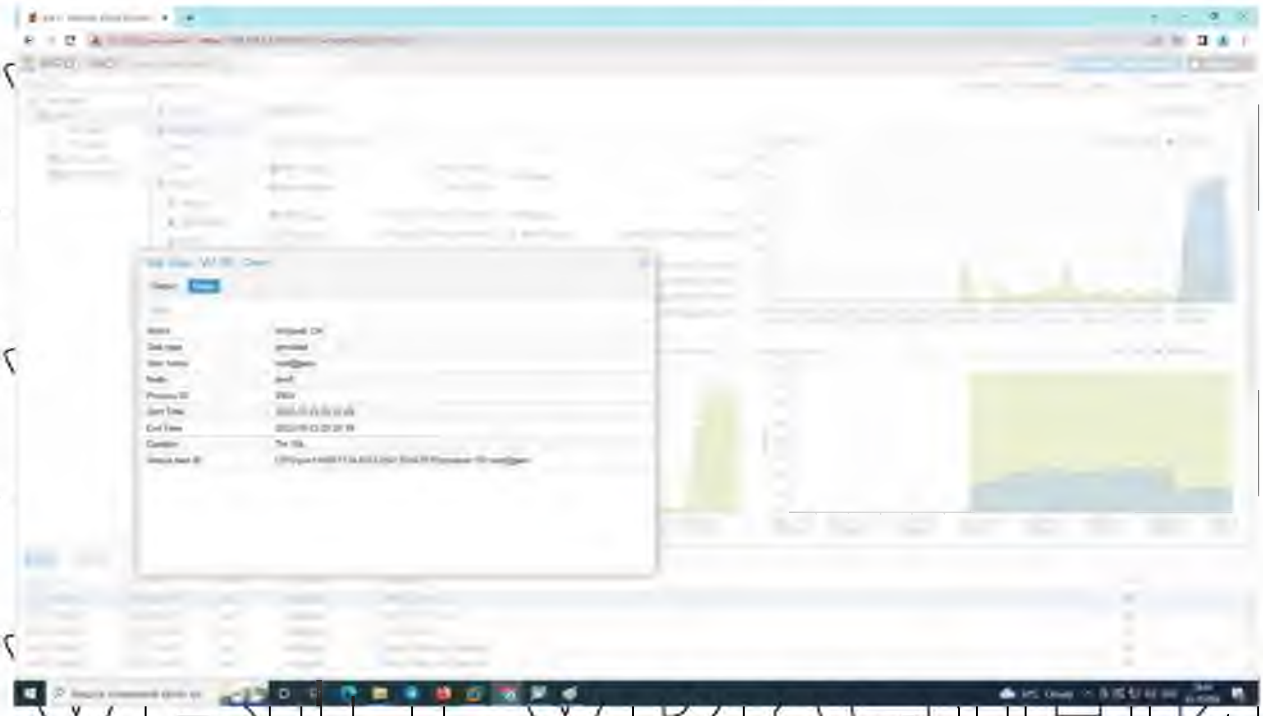


Рисунок 3.35 – Завершена задача по клонуванню ВМ

3.2.2 Об’єднання серверів у кластер

Для більш зручного керування інфраструктурою використовують кластерні рішення – об’єднання декількох серверів в одну систему для забезпечення можливості резервування ресурсів та централізованого адміністрування. Proxmox VE також підтримує дану функцію, можно було вирішено об’єднати 2 сервери в один кластер. Для цього заходимо у відповідне меню на панелі керування. Слід вказати ім’я кластера та його IP-адресу.

Рисунок 3.36 – Задання параметрів кластеру

Запуститься процес, результатом якого стане створення кластеру.

Рисунок 3.37 – Створений кластер

Для того, щоб приєднати до кластеру інший сервер, слід натиснути на меню «інформація про приєднання», де скопіювати дані.

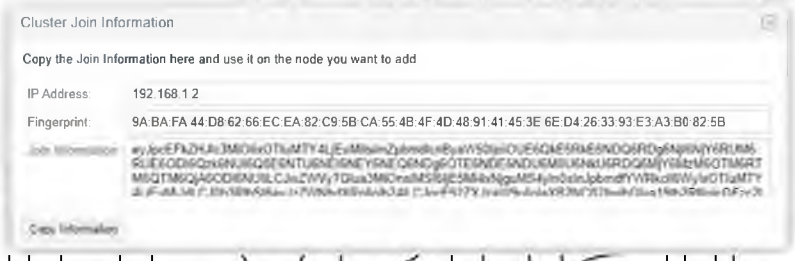


Рисунок 3.38 – Інформація для приєднання до кластеру

Після того, як кластер створено, переходимо на сторінку керування другим сервером. Слід натиснути на кнопку «приєднатися до кластеру», куди вставити скопійовану раніше інформацію про приєднання, що являє собою дані про IP-адресу кластера та 1 сервера і ключ. Також слід ввести пароль root [18].

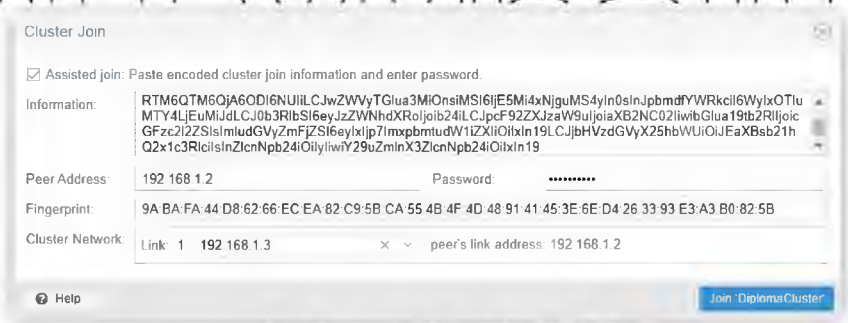


Рисунок 3.39 – Приєднання до кластеру

Після того, як кластер створено, переходячи на адресу будь якого з хостів, ми будемо бачити інформацію про обидва сервери та всі їх ресурси (віртуальні машини, контейнери, сховища та ін.)

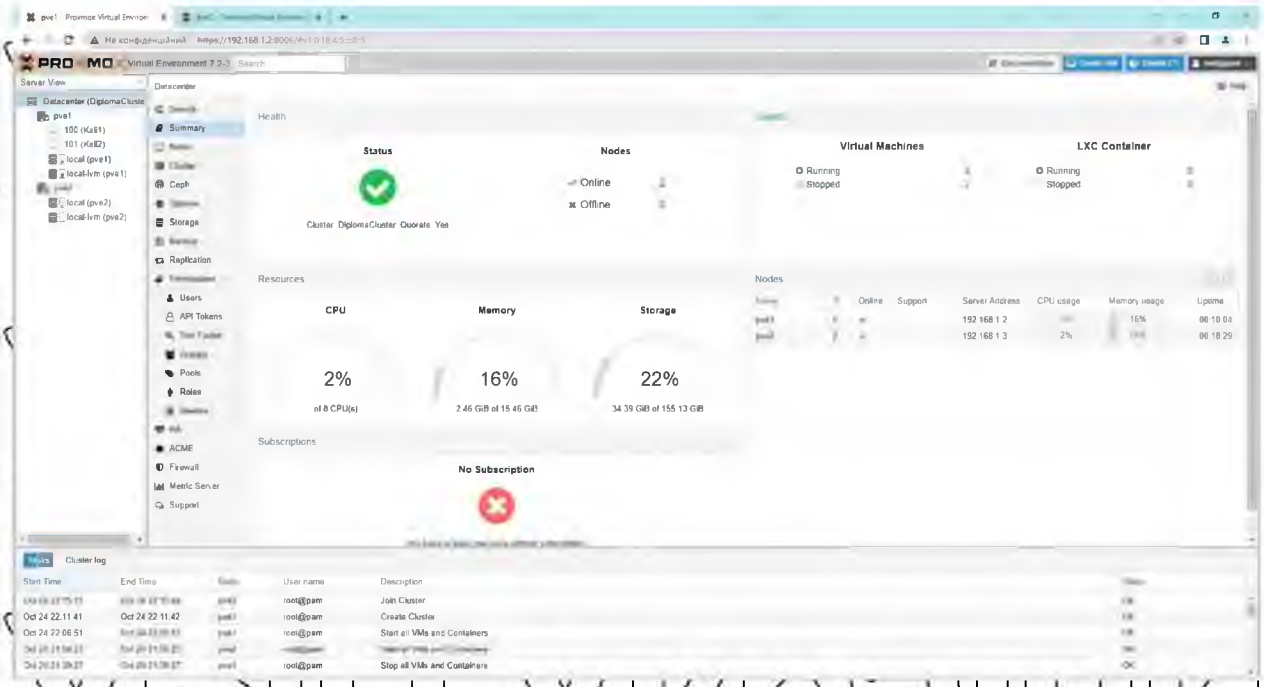


Рисунок 3.40 – Інформація про ресурси кластеру

Створення кластеру надає велику кількість переваг, одна з яких – можливість міграції віртуальних машин, що містяться на серверах, на інші вузли кластеру. Для цього обираємо потрібну віртуальну машину та клацаємо на опцію «мігрувати», вказавши на який вузол.

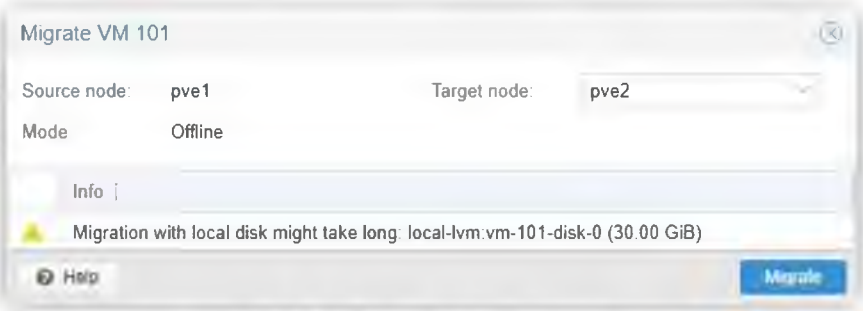


Рисунок 3.41 – Параметри міграції віртуальної машини

Запуститься вікно задачі міграції, результатом якої буде перенесення віртуальної машини на інший сервер. Після закінчення процесу міграції запускаємо перенесену віртуальну машину для подальшої роботи. Віртуальна машина успішно запускається, і не видає жодних помилок.

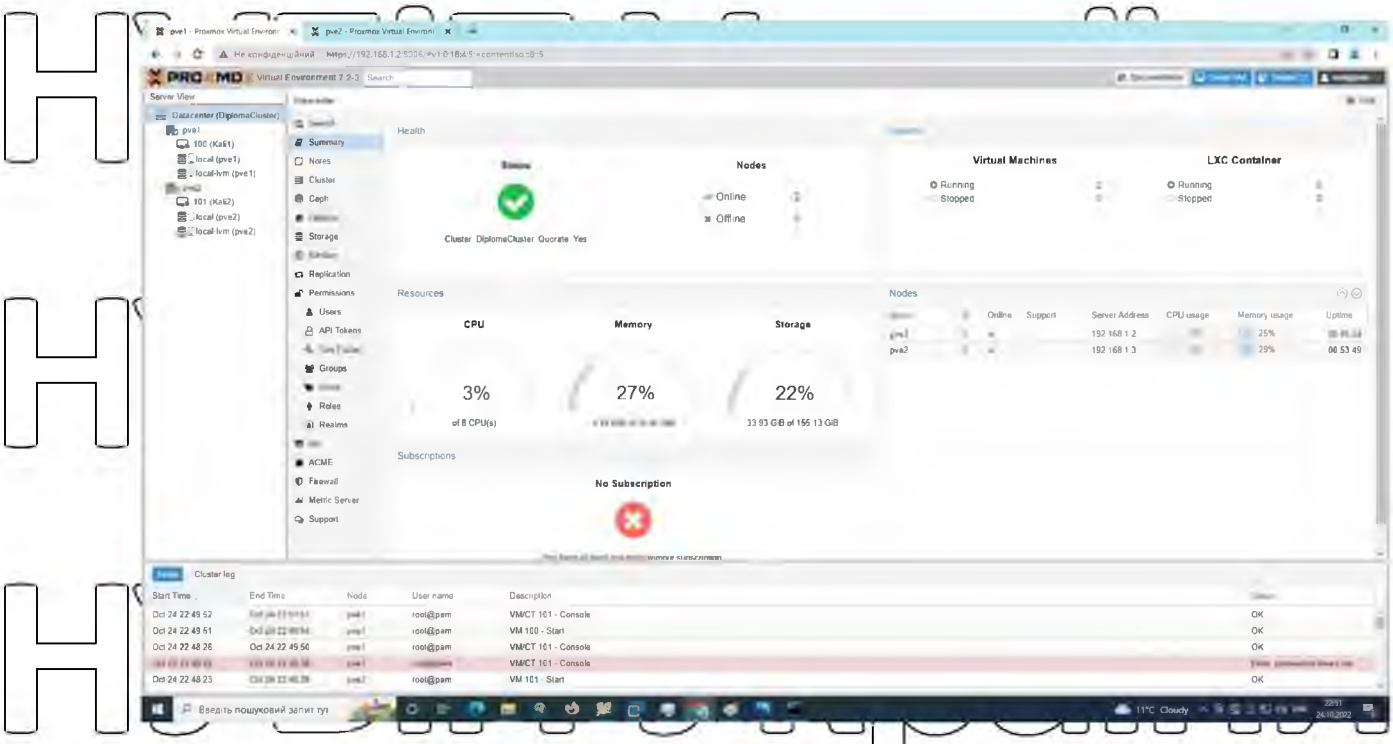


Рисунок 3.42 – Успішне перенесення ВМ

3.2.3 Побудова мережі

Для побудови моделі мережі на мережевих пристроях слід перейти на веб-сторінку створеної раніше віртуальної машини EVE-NG, у лабораторну роботу та додати необхідні пристрої.

В даному випадку, виходячи з досвіду знайомства з мережами навчальних закладів, на робочу поверхню було додано 1 маршрутизатор (який виступає в ролі і фаєрвола) і 2 комутатори ядра, один з яких відповідає за серверний сегмент, а інший – за користувацький. Також були додані комутатори доступу, що підключені до комутатора ядра, що відповідає за користувацький сегмент, де в свою чергу є 2 групи: 1 – комутатори, що розміщені в навчальних лабораторіях, 2 – розміщені на кафедрах факультету. Відповідно до цього, політики доступу для користувачів з цих 2 сегментів відрізняються – користувачі, що приєднані через комутатори

кафедр мають більше прав доступу до локальних ресурсів, що знаходяться на серверах факультету.

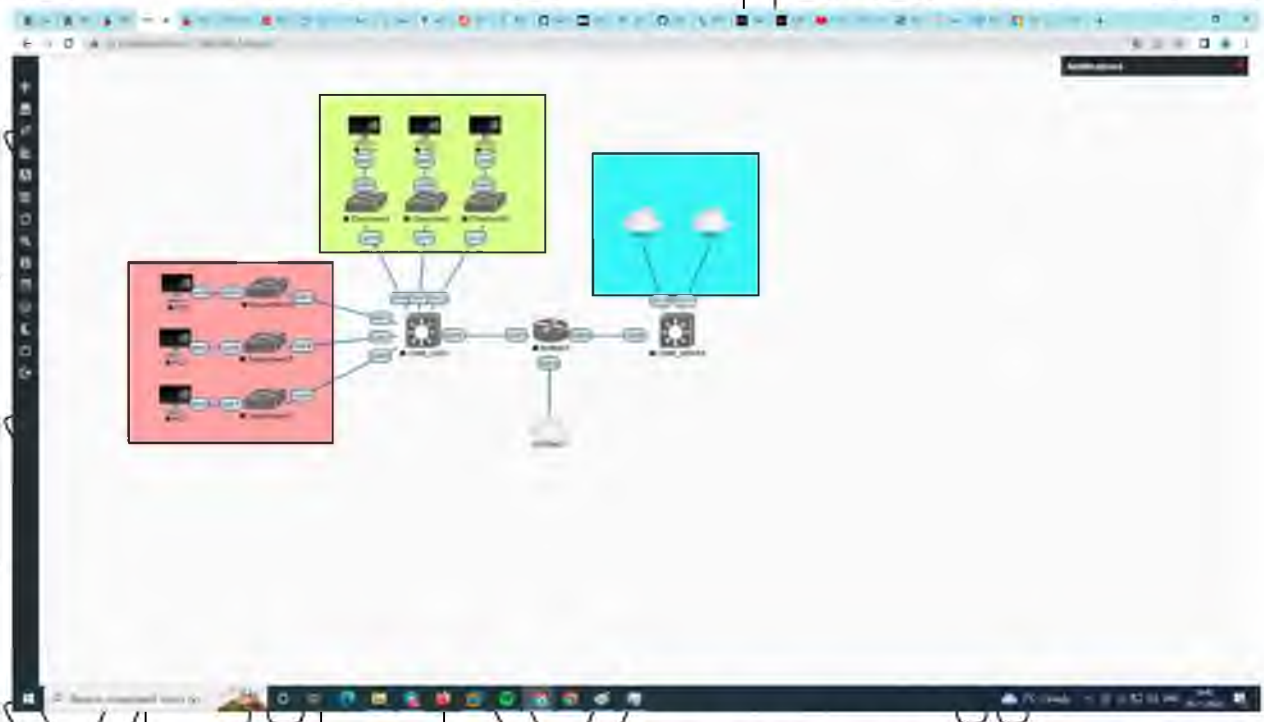


Рисунок 3.43 – Схема мережі навчального закладу

Після того, як на робочу поверхню були додані пристрої, слід провести між ними зв'язки. Коли це виконано, слід запускати пристрої. Віртуальній машині EVE-NG слід виділяти достатньо ресурсів, адже при запуску усіх пристроїв вона має високе навантаження

В даному випадку ВМ було виділено 2 процесорних ядра та 4 ГБ оперативної пам'яті, однак цього було замало для повноцінної роботи моделі, оскільки завантаження процесора сягало 100%, а оперативної пам'яті 67%. Якщо завантаженість процесора після запуску пристроїв спадає, то об'єм зайнятого простору оперативної пам'яті не зменшується.

Фактично, підключення наших пристроїв в моделі мережі навчального закладу виглядають так, як подано на рисунку нижче.

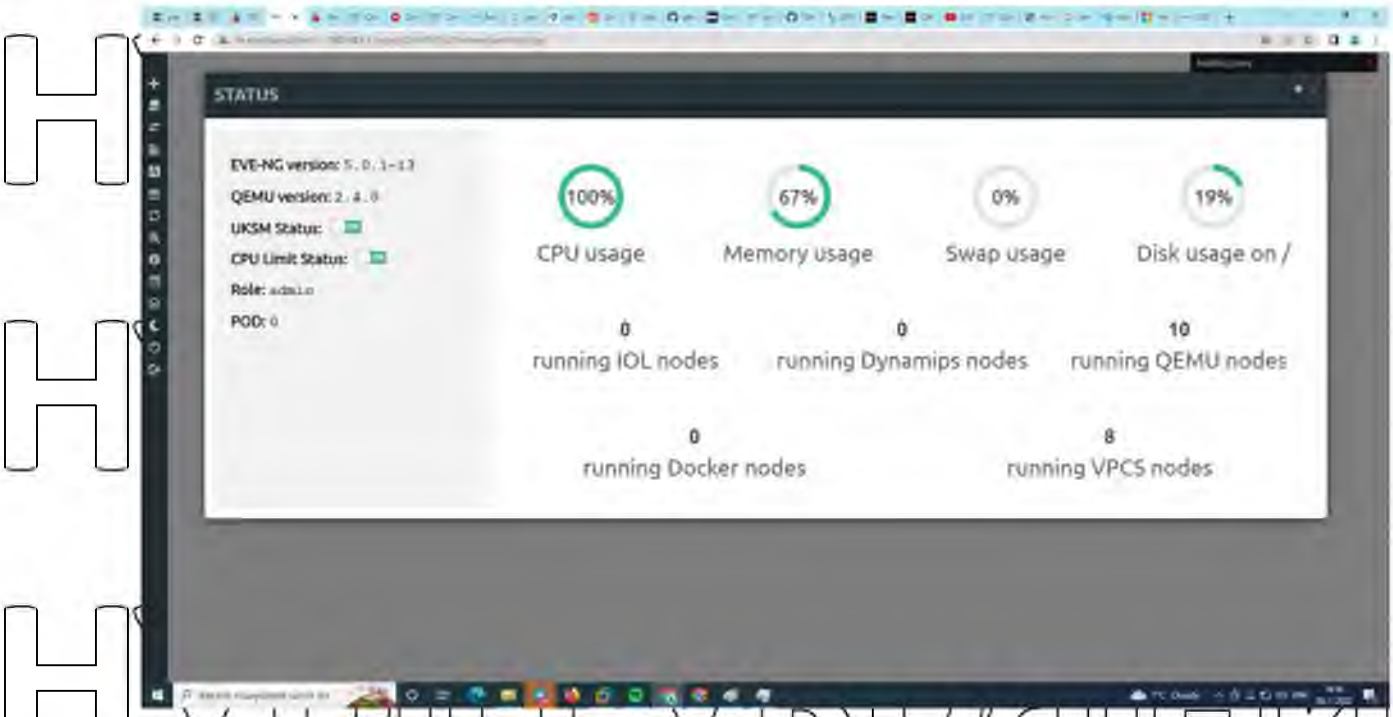


Рисунок 3.44 – Завантаженість ВМ при запуску вузлів мережі

Всі пристрої підключаються до віртуальних інтерфейсів VmWare, яка в свою чергу до мережевого інтерфейсу персонального комп'ютера. Сам ПК приєднаний до маршрутизатора, який вже підключений до мережі провайдера.

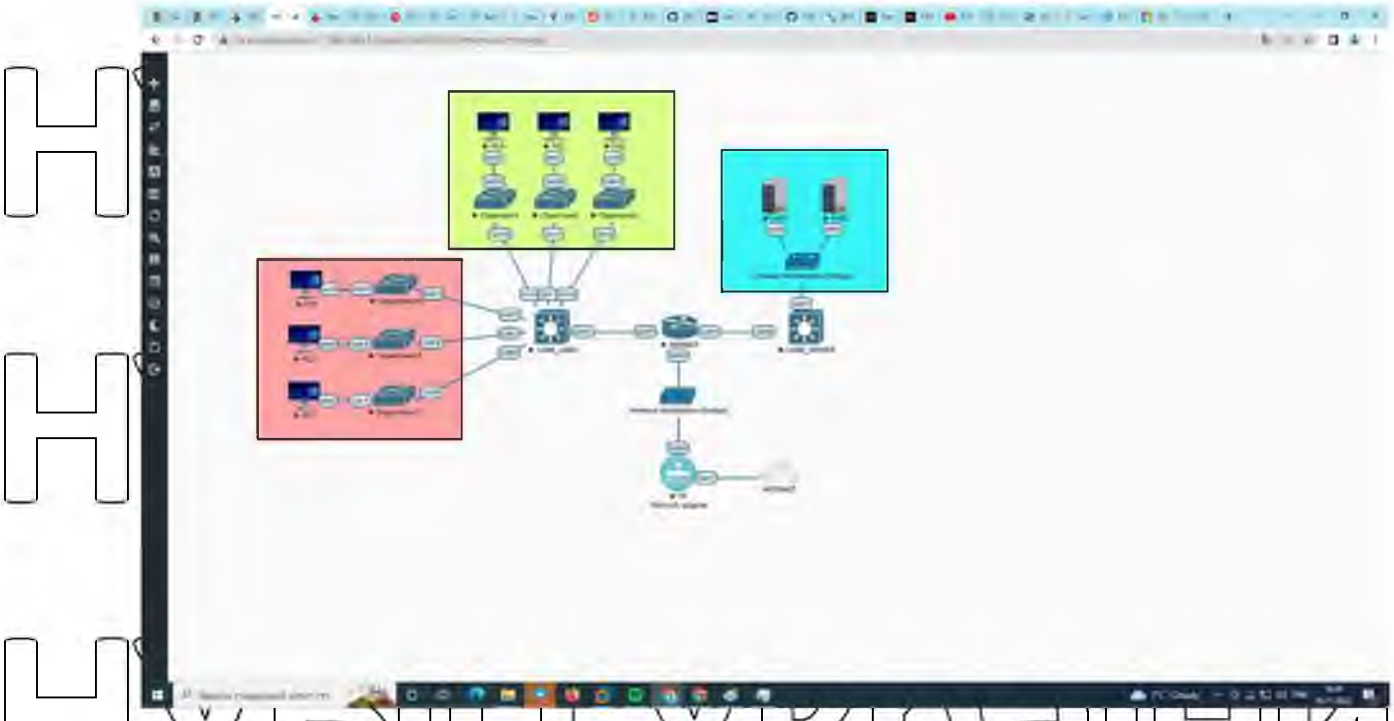


Рисунок 3.45 – Реальні підключення пристроїв

Після того, як вузли запущені, налаштовуємо мережу. Для цього слід натиснути на зображення мережевого пристрою і перейти у додаток Putty, що являється SSH клієнтом для підключення до мережевих пристроїв.

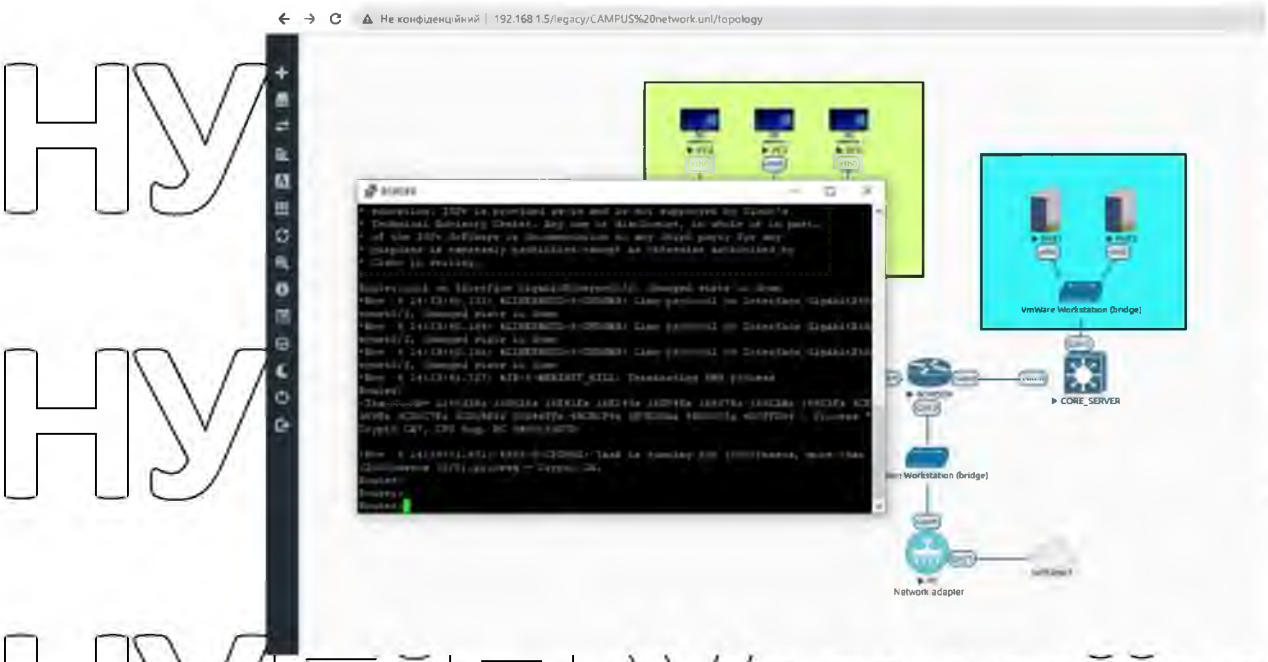


Рисунок 3.46 – Підключення маршрутизатора через Putty

В межах дослідження захисту інформації в начальному закладі було обрано одразу змінити налаштування мережі, аби зробити її більш захищеною. Одна з характеристик захисту інформації – доступність ресурсів. Якщо один з ключових пристроїв вийде з ладу, аби вся система не втратила працездатність. В реаліях навчальних закладів України на сьогодні навряд чи можна зробити повноцінне резервування всіх ключових вузлів мережі, однак на наведеній вище схемі мережі можна зробити резервування комутаторів ядра та їх зв'язків між собою та маршрутизатором. Для цього слід провести зв'язки від серверів та комутаторів доступу користувачів до обох комутаторів ядра. Більшість комутаторів доступу, на сьогодні, для цього мають 2-4 висхідних порти, так само як і сервери – мережеві карти на мінімум 2 порти.

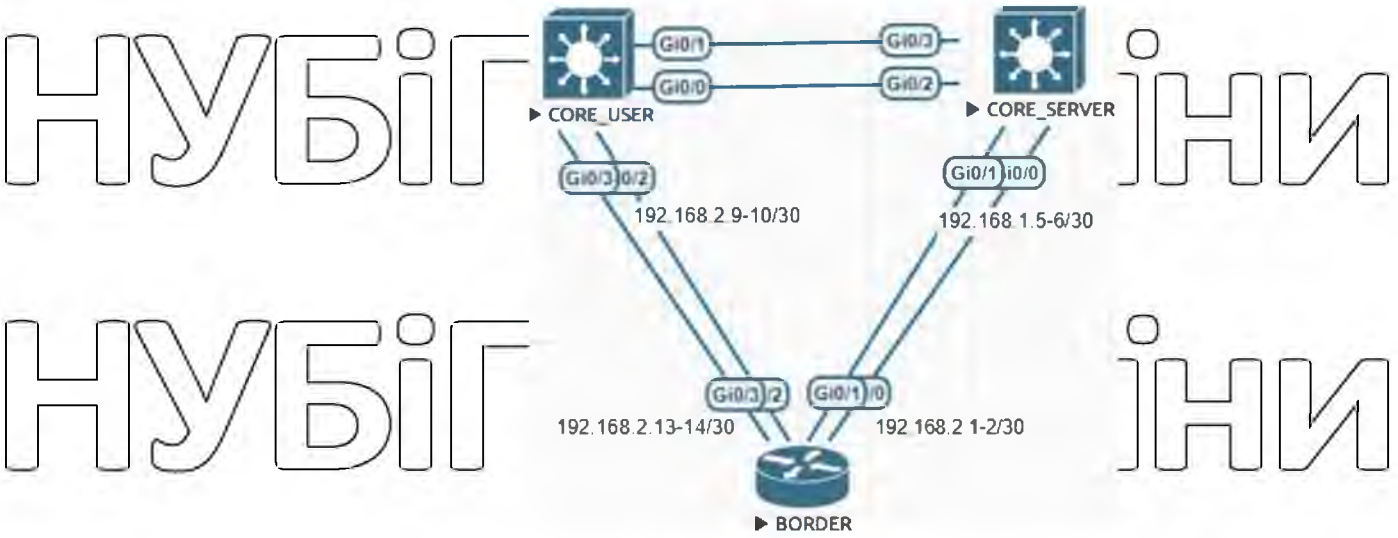


Рисунок 3.47 – Забезпечення відмово стійкості комутаторів

Після того як налаштовано нові зв'язки, приєднуємось до пристроїв та виконуємо налаштування. В першу чергу слід встановити пароль на різні режими пристроїв, а також вказати вірну назву пристроїв, яка б відповідала наведеній вище схемі. Окрім цього, виконуємо налаштування IP-адрес інтерфейсів.

```
Enter configuration commands, one per line.  End with CNTL/Z.
BORDER(config)#interface g0/0
BORDER(config-if)#ip address 192.168.2.1 255.255.255.252
BORDER(config-if)#no shutdown
BORDER(config-if)#exit
BORDER(config)#interface g0/1
BORDER(config-if)#ip address 192.168.2.5 255.255.255.252
BORDER(config-if)#no shutdown
BORDER(config-if)#exit
BORDER(config)#
*Nov  6 17:20:40.009: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Nov  6 17:20:41.010: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
BORDER(config)#interface g0/2
BORDER(config-if)#ip address 192.168.2.10 255.255.255.252
BORDER(config-if)#no shutdown
BORDER(config-if)#exit
BORDER(config)#
*Nov  6 17:26:15.197: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
*Nov  6 17:26:16.202: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
BORDER(config)#interface g0/3
BORDER(config-if)#ip address 192.168.2.14 255.255.255.252
BORDER(config-if)#no shutdown
BORDER(config-if)#exit
BORDER(config)#
*Nov  6 17:26:43.153: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
*Nov  6 17:26:44.153: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to up
BORDER(config)#exit
BORDER#
*Nov  6 17:28:05.527: %SYS-5-CONFIG_I: Configured from console by console
BORDER#copy ru
BORDER#copy running-config star
BORDER#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BORDER#
*Nov  6 17:29:23.760: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Nov  6 17:29:24.745: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
BORDER#
```

Рисунок 3.48 – Налаштування інтерфейсів маршрутизатора

Для зв'язку маршрутизатора та комутаторів ядра налаштовуємо протокол динамічної маршрутизації, що підтримується більшістю виробників – OSPF.

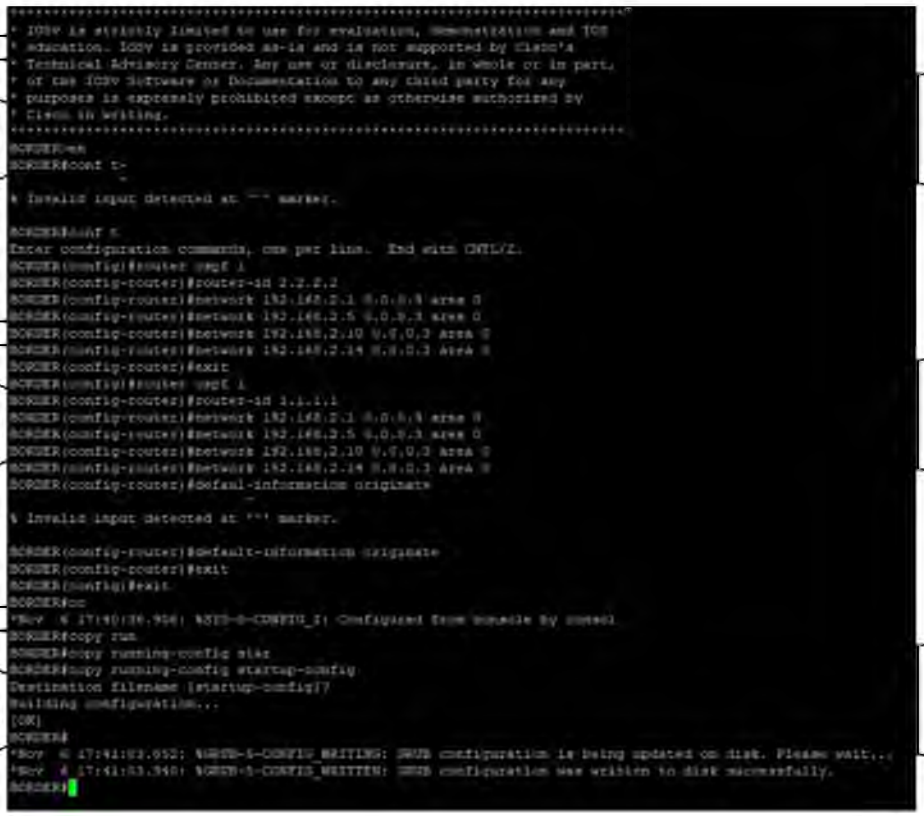


Рисунок 3.49 – Налаштування протоколу OSPF

Далі на комутаторах ядра слід створити віртуальні мережі (VLAN), аби розділити трафік на підмережі, для забезпечення безпеки ресурсів, до яких слід забезпечити обмежений доступ. Також на комутаторах слід налаштувати протокол STP, аби не виникали мережеві петлі, протоколи DHCP снупінгу, інспекції ARP пакетів, фільтрацію графіку на предмет Flood-атак.

3.2.4 Налаштування фільтру DNS-адрес

Для забезпечення безпеки мережі важливим є відсіювання усього небажаного трафіку, що може заходити в мережу. Для забезпечення цього є доречним використання DNS-фільтру на базі Linux, під назвою PI-Hole [19].

Першим етапом є завантаження на сервер PVE образу серверної ОС Ubuntu Linux. Далі за аналогією кроків раніше створюємо ВМ. Для роботи даної системи не потрібні великі потужності, то виділяємо їй 2 ядра та 2Гб оперативної пам'яті та 10 ГБ дискового простору.

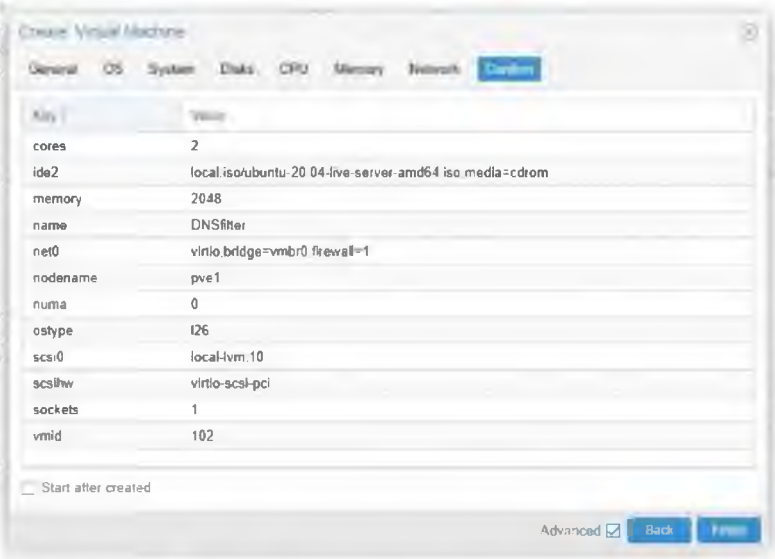


Рисунок 3.50 – Параметри віртуальної машини

Після запуску слід налаштувати ті ж характеристики, що і при встановленні ОС на віртуальні машини раніше – вказати країну, часовий пояс, ім'я та пароль користувача, IP-адресу машини, який набір додатків слід встановити.

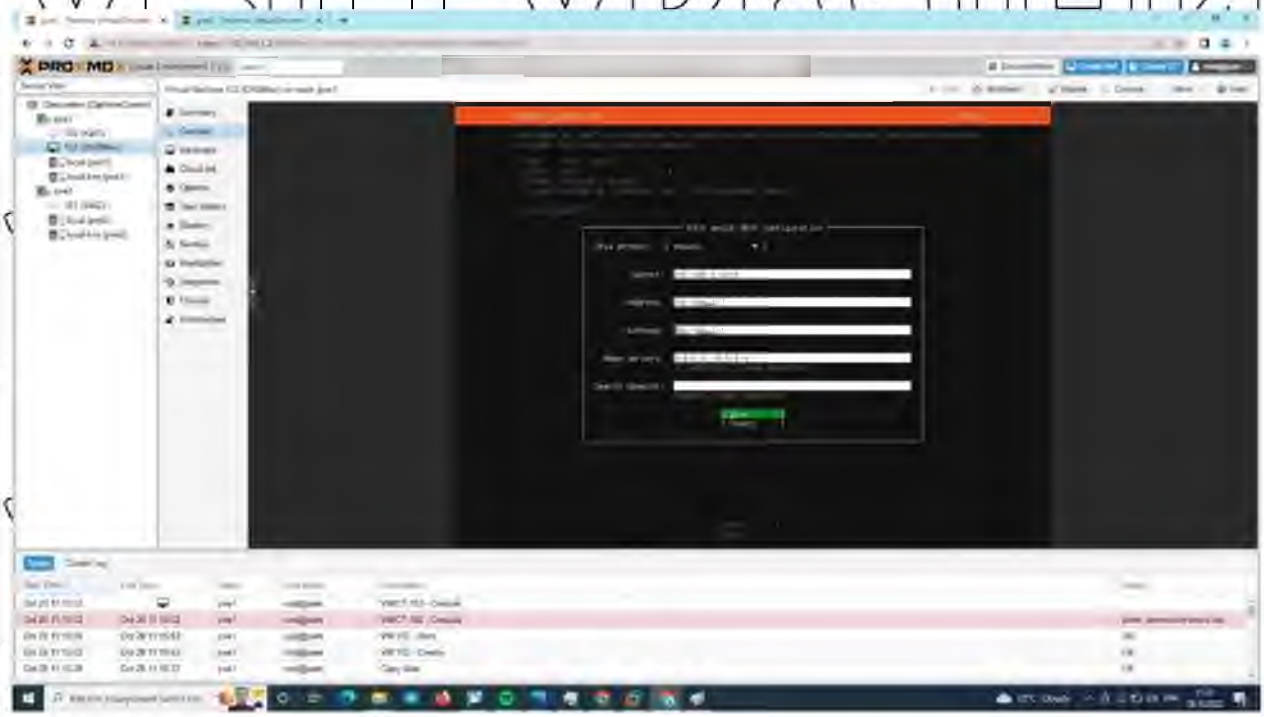


Рисунок 3.51 – Мережеві налаштування

Після встановлення ОС та перезавантаження системи слід ввести команду на встановлення пакету Pi-Hole.

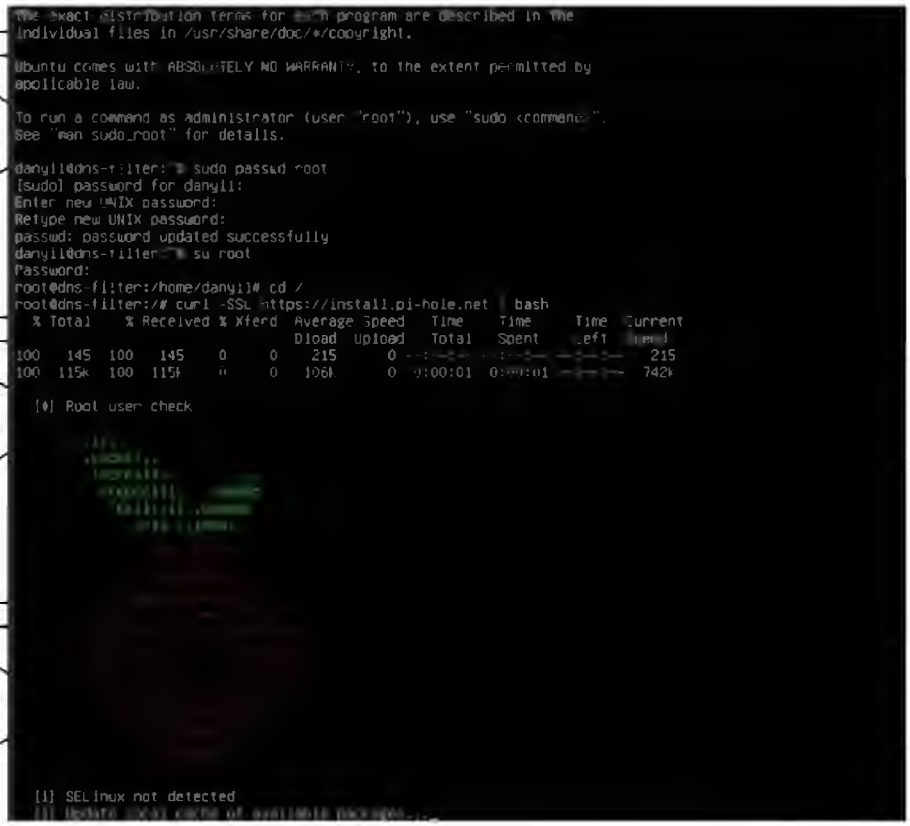


Рисунок 3.52 – Встановлення пакету Pi-Hole

Після встановлення перед користувачем виникає меню налаштування вже самого фільтру DNS-адрес.

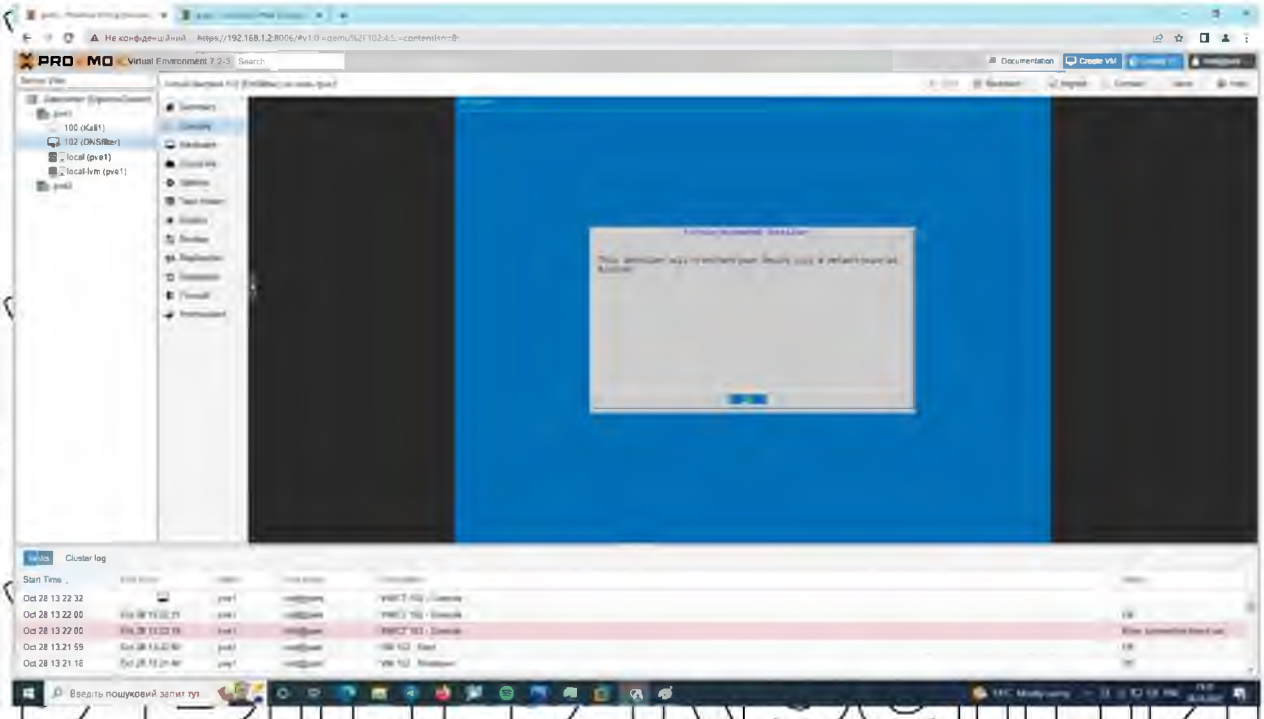


Рисунок 3.53 – Налаштування Pi-Hole

Далі після завершення процесів встановлення та налаштування системи слід створити нового користувача.

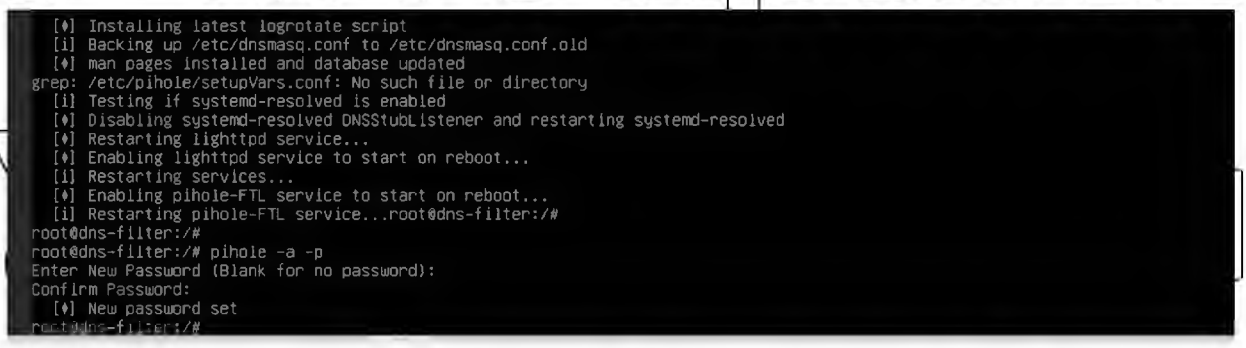


Рисунок 3.54 – Створення нового користувача Pi-Hole

Після цього заходимо у веб-браузер та вводимо IP-адресу віртуальної машини. Перед нами відкриється вікно авторизації.

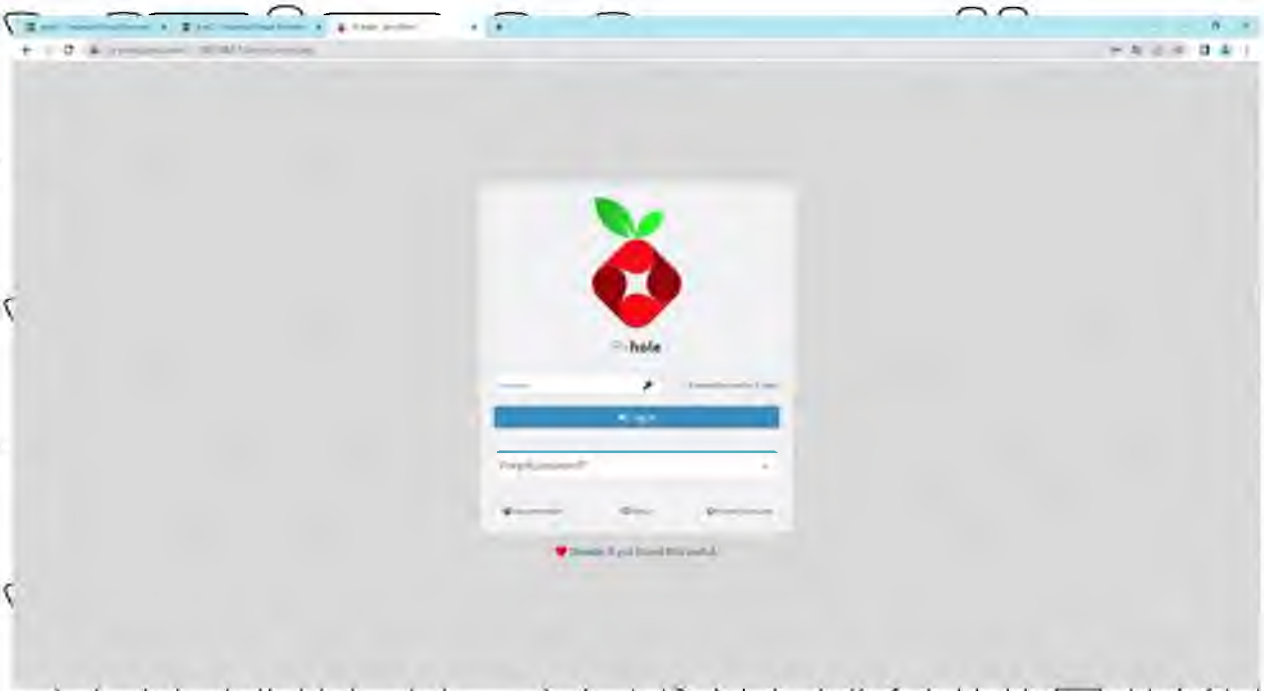


Рисунок 3.55 – Авторизація в системі

По замовчуванню Pi-Hole не має списків адрес та доменів, трафік з яких слід блокувати фільтрації. Однак їх можна знайти у відкритому доступі в інтернеті. Знаходимо їх та додаємо в Pi-Hole.

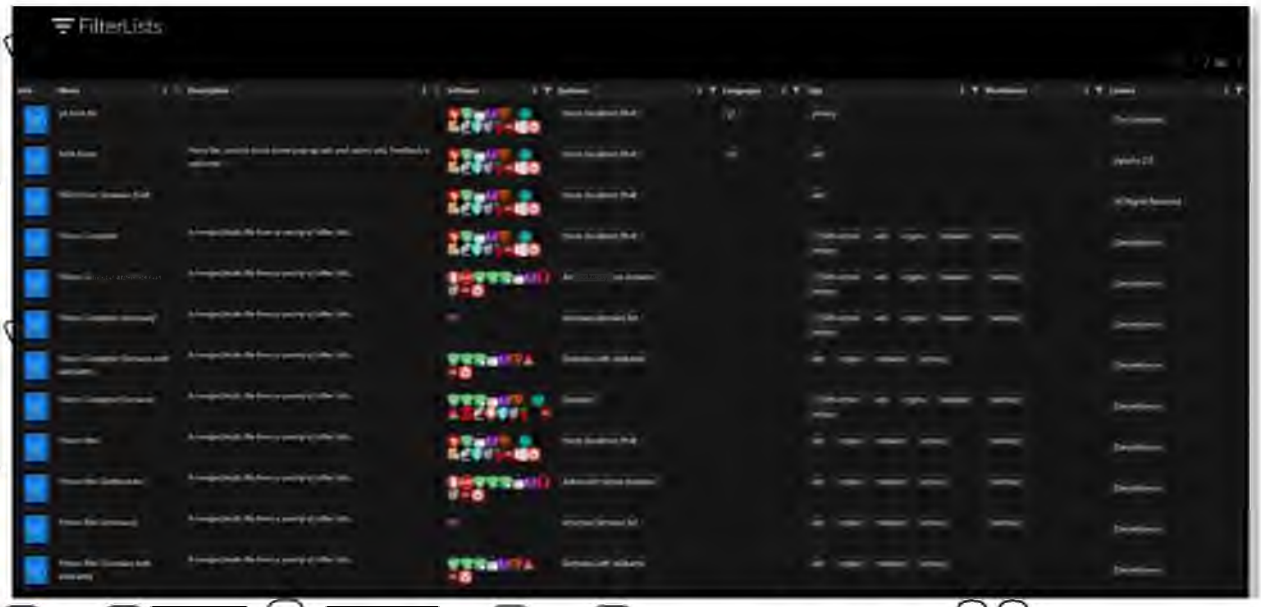


Рисунок 3.56 – Доступні списки фільтрації адрес

Для більшої безпеки мережі рекомендують додавати та застосовувати декілька різних списків.

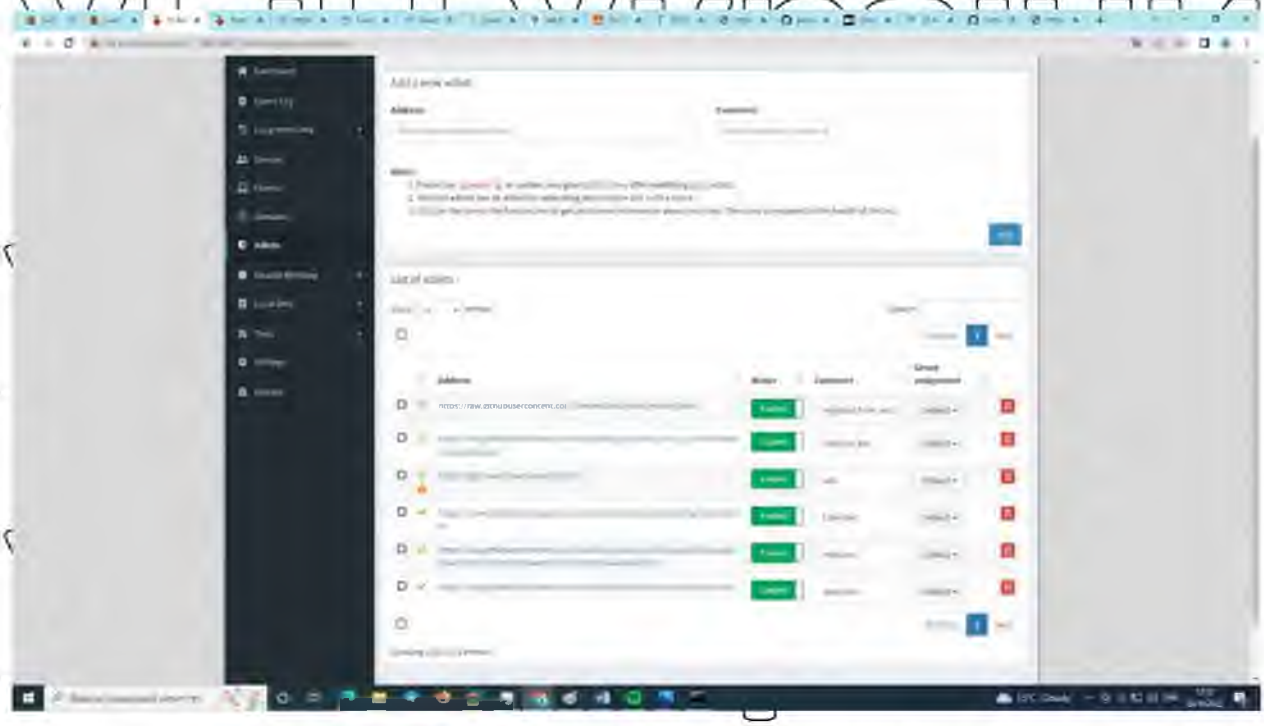


Рисунок 3.57 – Додані списки фільтрації адрес

Для того, щоб графік почав фільтруватися треба перезавантажити процес Pi-Hole на сервері.

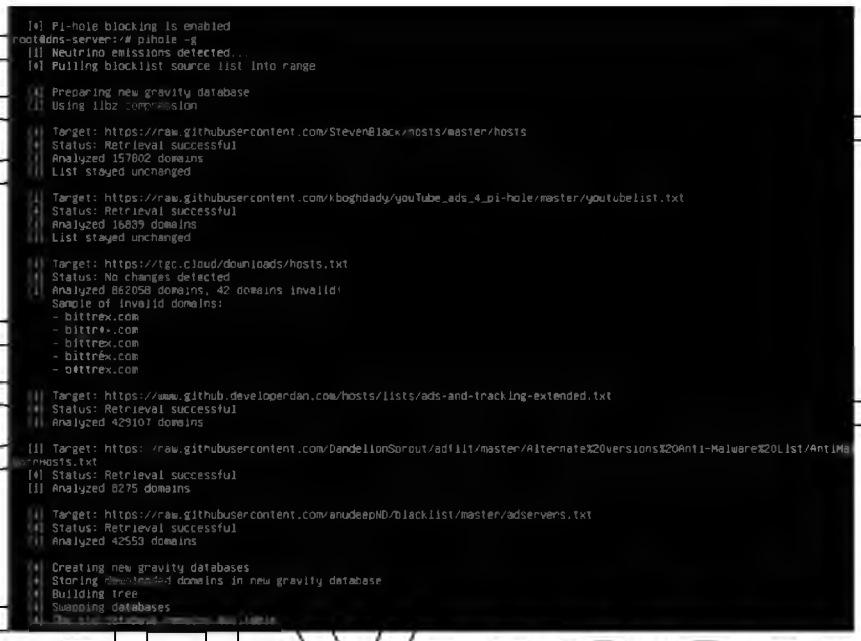


Рисунок 3.58 – Перезавантаження процесу Pi-Hole

Далі слід на маршрутизаторі та віртуальних машинах в полі DNS-серверу вказати IP-адресу віртуальної машини з Pi-Hole. Сама Pi-Hole вже переадресовує трафік на заданий зовнішній DNS-сервер, в даному випадку був обраний DNS-сервер Google.

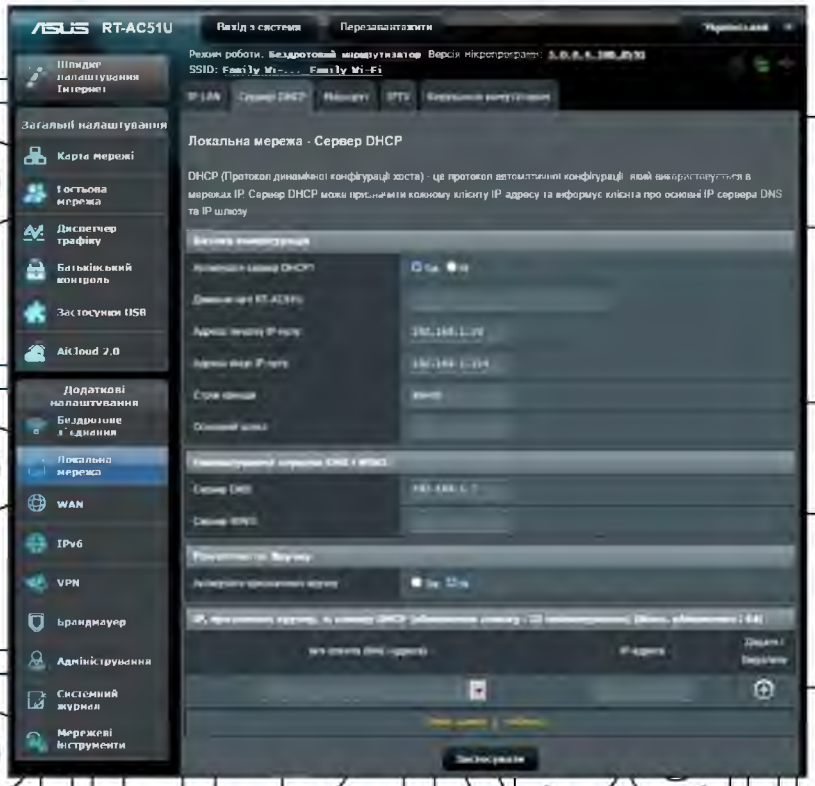


Рисунок 3.59 – Вибір DNS-серверу

3.2.5 Налаштування системи розпізнавання вторгнень

Для того, щоб ще більше посилити захист мережі, окрім забезпечення безпеки на окремих її вузлах та фільтрації DNS-адрес, бажано додати до системи віртуальну машину, яка б аналізувала трафік на предмет свідчень про початок кібератаки. Існує декілька таких систем з відкритим кодом, найпопулярнішою з яких є IPS Suricata. Suricata — це високопродуктивне програмне забезпечення для аналізу мережі та виявлення загроз, яке використовується багатьма приватними і державними організаціями [20]. Дана система розпізнавання вторгнень встановлюється як додаток на інші операційні системи. В даному випадку було вирішено створити для неї окрему віртуальну машину на базі Kali Linux (Debian).

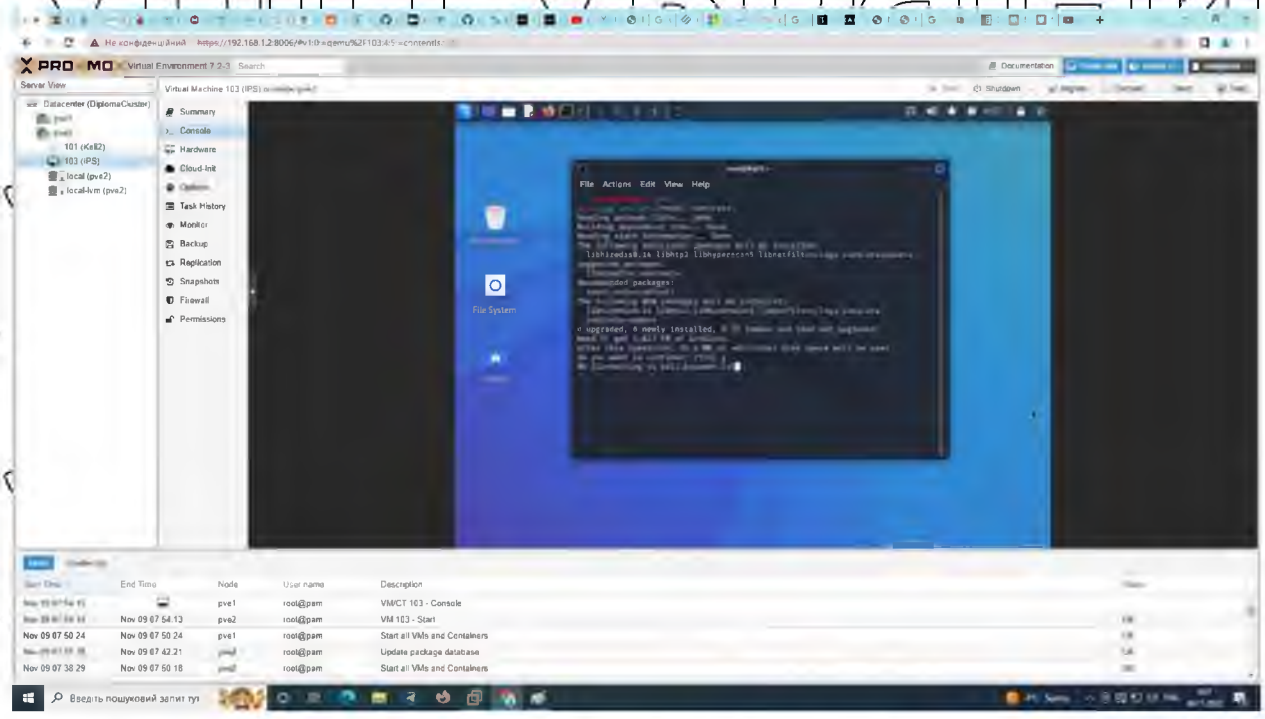


Рисунок 3.60 — Встановлення пакету Suricata

Після того, як пакет встановився, запускаємо процес Suricata та переглядаємо його статус.

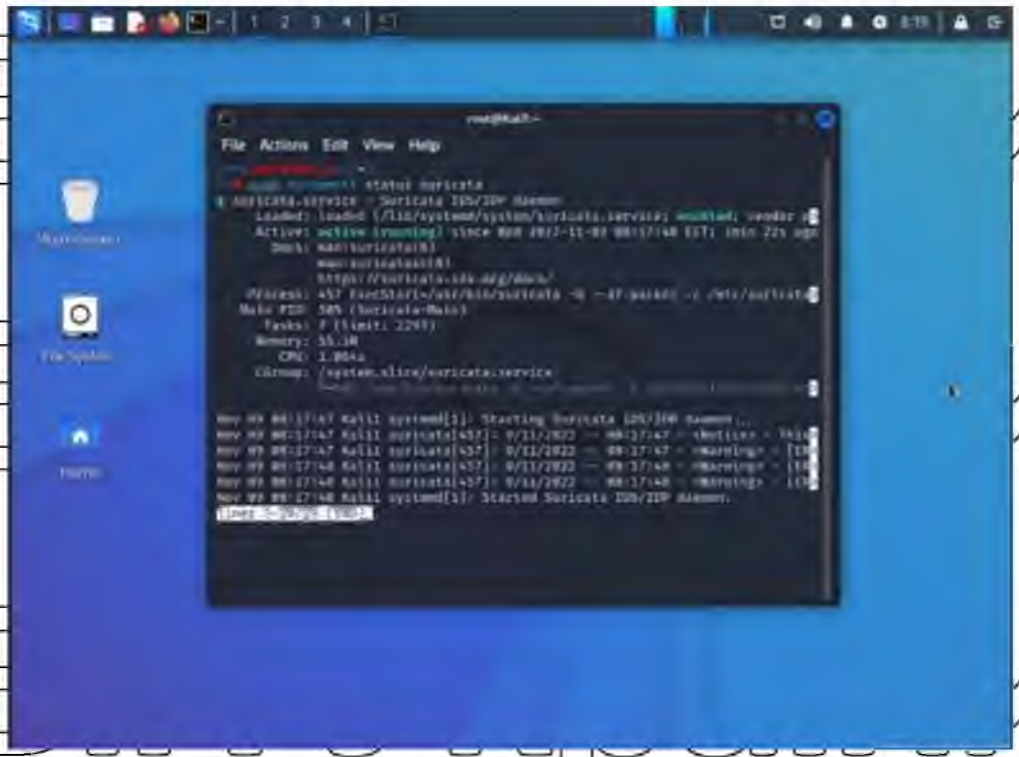


Рисунок 3.61 – Активний статус процесу Suricata

Після того, як ми впевнились, що процес запущено, переходимо до теки, де зберігається Suricata та переглядаємо файли.

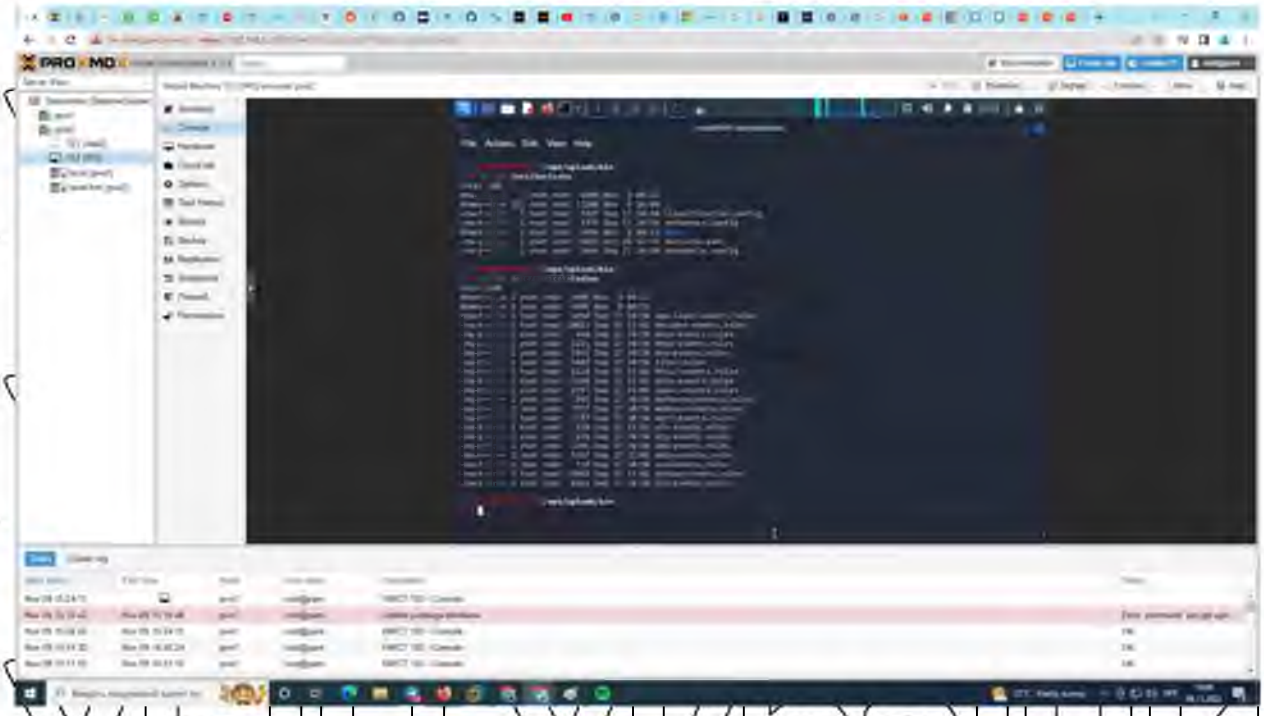


Рисунок 3.61 – Перегляд файлів Suricata

Рисунок 3.62 – Редагування конфігураційного файлу Suricata

Заходимо конфігураційний файл suricata.yaml, та відкриваємо його. Тут слід додати дозвіл на збереження логів системи.

Рисунок 3.63 – Додаємо адреси підмереж для сканування

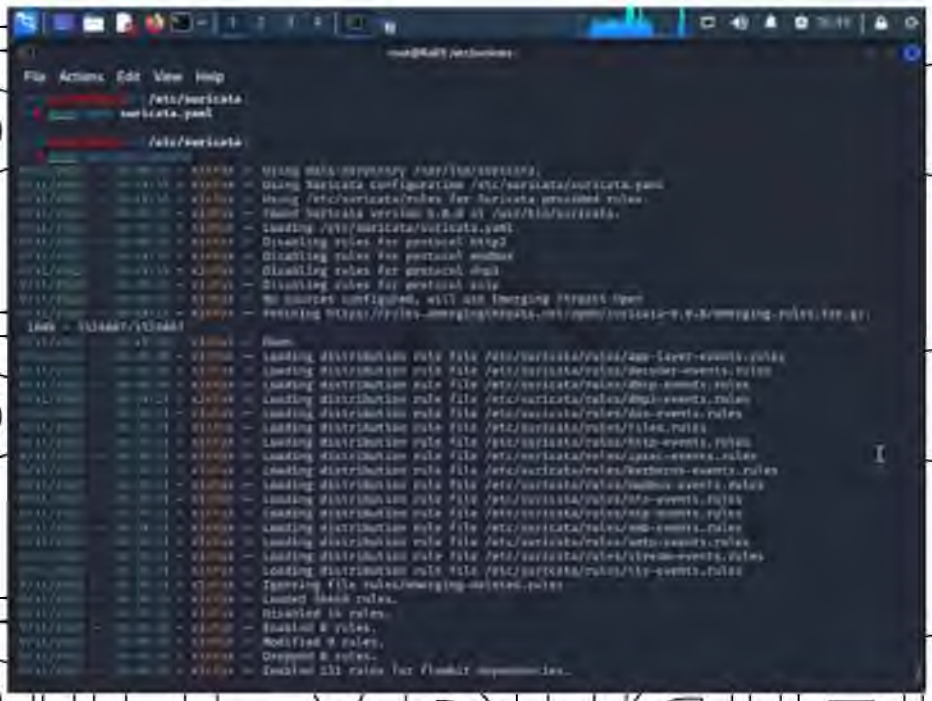


Рисунок 3.64 – Оновлення додатку Suricata

Окрім редагування дозволу на збереження логів, додаємо адреси мереж, які необхідно сканувати на предмет знаходження шкідливого графіку та початку вторгнень. Оновлюємо додаток Suricata.

Рисунок 3.65 – Оновлення списків сигнатур

Після цього запускаємо команду на оновлення списків сигнатур загроз, що доступні для Suricata. Обираємо доступний список та виконуємо команду на дозвіл застосування даного списку.

Рисунок 3.66 – Дозвіл використання списку сигнатур

3.2.6 Налаштування платформи Splunk

Splunk - це програмне забезпечення, яке обробляє і витягує інформацію з машинних даних та інших форм великих даних. Ці машинні дані генеруються процесором, на якому працює веб-сервер, пристрої IOT, журнали з мобільних додатків тощо. Немає необхідності надавати ці дані кінцевим користувачам, проте вони надзвичайно важливі для розуміння, моніторингу та оптимізації продуктивності машин.

Splunk може читати ці неструктуровані та напів-структуровані дані. Після прочитання даних, він дає змогу шукати, відзначати, створювати звіти та інформаційні панелі за цими даними. З появою великих даних Splunk тепер може приймати великі дані з різних джерел, які можуть бути або не бути машинними даними, і виконувати аналітику великих даних.

Таким чином, завдяки простому інструменту для аналізу журналів, Splunk пройшов довгий шлях, щоб стати загальним аналітичним інструментом для неструктурованих машинних даних і різних форм великих даних.

Splunk може приймати різні формати даних, як-от JSON, XML і неструктуровані машинні дані, як-от веб-сторінки та журнали застосунків. Неструктуровані дані можуть бути змодельовані в структуру даних у міру необхідності користувачем.

Отримані дані індексуються Splunk для прискорення пошуку і запитів у різних умовах. Пошук у Splunk включає використання індексованих даних з метою створення метрик, прогнозування майбутніх тенденцій і визначення закономірностей у даних [21].

Для роботи з платформою Splunk завантажуємо з офіційного сайту пакет програми на диск віртуальної машини, на якій встановлена Suricata.

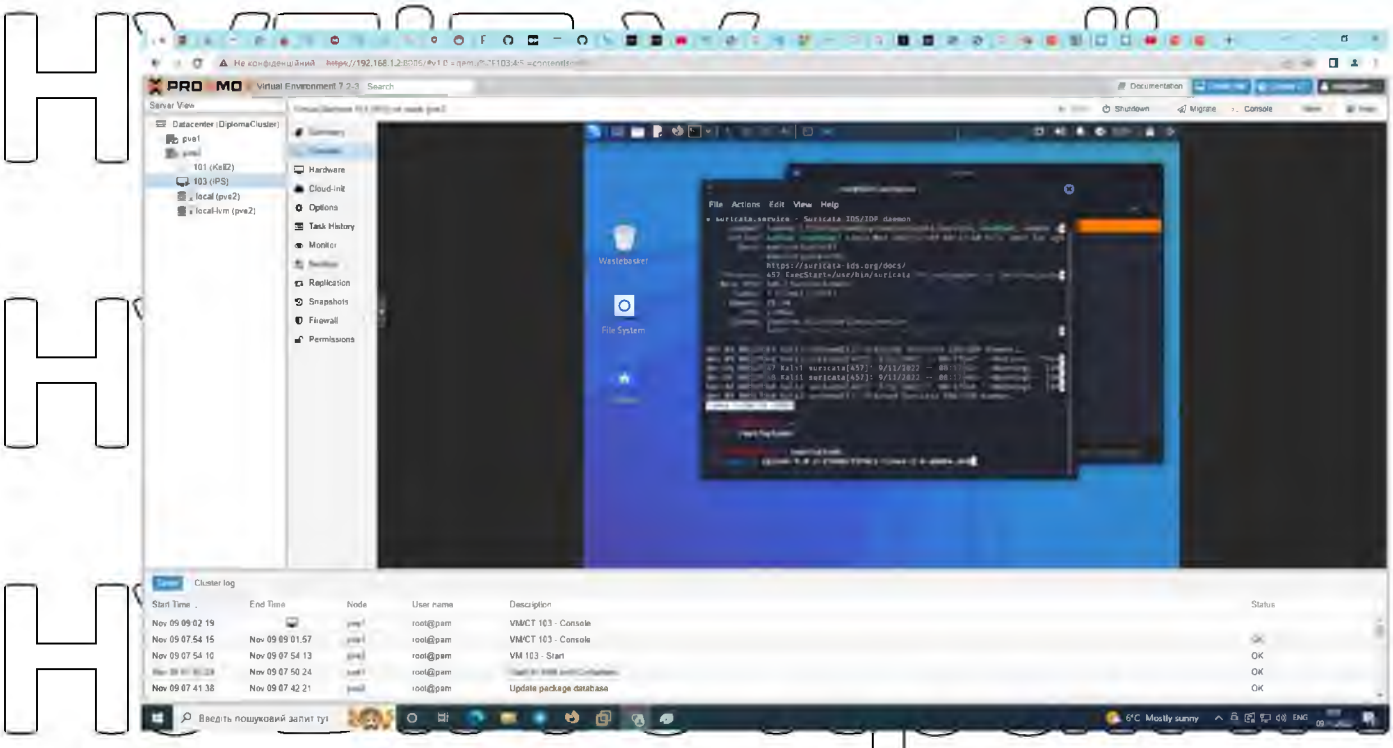


Рисунок 3.67 – Розпакування пакету Splunk

Розпаковуємо архів та даємо команду на запуск програми. Під час її встановлення треба буде ввести пароль для нового користувача.

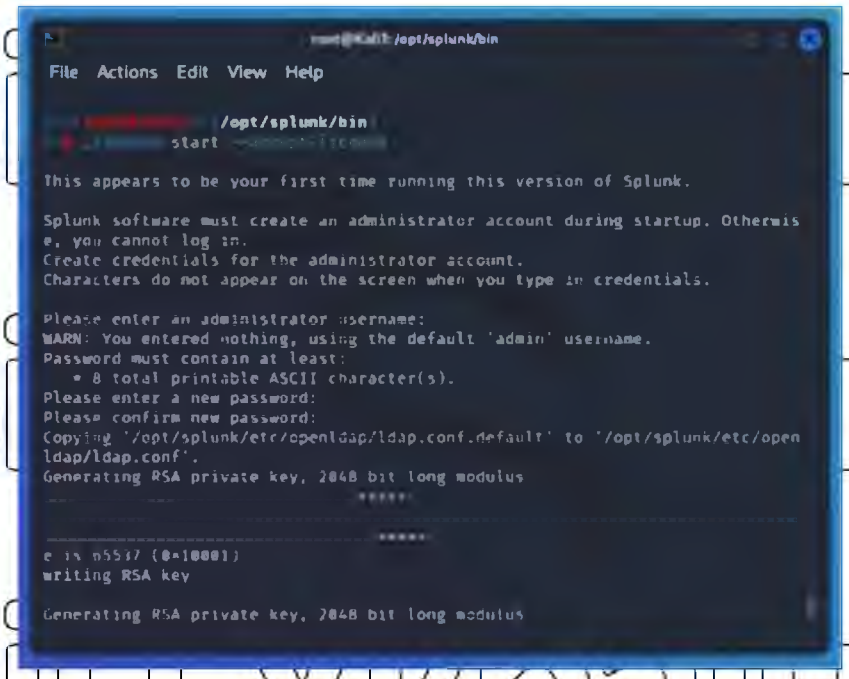


Рисунок 3.68 – Запуск додатку Splunk

Після того, як додаток було встановлено переходимо у веб браузер та в пошуковий рядок вставляємо адресу віртуальної машини.

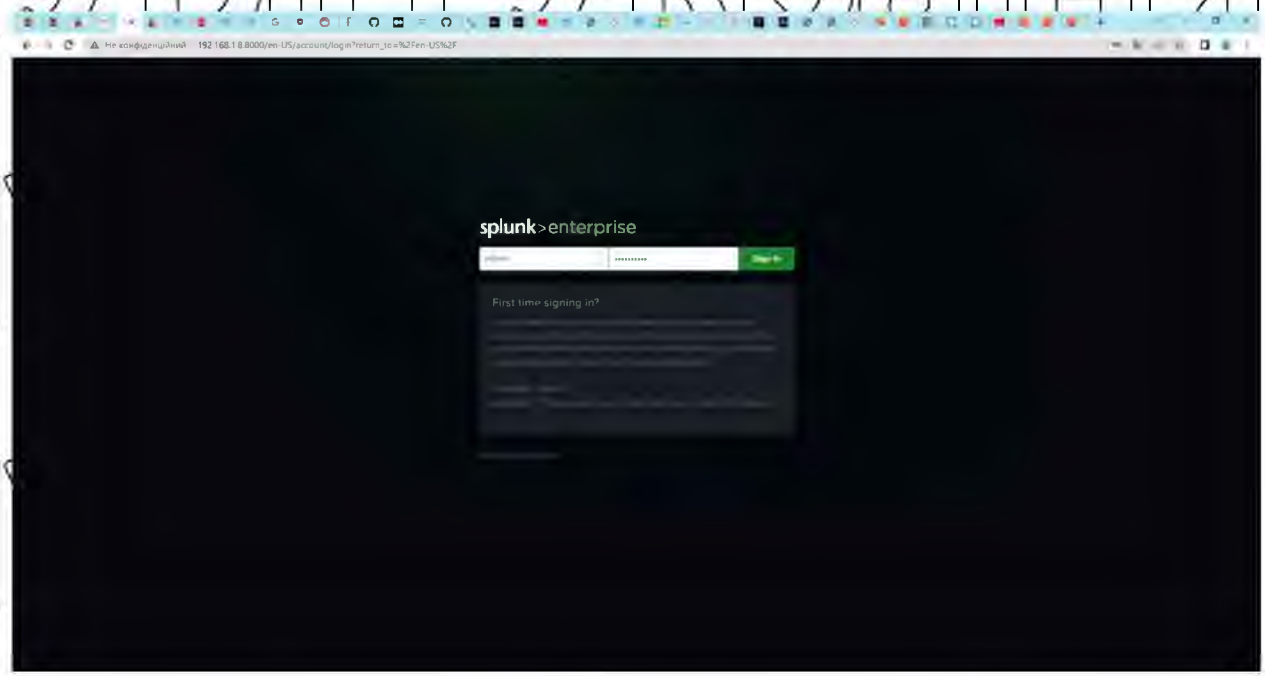


Рисунок 3.69 – Авторизація у веб-сторінці керування додатком Splunk

Відкривається вікно авторизації, куди слід ввести пароль, який був введений раніше для нового користувача.

Рисунок 3.70 - Стартове вікно додатку Splunk

Для того, щоб не треба було після кожного запуску машини наново запускати додаток, виконуємо команду для запуску процесу при старті ВМ.

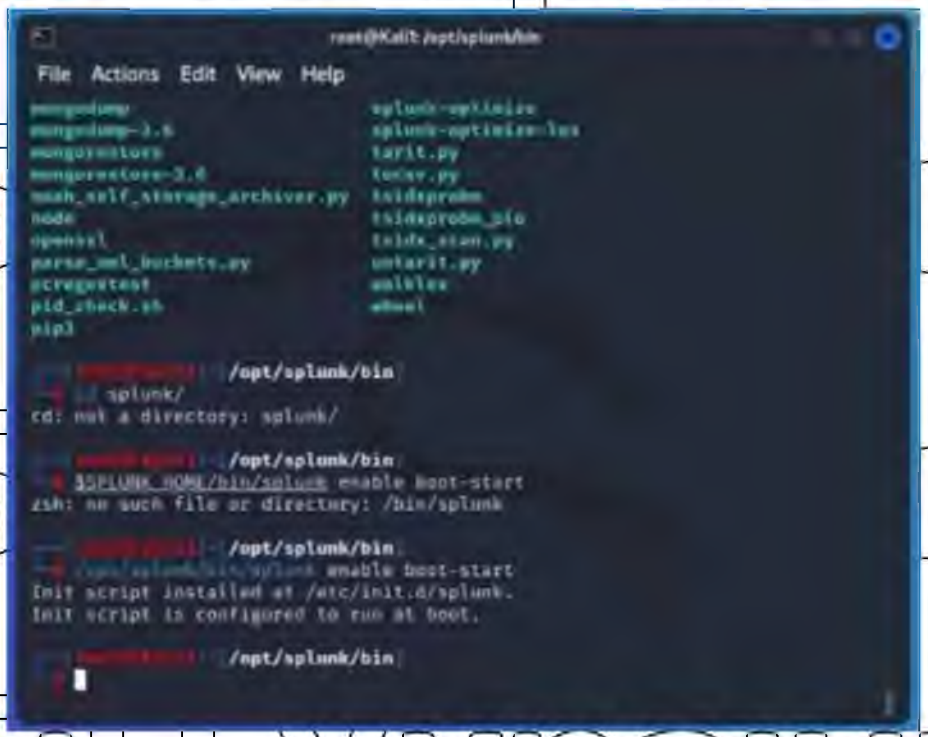


Рисунок 3.71 – Виконання команди запуску додатку при старті машини

Для того, щоб додаток збирав інформацію слід вказати місце, звідки йому брати для опрацювання логи додатку Suricata. Для цього через веб-панель керування переходимо у меню «додати дані» -> «монітор», де вказуємо шлях до даних Suricata та зберігаємо налаштування.

Рисунок 3.72 – Вказання місця зберігання логів для їх аналізу

3.3 Тестування моделі захищеної мережі

3.3.1 Тестування фільтру DNS-адрес Pi-Hole

Після того, як завершене налаштування мережі, слід перевірити її працездатність. Для цього ВМ з Pi-Hole була вказана як основний DNS-сервер на всіх пристроях, та на крайньому маршрутизаторі. Сам додаток Pi-Hole дозволяє в режимі реального часу переглядати, які запити блокуються, а які дозволяються. Зручно виводить статистику у формі діаграм та дозволяє переглядати їх деталі.

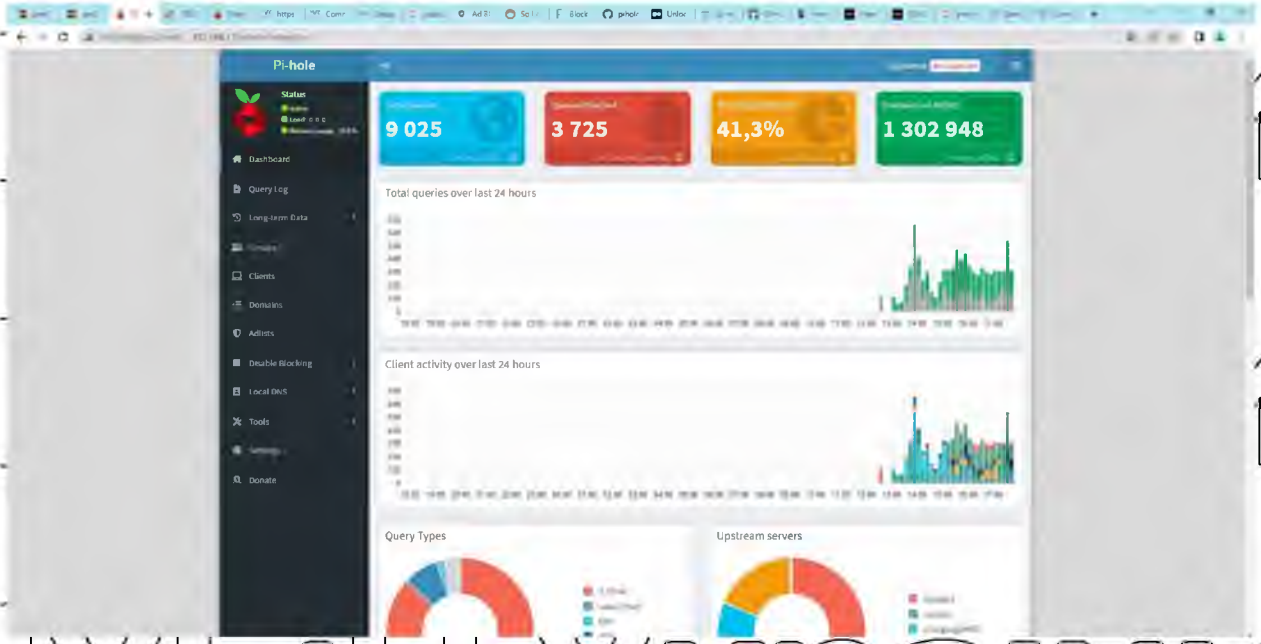


Рисунок 3.73 – Загальна статистика роботи Pi-Hole

З отриманих результатів видно, що система за 5 годин роботи заблокувала більше 3700 шкідливих запитів, що складає більш ніж 41% від усього трафіку, що заходив в мережу. Результативність системи доведена.

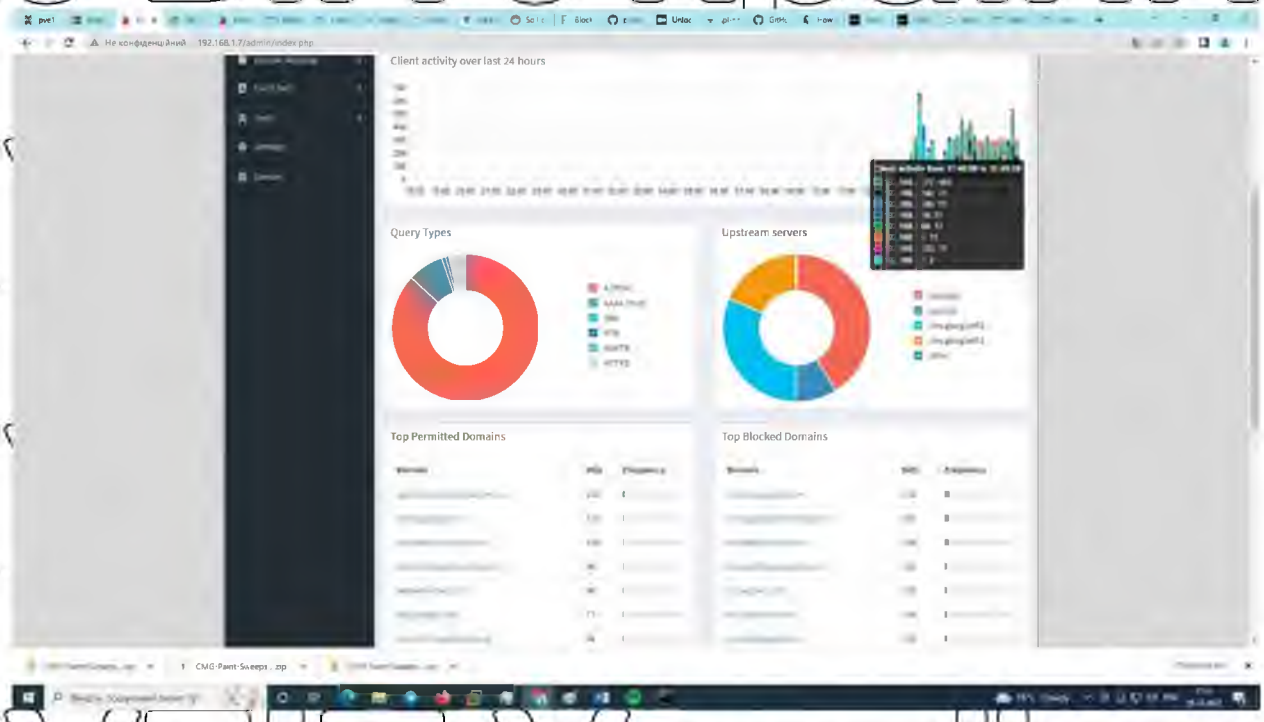


Рисунок 3.74 – Кругова діаграма по типам запитів та серверів

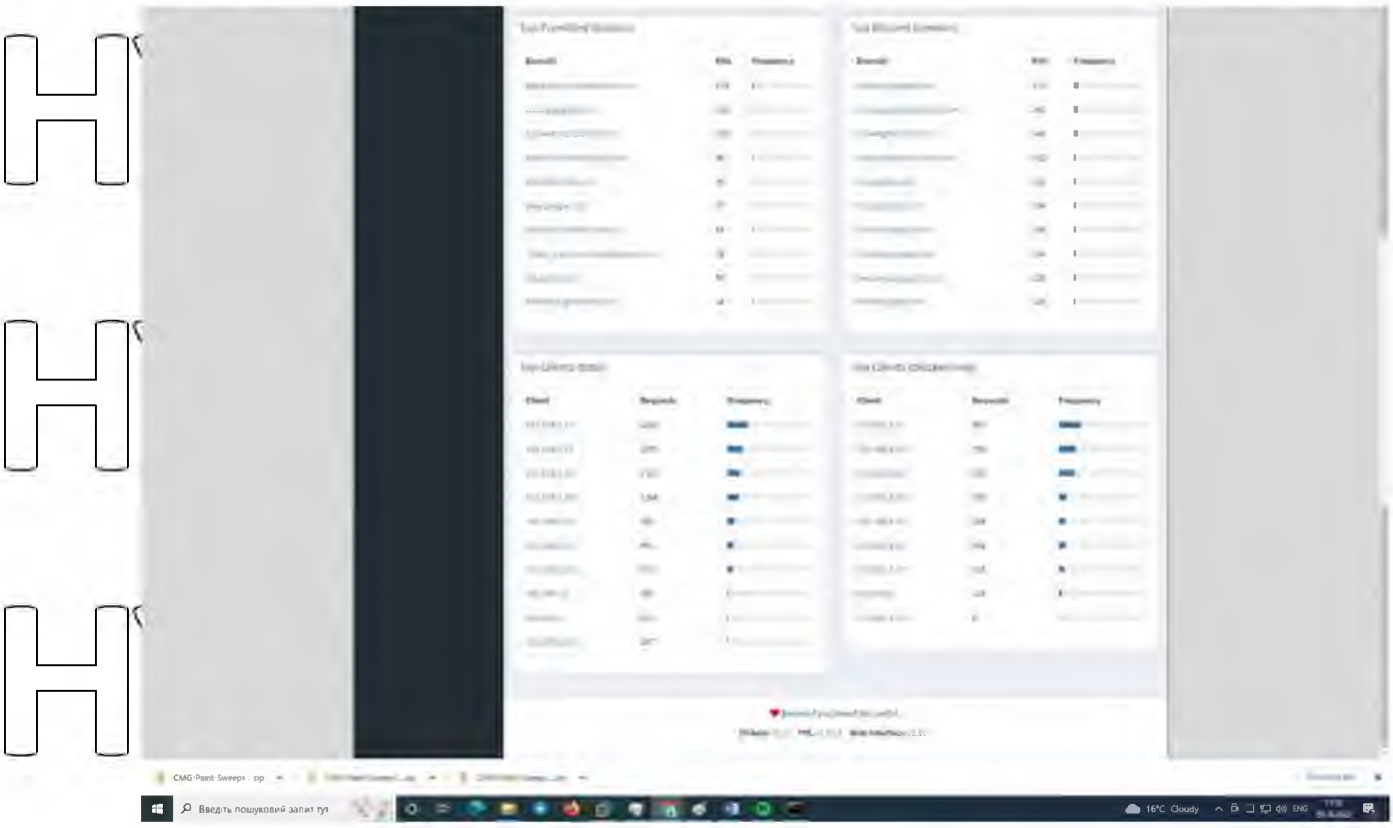


Рисунок 3.75 – Топ дозволених та заборонених доменів по відвідуваності

Окрім загальної інформації про заблоковані загрози Pi-Hole надає можливість перегляду інформації по тому, до яких заборонених доменів йде найбільше звертань, від яких клієнтів йде найбільше запитів – як в цілому, так і шкідливих зокрема.

3.3.2 Тестування IPS Suricata та платформи Splunk

Після того, як було налаштовано зв'язку системи виявлення вторгнень Suricata та платформи Splunk остання почала отримувати системні сповіщення від першої. Всього за годину системою було надіслано 20 сповіщень про порушення правил безпеки та блокування відповідного трафіку, що дає змогу стверджувати, що така система є необхідною частиною мережі будь якого закладу. Сама плафторма Splunk надає можливість відсортувати сповіщення зручним чином, аби як найдетальніше оцінити стан безпеки мережі.

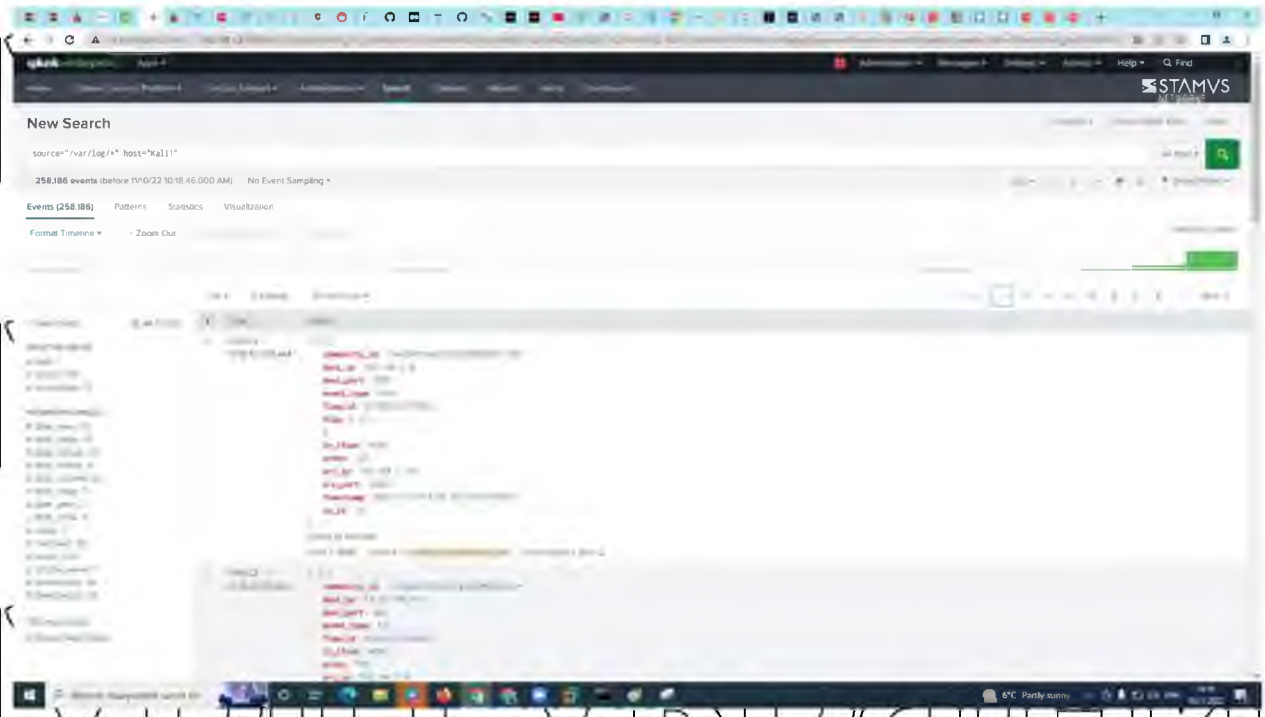


Рисунок 3.76 – Системні сповіщення від Suricata

Окрім можливості сортувати сповіщення, Splunk також надає можливість будувати графіки для розуміння динаміки зміни поведінки трафіку в мережі та власного реагування на це.

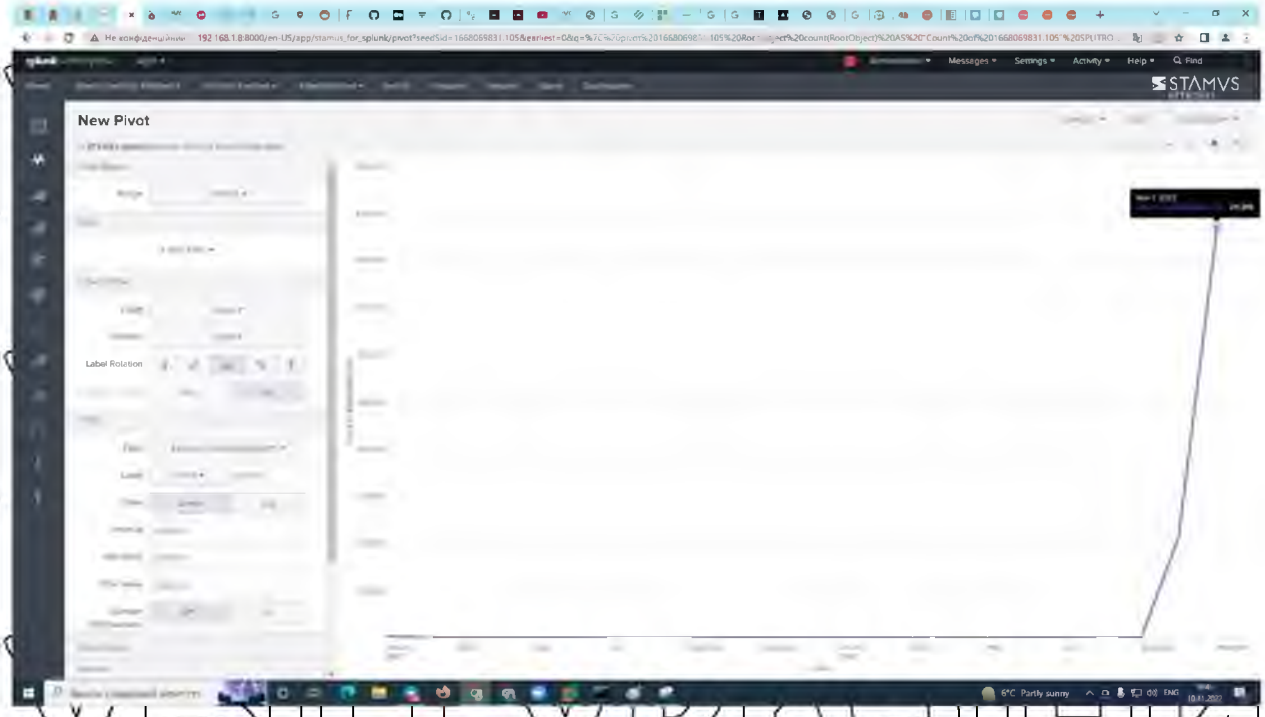


Рисунок 3.77 – Графічне відображення сповіщень від Suricata

ВИСНОВКИ

В ході роботи було досліджено методи захисту інформації в локальних мережах, а також спроектовано модель мережі навчального закладу та системи захисту інформації в її межах.

Важливість даної теми пояснюється тим, що для України питання захисту інформації особливо гостро постало у 2014 році через події анексії Криму військами російської федерації та початку бойових дій у Луганській та Донецькій областях. Починаючи з цього часу наша держава постійно атакується як фізично, так і в цифровому просторі. Повномасштабне вторгнення рф в Україну також внесло свій вклад у кібербезпеку. Згідно рейтингу кіберсили держав світу, оприлюдненого Гарвардським Центром науки і міжнародних відносин Белфера, за 2022 рік Україна посідає 12 місце, що значно краще ніж було у 2020 році – тоді вона посідала 20 місце, а в рейтингу захисту державних ресурсів Україна знаходиться аж на 2 місці.

Модель «цибулини» показує, що чим більше шарів захисту мають дані, тим зловмиснику складніше викрасти дані з неї. Через що експерти рекомендують будувати мережу з декількома рівнями апаратного та програмного захисту.

В межах роботи було побудовано модель мережі, де мережеві пристрої були з емульовані у віртуальній машині зі встановленим додатком EVE-NG, а інші ресурси були відтворені завдяки серверній системі віртуалізації Proxmox VE. На хостах під управлінням PVE було розгорнуто систему виявлення загроз IPS Suricata, платформу Splunk та фільтр DNS-адрес Pi-Hole.

З отриманих результатів видно, що фільтр DNS-адрес Pi-Hole за 5 годин роботи заблокував більше 3700 шкідливих запитів, що складає більш ніж 41% від усього трафіку, що заходив в мережу. Всього за годину системою IPS Suricata було надіслано 20 сповіщень про порушення правил безпеки та блокування відповідного трафіку, що дає змогу стверджувати, що така система є необхідною частиною мережі будь якого закладу. Результативність системи доведена.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Топ 10 cyber risks for business URL: https://10guards.com/en/articles/2022-top-10-cyber-risks-for-business/ (дата звернення: 13.08.2022).

2. Top 7 cybersecurity trends in 2022 URL: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/top-7-cybersecurity-trends-in-2022/# (дата звернення: 15.08.2022).

3. Cybersecurity threats 2022 URL: https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/ (дата звернення: 20.08.2022).

4. Cyber-power National Index 2022 https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (дата звернення: 10.08.2022).

5. Threat detection methods URL: https://www.snowflake.com/guides/threat-detection-methods (дата звернення: 22.08.2022).

6. What are the different methods of threat detection URL: https://socradar.io/what-are-the-different-methods-of-threat-detection/ (дата звернення: 19.08.2022).

7. Think like a hacker: 3 cybersecurity models used to investigate intrusions URL: https://www.comptia.org/blog/think-like-a-hacker-3-cybersecurity-models-used-to-investigate-intrusions (дата звернення: 16.08.2022).

8. Проблеми інформаційної безпеки освіти в умовах глобалізації URL: https://er.knutd.edu.ua/bitstream/123456789/14498/1/PIONBUG_20191004_P125-126.pdf (дата звернення: 23.08.2022).

9. What switches are best for school districts URL: https://info.hummingbirdnetworks.com/blog/bid/315722/what-switches-are-best-for-school-districts (дата звернення: 26.08.2022).

10. How many firewalls do you need URL: https://www.techtarget.com/searchsecurity/tip/How-many-firewalls-do-you-need (дата звернення: 01.09.2022).

11. Network availability and high availability networks URL: https://netcraftsmen.com/network-availability-and-high-availability-networks/ (дата звернення: 28.08.2022).

12. What is a UPS and How Does it Protect Your Network? https://ltnow.com/blog/ups-protect-network/ (дата звернення: 25.08.2022).

13. Join two network with different ISP https://serverfault.com/questions/847702/join-two-network-with-different-isp (дата звернення: 03.09.2022).

14. Proxmox Virtual Environment URL: https://www.proxmox.com/en/proxmox-ve (дата звернення: 07.12.2021).

15. Eve-ng network emulation URL: https://www.eve-ng.net/ (дата звернення: 03.02.2022).

16. How to add cisco IOU/IOL to EVE-NG URL: https://networkhunt.com/how-to-add-cisco-iou-iol-to-eve-ng/ (дата звернення: 20.09.2022).

17. How to install xrdp on Debian 10 URL: https://tecadmin.net/how-to-install-xrdp-on-debian-10/ (дата звернення: 17.09.2022).

18. How to create PVE cluster URL: https://pve.proxmox.com/wiki/Cluster_Manager (дата звернення: 26.07.2022).

19. Network-wide protection URL https://pi-hole.net/ (дата звернення: 11.02.2021).

20. Suricata: home URL: https://suricata.io/ (дата звернення: 03.10.2022).

21. SPLUNK короткий посібник https://coderlessons.com/tutorials/bolshie-dannye-i-analitika/vyuchit-splunk/splunk-kratkoe-rukovodstvo (дата звернення: 20.10.2022).

22. Стаття 32: https://constitution.in.ua/articles/32/ (дата звернення: 02.06.2022).

23. Решетніков Д.Ю., науковий керівник Лахно В.А. «Безпека інформації в локальній мережі», XII Міжнародна науково-практична конференція молодих вчених «Інформаційні технології: економіка, техніка, освіта ‘2021» (11-12 листопада 2021 року Київ, НУБіП України) с.152-153 URL: https://drive.google.com/file/d/1LhyVBHBvpMKiV3gIJFsF3EKv_n6MfY2L/view (дата звернення: 29.06.2022).

24. Про затвердження Указу Президента України "Про продовження строку дії воєнного стану в Україні" URL: https://zakon.rada.gov.ua/laws/show/2500-20#Text (дата звернення: 21.08.2022).

25. Закон України Про захист персональних даних URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 03.06.2022).

26. Указ Президента України №341/2022 URL: https://www.president.gov.ua/documents/3412022-42617 (дата звернення: 17.09.2022).

27. 4 Ways to Detect Cybersecurity Threats URL: https://goavant.net/blog/guide-to-cyber-threat-detection/ (дата звернення: 13.05.2022).

28. A Comprehensive Cybersecurity Defense Framework for Large Organizations URL: https://www.semanticscholar.org/paper/A-Comprehensive-Cybersecurity-Defense-Framework-for-Smith/35602543da0c0dc35f1069587f7c62684f80fc93 (дата звернення: 11.08.2022).

29. The Layered Cybersecurity Model for Small & Medium Business Protection URL: https://medium.datadriveninvestor.com/layered-cyber-security-model-for-small-medium-business-protection-64b293133de4 (дата звернення: 04.09.2022).

30. Cybersecurity in the Three Lines Model URL: https://www.linkedin.com/pulse/cybersecurity-three-lines-model-jerry-perullo (дата звернення: 29.10.2022).

31. Конституція України : права, свободи та обов'язки людини і громадянина URL: https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-ii (дата звернення: 01.11.2022).

32. 11 найпотужніших програмних засобів CyberSecurity у 2021 році URL: https://uk.myservername.com/top-11-most-powerful-cybersecurity-software-tools-2021 (дата звернення: 30.07.2022).

33. Top 10 Kali Linux Tools For Hacking URL: https://www.geeksforgeeks.org/top-10-kali-linux-tools-for-hacking/ (дата звернення: 09.09.2022).

34. Top 25 best Kali Linux tools URL: https://linuxhint.com/top-25-best-kali-linux-tools/ (дата звернення: 11.09.2022).

35. Splunk URL: https://techexpert.ua/it-products/splunk-platform/ (дата звернення: 25.09.2022).

36. Закон України про вищу освіту https://zakon.rada.gov.ua/laws/show/1556-18#Text (дата звернення: 05.07.2022)

37. Splunk Enterprise URL: https://roi4cio.com/catalog/product/splunk-enterprise (дата звернення: 26.09.2022).

38. Splunk TA for Suricata URL: https://splunkbase.splunk.com/app/2760 (дата звернення: 20.09.2022).

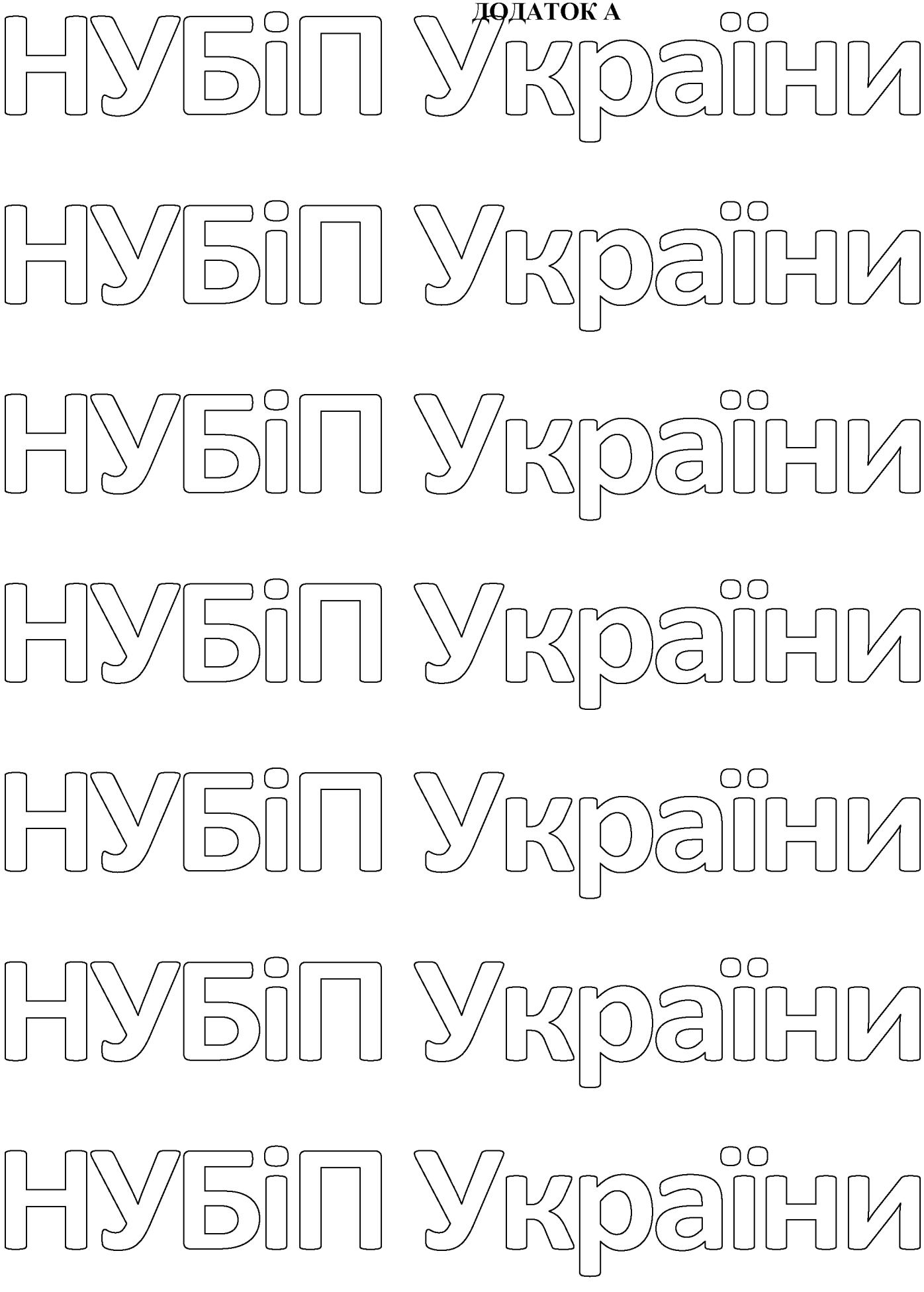
39. Решетніков Д.Ю., науковий керівник Лахно В.А. «Кібератака на локальну мережу та методи захисту», XIII Міжнародна науково-практична конференція молодих вчених «Інформаційні технології: економіка, техніка, освіта '2022» (26-27 жовтня 2022 року Київ, НУБіП України) с.118-119 URL: https://drive.google.com/file/d/1f2AWPKVqk3WOs2Eh0q6fSuA2qpqQeD97/view (дата звернення: 10.11.2022).

40. Open Source IDS Tools: Comparing Suricata, Snort, Bro (Zeek), Linux URL: https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview (дата звернення: 28.08.2022).

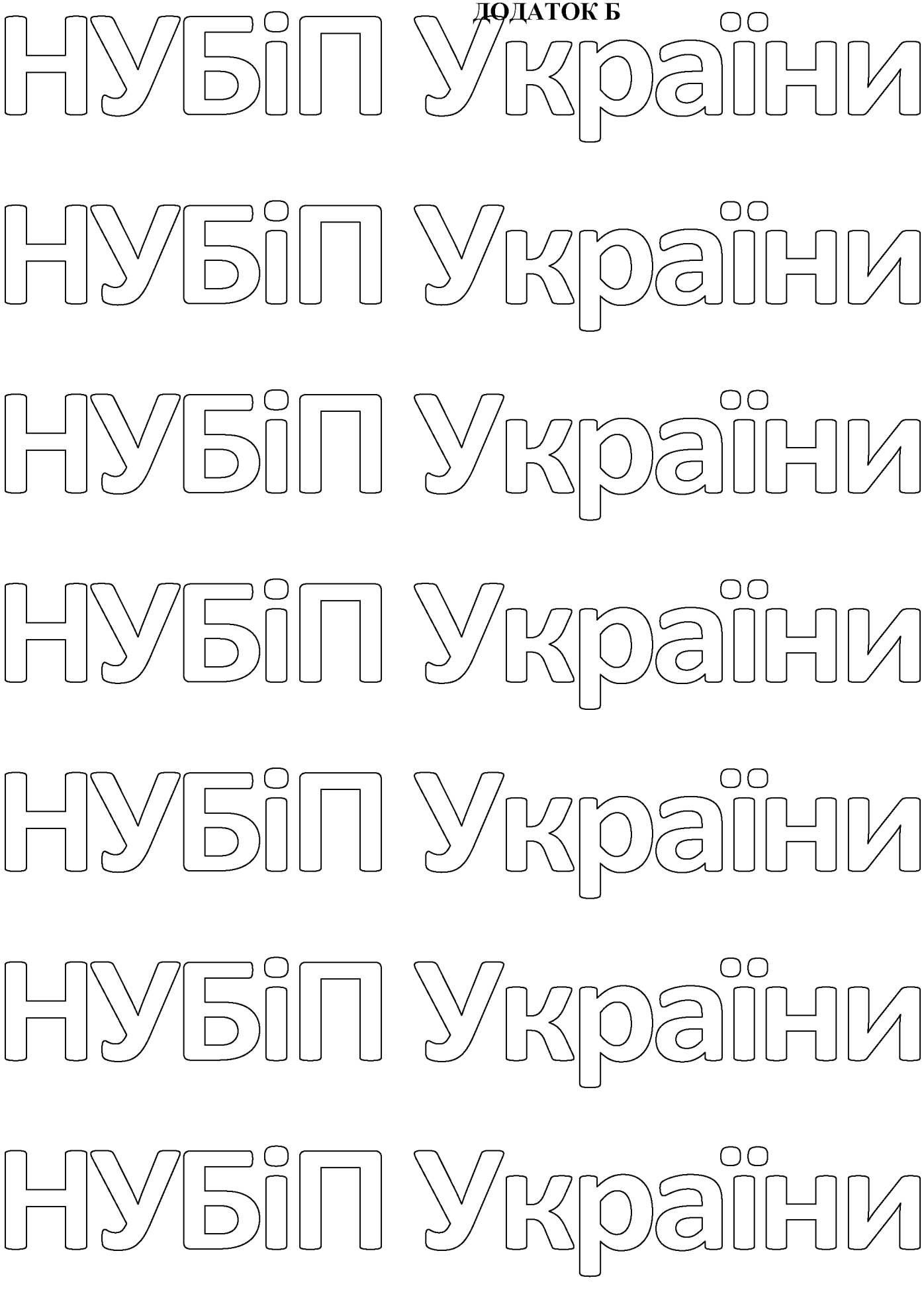
41. Installing & Configuring Suricata URL: https://www.youtube.com/watch?v=UXKbh0jPPpg (дата звернення: 15.09.2022).

42. Закон України «Про основні засади забезпечення кібербезпеки України» https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 19.08.2022).

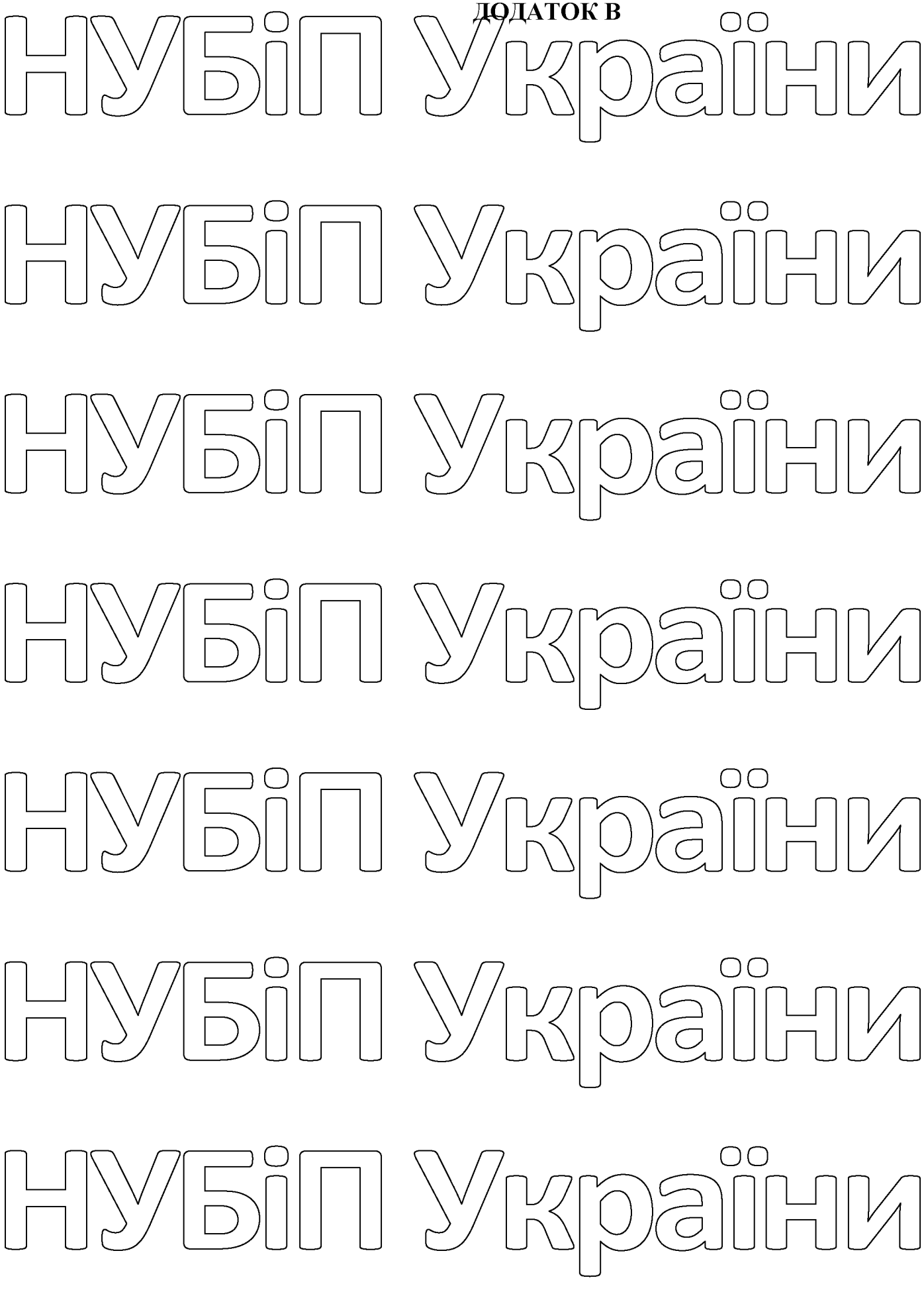
ДОДАТОК А


НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України

ДОДАТОК Б


НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України

ДОДАТОК В


НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України

ДОДАТОК Г

НУБіП України

НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України
НУБіП України