ВСТУП

Бакалаврська робота присвячена підвищенню безпеки в мережі компанії «ЮЛерн».

Питання забезпечення мережевої безпеки, стоїть на першому місті для будь-якого підприємства. Оскільки ігнорування безпеки роботи мережі, може привести до суттєвих збитків та втрати важливої інформації. Разом з цим, існують певні проблемні питання щодо реалізації таких рішень. Основну роль у забезпечені мережевої безпеки, відіграють апаратні комплекси та розділ мережі на безпечні внутрішні підрозділи. Застосування новітніх засобів безпеки, є важливим питанням та забезпечує безперебійну роботу інформаційної складової підприємства, отже тема дипломного проекту, є актуальною.

Метою роботи, є розроблення практичних рекомендацій для підвищення ефективності протидії несанкціонованого доступу до мережі підприємства «ЮЛерн». та запобігання зовнішнім атакам.

Об’єктом дослідження, є процеси забезпечення безпеки, моделі та архітектура мережі підприємства «ЮЛерн»,

Предмет дослідження – методи проектування збору, обробки та зберігання статистичної інформації щодо аналізу мережевої безпеки підприємства «ЮЛерн».

Завдання:

— Проаналізувати мережевий трафік підприємства «ЮЛерн».

— Визначити засоби виявленням і блокуванням підозрілих пакетів.

— Дослідити способи фільтрації мережевого трафіку, у тому числі і повідомлень.

— Проаналізувати роботу брандмауерів, проксі-серверів та серверів NAT.

Завдання:

Проаналізувати мережевий трафік підприємства «ЮЛерн».

Визначити засоби виявленням і блокуванням підозрілих пакетів.

Дослідити способи фільтрації мережевого трафіку, у тому числі і повідомлень.

Проаналізувати роботу брандмауерів, проксі-серверів та серверів NAT.

На підставі проведеного аналізу, запропонувати рекомендацій, щодо удосконалення забезпечення мережевої безпеки підприємства «ЮЛерн».

1. АНАЛІТИЧНИЙ ОГЛЯД РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Аналіз підходів до забезпечення безпеки в мережі

Незважаючи на розвиток інформаційних технології, запобігання мережевих атак, і досі потребує постійного моніторингу всіх систем мережі і залишаються важливим компонентом в роботі компанії. Загрози можливо поділити на зовнішні, внутрішні або корпоративні. На рисунку 1.1 , зображено мережеве TCP-з'єднання, з використанням фільтрації даних, для попередження зовнішніх атак.

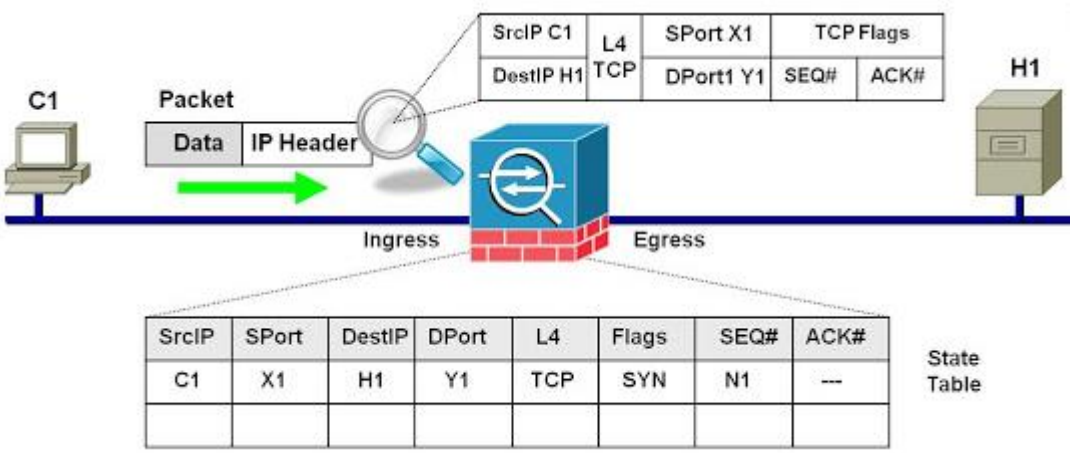


Рисунок 1.1. Мережеве з'єднання за допомогою протоколу TCP.

Швидше за все, ці атаки будуть включати одне або декілька з наступних дій:

1. Розподілена відмова в обслуговуванні (DDoS) - це скоординована атака з багатьох пристроїв, званих зомбі, з метою ослаблення або припинення публічного доступу до веб-сайту та ресурсів організації.

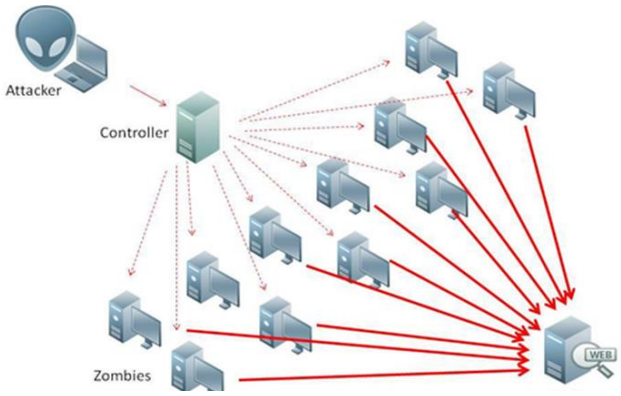


Рисунок 1.2. Розподілена відмова в обслуговуванні.

Атаки відмови в обслуговуванні можуть бути виявлені у різних формах, але їх об’єднує спільна мета, це зупинити доступ до будь-якого ресурсу, наприклад доступу до Інтернет, локальної мережі, корпоративної мережі, Інтернет-сторінок, електронної пошти, тощо.

Для реалізації атаки відмови в обслуговуванні існує декілька способів, самими розповсюдженими, є загрузка по стеку протоколу TCP і атаки на сервер DNS.

Атаки на стек протоколу керування передачею TCP блокують Веб-трафік, якій проходить відповідно по протоколам HTTP та HTTPS і для запобігання нескінченної передачі перевантаженого каналу, необхідно встановлювати обмеження на кількість разів, коли пакет може бути повторно надісланий, перш ніж повністю вимкнути з'єднання.

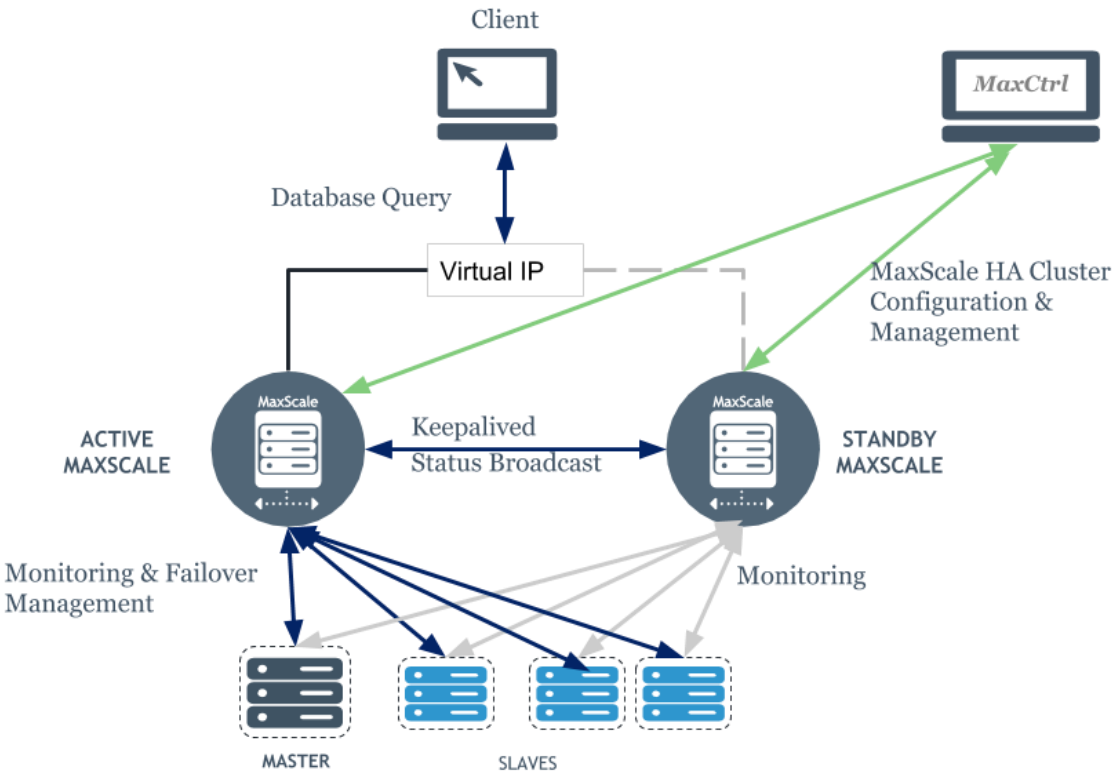


Рисунок 1.3. Розподілена відмова в обслуговуванні.

Відмови в обслуговуванні можуть бути направлені на сервери доменних імен DNS, по протоколу UDP.

За даними аналітичних сайтів, за минулий рік, з 7 вересня по 6 грудня, було зафіксовано 22 млн. кібератак в Україні, більшість з яких була направлена саме на протоколи TCP та UDP.

Рисунок 1.4 Аналітичні дані зафіксованих кібер-атак в Україні.

2. Крадіжка конфіденційної інформації — це тип атаки, при якій сервери або вузли мережі організації піддаються ризику крадіжки конфіденційної інформації.

3. Розповсюдження шкідливих програм — це тип атак, при яких до вузлів організації впроваджується шкідливе програмне забезпечення, яке завдає шкоди інформації або мережевому з'єднанню.

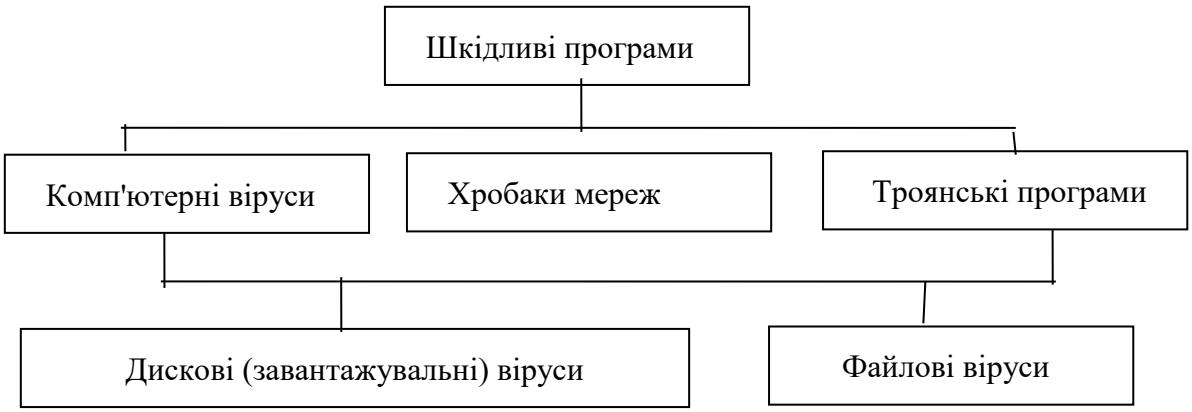


Рисунок 1.5. Схема класифікації шкідливих програм.

1.2. Аналіз засобів виявленням і блокування несанкціонованого доступу та втручання до інформаційних технологій компанії.

Забезпечення безпеки інформаційних технологій, комплексна проблема, яка охоплює правові, інформаційні та апаратні компоненти, а також розробку та вдосконалення інформаційно-комунікаційної системи на підприємстві.

Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати необхідні засоби і побудувати надійну систему захисту. [3] Нижче розглянуто засоби забезпечення інформаційної безпеки, її конфіденційності і водночас доступності.

Таблиця 1.1 Системи забезпечення мережевої безпеки.

Назва системи забезпечення мережевої безпеки	**Основні задачі**
Security information management, SIM	Аналіз інформаційної безпеки на основі збору даних, таких як файли журналів.
Network-based IDS, NIDS	Мережева система виявлення вторгнень
Host-based intrusion detection system, HIDS	Системи виявлення вторгнень на основі хоста
Security information and event management, SIEM	Аналіз у режимі реального часу попереджень про небезпеку, яка генеруються програмами та мережевим обладнанням.
Data Leak Prevention, DLP	Програмні або програмно-апаратні засоби для запобігання витоків
Information Protection and Control, IPC	Системи захисту конфіденційної інформації від внутрішніх загроз.
Protocol-based IDS, PIDS	Система, яка відстежує і аналізує комунікаційні протоколи зі зв'язаними системами або користувачами.

Розглянемо основні засоби забезпечення мережевої безпеки:

Управління мережевою безпекою (Security information management, SIM) – це системи, які збирають та аналізують мережевий трафік, для запобігання вторгнень в мережу, кібератак, виявлення шкідливих додатків та руйнування даних. Системи управляння мережевою безпекою збирають інформацію з мережевих пристроїв, вузлів мережі, пристроїв безпеки. В систему управління мережевою безпекою,

входять також задачі ідентифікації та інструменти управління уразливими елементами. До функцій, які виконують системи управління мережевою безпекою, можливо віднести:

— попередження вторгнень та руйнування даних на основі визначених налаштувань;

— відправка звітів, логування та аудит;

— забезпечення необіжного рівня деталізації.

Мережева система виявлення вторгнень (Intrusion detection system Network-based, NIDS), перевіряє мережевий трафік, відслідковуючи вузли мережі, та на основі перевірок, показує вторгнення. Мережева система виявлення вторгнень отримує доступ до мережевого трафіку за допомогою зв’язку з комунікаційним обладнання, таким як маршрутизатори, комутатори, повторювачі, мости, які налаштовані на відображення портів або мережевий TAP пристрій. Традиційна мережева система виявлення вторгнень складається з сенсорів, які переглядають мережевий трафік або журналів і передають аналізатору, аналізатори шукають в отриманих даних признаки шкідливих подій і у разі успішного виявлення, відправляють результати в адміністративний інтерфейс. Залежно від місця розташування системи виявлення вторгнень, діляться на мережеві і вузлові. Мережеві відстежують весь мережевий трафік того сегмента, де вони встановлені, а вузлові відстежують в межах одного комп'ютера. На рисунку 1.6 показана загальна схема розташування мережевих систем виявлення вторгнень.

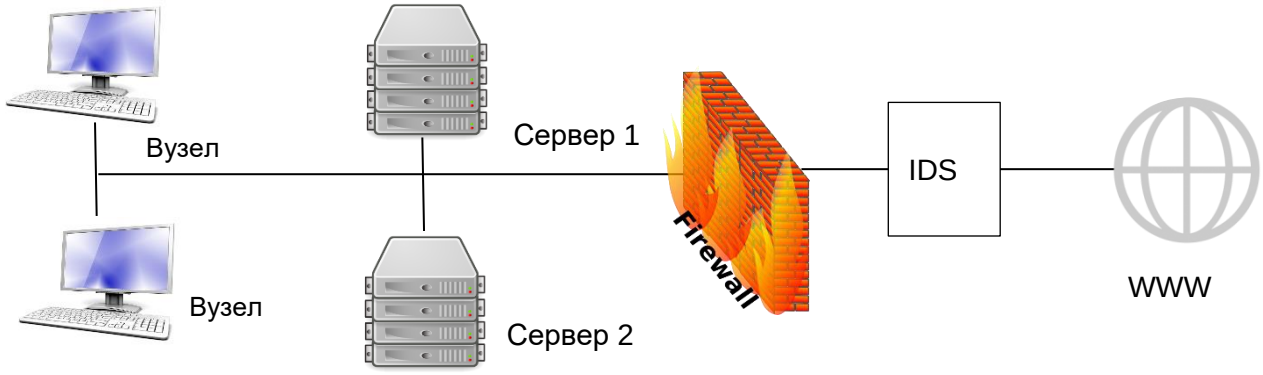


Рисунок 1.6 Схема розташування в мережі систем виявлення вторгнень.

На рисунку 1.7 наведено результат класичної системи виявлення вторгнень Snort. Це система з відкритим кодом, створена Мартином Решем, згодом її придбала компанія Cisco. Система включає в себе сниффер пакетів, підтримує настройку правил і особистих налаштувань.

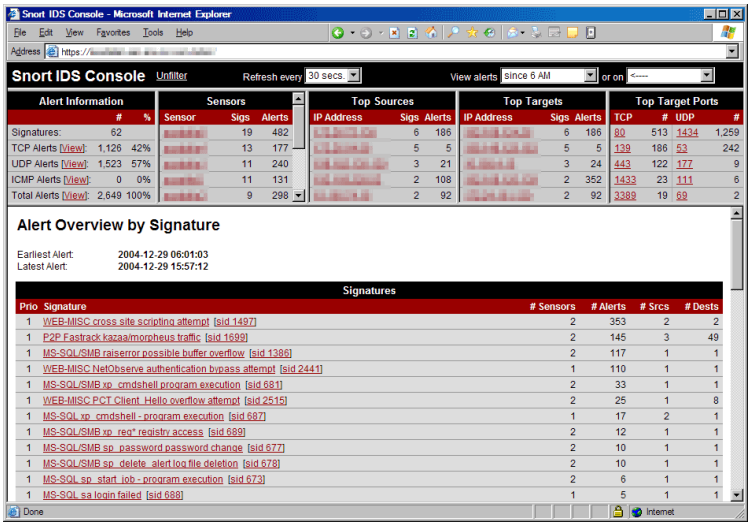


Рисунок 1.7 Система виявлення вторгнень Snort.

На рисунку 1.8 представлено результат роботи системи виявлення вторгнень Suricata. Це система з відкритим вихідним кодом, яка здатна виявляти загрози по налаштованим сигнатурам і підтримує багато модулів виявлення вторгнень в мережу.

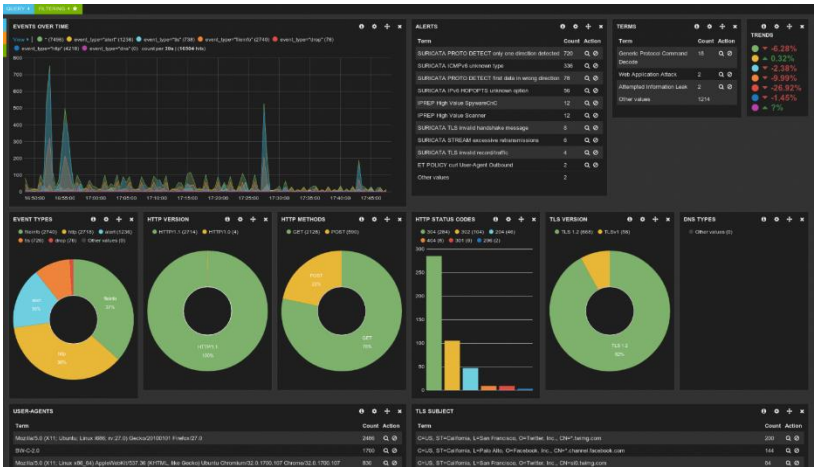


Рисунок 1.8 Система виявлення вторгнень Suricata.

Технології IDS відрізняються різними способами виявлення шкідливої активності в мережевому трафіку і їх можна розділити за наступними типами технологій:

— сигнатурні IDS, які відстежують певні шаблони в трафіку і працюють подібно антивірусному програмному забезпеченню.[6] Недоліками такого підходу, є те, що сигнатури повинні постійно бути актуальними, інакше IDS подібного типу не здатні виявити незнайомі атаки. Сигнатурні системи виявлення вторгнень також можна розділити на два типи, ті які відстежують шаблони, тобто порівнюють мережеві пакети з сигнатурами, і ті, які відстежують стан, тобто порівнюють дії з шаблонами. Під станом, мається на увазі будь-яка зміна в роботі системи або мережі, котра приводить до відхилення еталонної роботи;

— IDS, засновані на аномаліях, тобто системи виявлення вторгнень, які відслідковують поведінку системи перед початком роботи, дивлячись що відбувається при нормальній діяльності системи або мережі і цей період є етапом навчання і зрівнюють з поточною роботою. Такий підхід може бути застосований там, де необхідно виявляти незнайомі атаки. Аномалії, в свою чергу, в даній категорії поділяються на три типи: статистичні IDS, ті які створюють профіль штатної діяльності системи і порівнюють весь прохідний у мережі трафік з діяльністю цього профілю; другі це аномалії протоколів IDS, які аналізують трафік з метою виявлення фрагментів нелегітимного використання протоколів; третій тип, це аномалії трафіку IDS, які виявляють нелегітимні дії в мережевому трафіку

— IDS, засновані на правилах, тобто системи виявлення вторгнень, які. використовують умову програмування засновану на правилі: «ЯКЩО ситуація ТОДІ дія». Такі системи виявлення вторгнень, схожі на експертні системи тим, що приймають рішення на основі логічних висновків і програмування на основі правил. В даному випадку знання, це правила, а аналізовані дані можна назвати фактами, до яких застосовуються правила.

До класифікації систем IDS, також відносяться системи, які діляться по типу аналізованого трафіку:

— IDS, заснована на протоколі (Protocol IDS), які аналізують комунікаційні протоколи зі зв'язаними системами або користувачами;[8]

— IDS, засновані на прикладних протоколах (Application Protocol-based IDS, APIDS), системи, які аналізують данні, переданні з використанням специфічних для певних програм протоколів.[8]

На рисунку 1.9 представлена декомпозиція роботи загальної системи виявлення вторгнень.

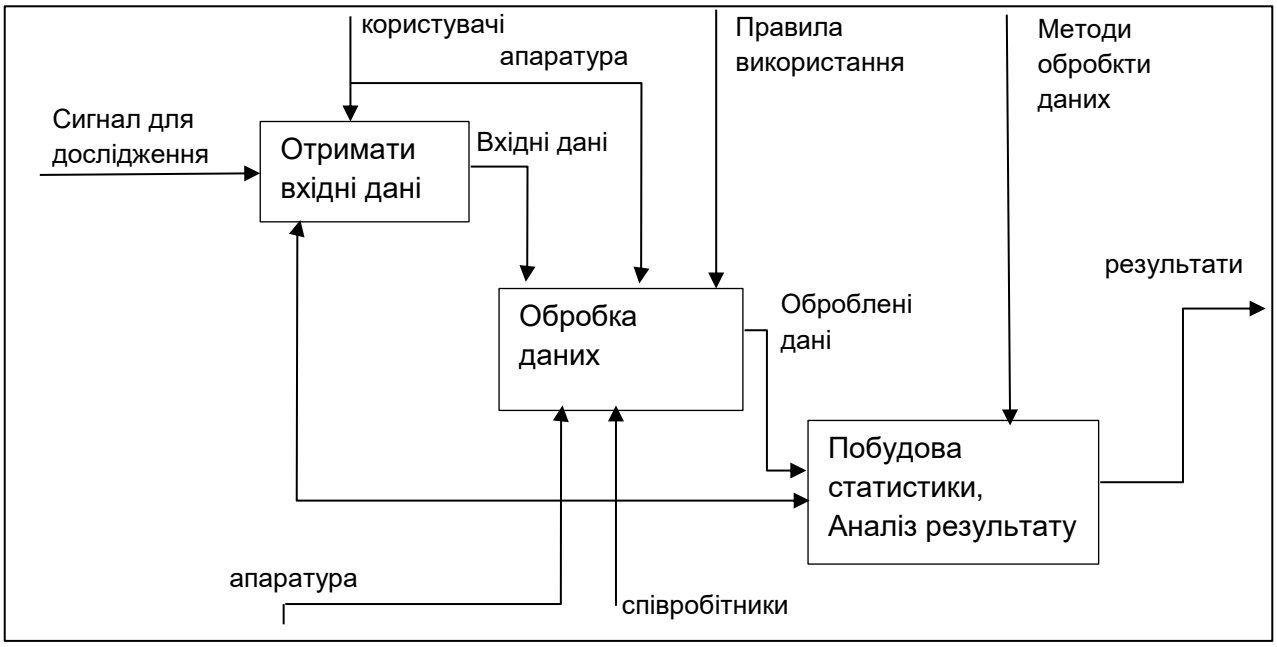


Рисунок 1.9 Декомпозиція роботи загальної системи виявлення вторгнень.

Альтернативою мережевим системам виявлення вторгнень, є вузлові системи виявлення вторгнень (Host-based intrusion detection system, HIDS), які направленні на виявлення вторгнень на самому вузлу мережі, наприклад стаціонарний комп’ютер, ноутбук, сервер, комунікаційне обладнання. Такі системи встановлюються на один хост всередині мережі та захищають тільки його. [10] HIDS аналізують всі вхідні і вихідні пакети подібно мережевим системам виявлення вторгнень, але тільки для одного пристрою. Система HIDS працює за принципом створення снапшотів файлів, тобто робить знімок поточної версії і порівнює його з попередньої, тим самим виявляючи можливі загрози. HIDS

встановлюють на критично важливі вузли мережі, такі як апаратні або програмні сервери.

Для виявлення вторгнень, системи відстежують журнали логування операційної системи, програмного забезпечення та дії користувачів, оброблюють інформацію логування в операційну систему та дії користувача на наявність ознак підозрілої активності.

Інший спосіб виявлення спроб вторгнення, це перевірка файлів конфігурації системи на наявність несанкціонованих змін. Вони також можуть перевіряти ці ж файли на наявність певних відомих шаблонів вторгнення. Наприклад, може бути відомо, що конкретний спосіб вторгнення працює шляхом додавання певної параметра в конкретний файл конфігурації, тоді система виявлення вторгнень знайде цей інцидент.

Незважаючи на те, що системи HIDS обробляють інформацію на одному вузлі мережі, вони не завжди встановлені безпосередньо на пристрої, який вони повинні захищати, деякі системи встановлюються на всіх комп'ютерах мережі, але альтернативою може виступати наявність тільки локального агента, а в деяких випадках системи HIDS, встановлюються віддалено без агента. Незалежно від того, як працюють системи HIDS, більшість з них мають централізовану консоль, з можливістю контролювати кожен екземпляр додатка і переглядати всі результати. На рисунку 1.10 представлено контекстну діаграму IDEF0 виявлення атак систем HIDS.

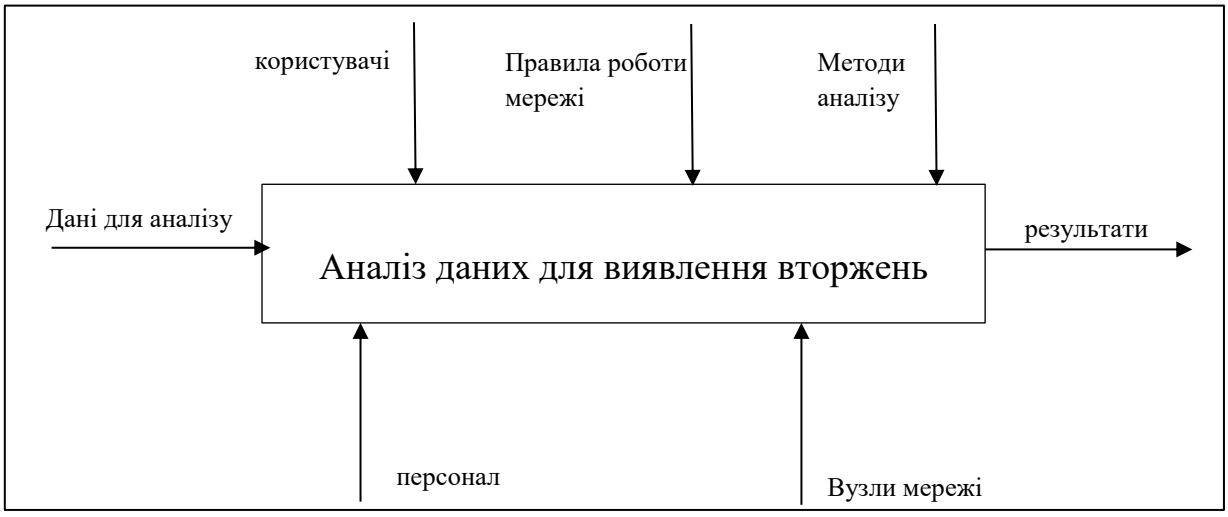


Рисунок 1.10 Контекстна діаграма IDEF0 виявлення втручання системи HIDS.

Розглянемо системи управління безпекою інформації (Security Information Management, SIM) та управління подіями безпеки (Security Event Management, SEM), які спочатку складались з двох систем, але з 2005 року ці поняття об’єднали в одне поняття управління безпекою інформації та подіями (Security information and event management, SIEM).

SIEM збирають інформацію для подальшого аналізу і класифікації системним адміністратором мережі або спеціалістом з безпеки, та. використовують для аналізу дані з наступних джерел:

— інформацію з логування додатків;

— інформацію, отриману з комунікаційного обладнання мережі;

— інформацію, отриману з міжмережевих екранів;

— інформацію, отриману зі сканерів вразливостей;

— інформацію, отриману з CRM-систем;

— інформацію, отриману з антивірусного програмного забезпечення.

На рисунку 1.11 наведено опис основних джерел подій систем SIEM.

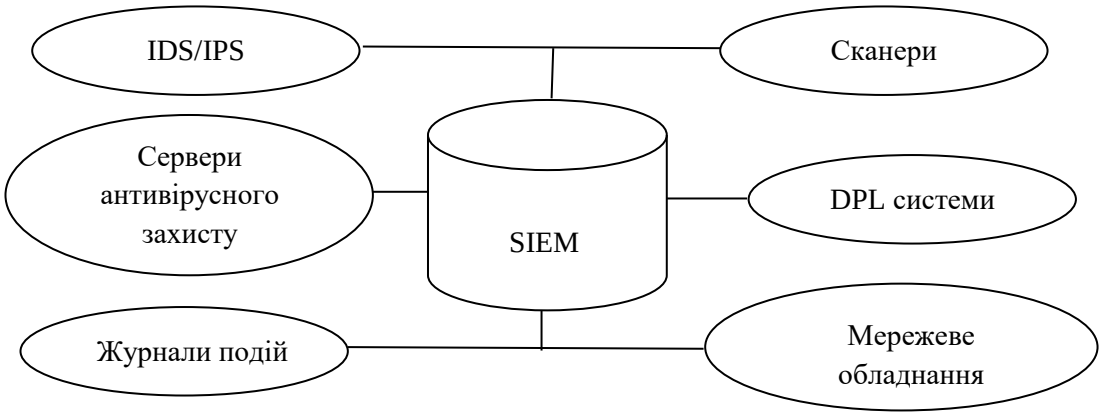


Рисунок 1.11 Опис основних джерел подій систем SIEM.

До лідерів побудови систем SIEM, відносяться:

— компанія Hewlett Packard з системою ArcSight;

— компанія IBM з системою QRadar SIEM;

— компанія Tibco з системою Loglogic;

— компанія McAfee з системою NitroSecurity;

— компанія Splunk;

— компанія LogRhythm.

Розглянемо системи захисту від витоку даних (Data Leak Prevention, DLP), які дозволяють захищати інформацію від несанкціонованого доступу, завдяки аналізу вразливостей протоколів та програмних засобів. На рисунку 1.12 показана загальна схема функціонування системи захисту від витоку даних.

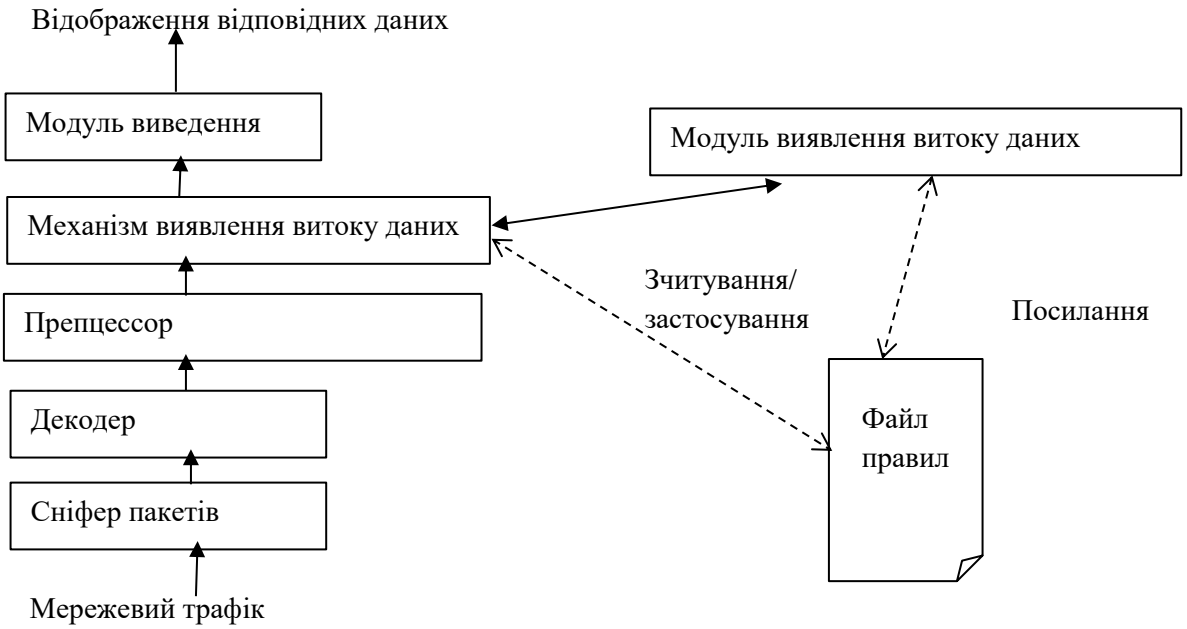


Рисунок 1.12 Загальна схема функціонування системи захисту від витоку даних.

Для запобігання витоку даних, контролюється весь внутрішній і зовнішній трафік мережі. Для моніторингу застосовуються дві схеми перехоплення, серверний і агентський. У першому випадку аналізується трафік на сервері, у другому перехоплення відбувається безпосередньо на робочих станціях. Залежно від потреб, способи перехоплення можуть комбінуватися або використовувати тільки певні модулі системи

Розглянемо технології захисту конференційної інформації (Information Protection and Control, IPC), які блокують підозрілі потоки даних, на основі

відстеження трафіку в комп'ютерній мережі. Системи IPC можна розглядати як задачу відстеження трафіку, на основі активності мережі, в реальному часі і швидкої реалізації реагування щодо запобігання атак.

Рішення класу IPC призначені для запобігання різних видів витоків інформації, корпоративного шпигунства і бізнес-розвідки.

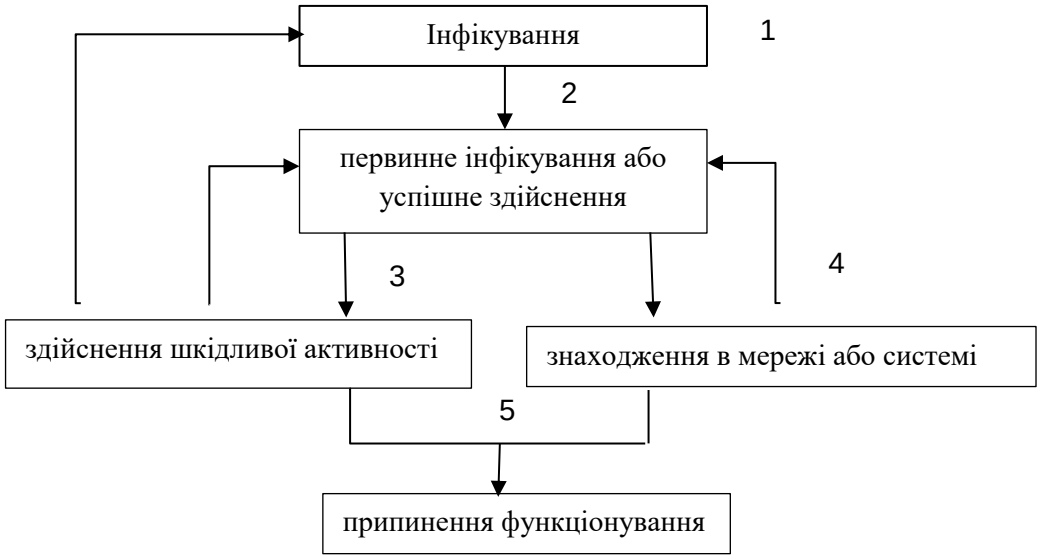


Рисунок 1.13 Життєвий цикл аномальної події в мережі компанії.

На рисунку 1.13, представлена схема функціонування аномальної події в мережі компанії. Розглянемо життєвий цикл аномальної події в мережі компанії, з врахуванням системи доменних імен. Життєвий цикл аномальної події в мережі, можна розділити на п’ять фаз:

— перша, це вторгнення в мережу;

— друга, це первинне інфікування або успішне здійснення з’єднання;

— третє, це здійснення шкідливої активності;

— четверте, це знаходження в мережі або системі;

— п’яте, це припинення функціонування.

Для запобігання витоку інформації, IPC з'єднує в собі дві основні технології: шифрування носіїв інформації і контроль технічних каналів витоку інформації Також в функціонал IPC-систем можуть входити системи захисту від несанкціонованого доступу

2. АНАЛІЗ БІЗНЕС-ПРОЦЕСІВ ТА ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ПІДПРИЄМСТВА «ЮЛЕРН»

2.1 Аналіз бізнес-процесів підприємства “Юлерн”

Бізнес-процеси, будь якої організації, є основою для формування вимог до забезпечення безпеки інформаційно-комунікаційної мережі. Аналіз мережевої безпеки, доцільно починати з визначення завдань і цілей діяльності підприємства.

Поняття бізнес-процес, є багатозначним, насамперед бізнес-процеси безперервні, мають певні входи, тобто постачання ресурсів, виникнення ідеї бізнесу, ідеї нового продукту, послуги тощо і мають виходи у вигляді продукту, що задовольняє потреби споживачів. Таким чином бізнес-процес охоплює всю організацію, зверху до низу. [1]

На рисунку 2.1 розглянуто загальну схему, яка визначає основні бізнес-процеси підприємства «Юлерн», які в свою чергу визначають задачі функціонування інформаційно-телекомунікаційної мережі «Юлерн». Процеси поділяються на зовнішні, та внутрішні. Що означає, що при забезпеченні безпеки, потрібно враховувати різні види атак та вразливостей інформаційно-телекомунікаційної системи. А також поділяти загрози на внутрішні та зовнішні.

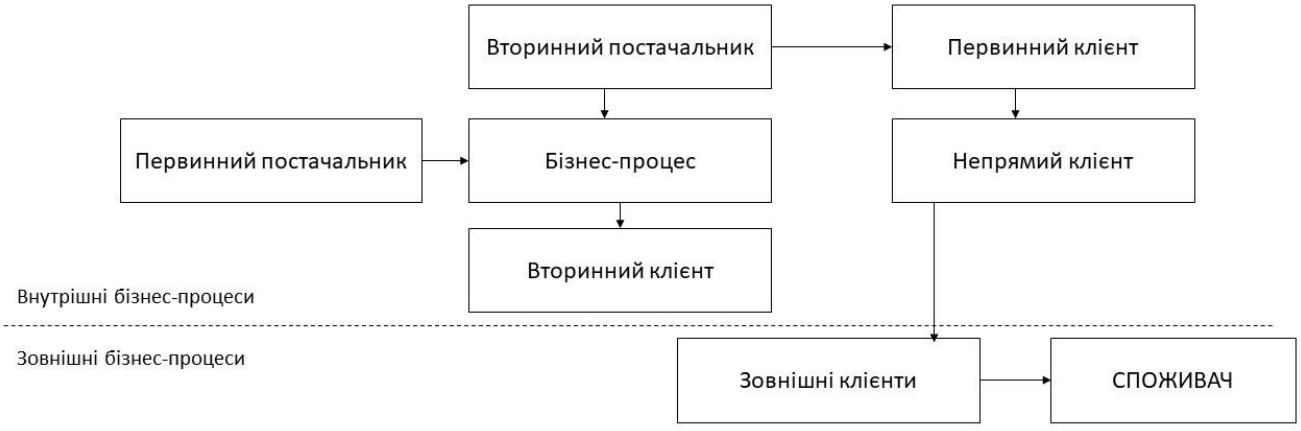


Рисунок 2.1 – Загальна структура мережі підприємства «Юлерн».

Для побудови інформаційної системи для аналізу мережевої безпеки підприємства, потрібно врахувати вимоги бізнесу, тобто бізнес-процеси таким

чином, щоб визначити які ризики може прийняти якісь бізнес, від яких ризиків можливо захистити інформаційно-телекомунікаційну мережу і за допомогою яких інструментів можлива реалізація.

Клієнти, з якими взаємодіє підприємство «Юлерн», розділяються на:

— первинні клієнти, ті, які одержують первинний вихід;
— вторинні клієнти, що знаходяться поза процесом і одержують вторинні виходи;
— непрямі клієнти, що не одержують первинного виходу, але є наступними в ланцюжку, тому пізніший за часом вихід відображається на них.
— зовнішні клієнти, за межами підприємства, які одержують вихід процесу: дистриб'ютори, агенти, роздрібні продавці, інші організації.
— зовнішні непрямі клієнти, споживачі.

До зовнішніх бізнес-процесів, відноситься взаємодія з зовнішніми клієнтами та споживачами. Що вказує на потребу використовувати авторизацію, аутентифікацію, та враховувати стратегію безпечної ідентифікації.

До внутрішніх процесів, відноситься взаємодія з постачальниками, непрямими клієнтами та вторинними клієнтами і постачальниками. Що вказує на потребу керування даними ззовні, враховувати наявність віддаленого доступу, хмарного зберігання даних та інших ресурсів, для будування захищеної мережі.

Ресурсами бізнес-процесів, можуть бути як матеріально-технічні, так і інформаційні.

На рисунку 2.2., показана загальна схема інформаційної технології підприємства «Юлерн», яка вказує на необхідність забезпечити аналіз інформації як апаратних так і програмних ресурсів, також окремо виділити аналіз трафіку меж системою управління даними та користувачами, виділити аналіз інформації, отриманої від інтерфейсів користувачів та аналізувати інформаційні ресурси.

Тобто, для аналізу мережевої безпеки, потрібно враховувати весь набір рішень інформаційно-телекомунікаційної технології, впровадженої на підприємстві «Юлерн», такі, як сегментація, існуючий набір засобів для

забезпечення захисту даних на кожному з сегментів мережі. Для детектування загроз, необхідна ідентифікація:

— користувачів;

— файлів;

— додатків;

— з’єднань.

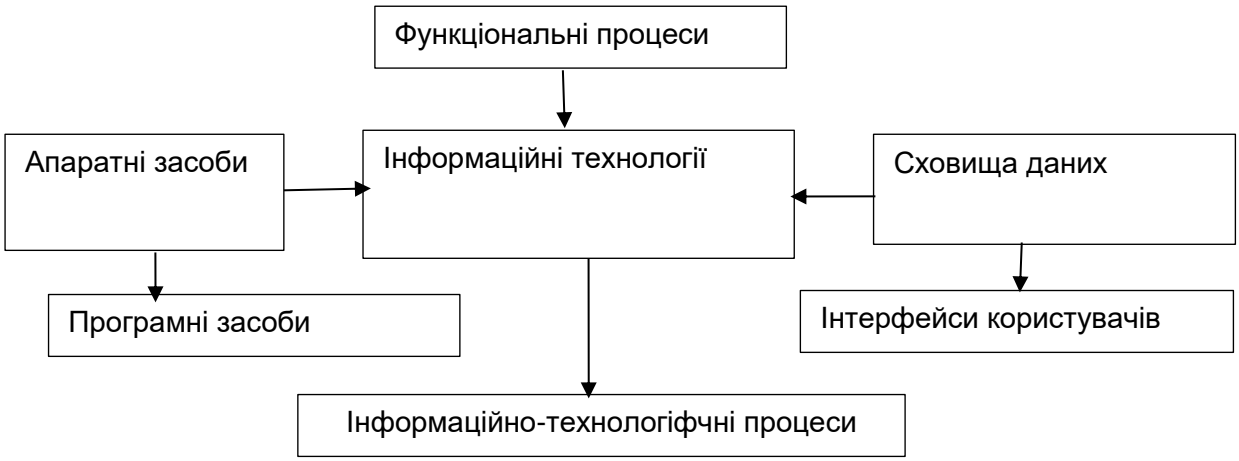


Рисунок 2.2 - Структура інформаційної технології

Таким чином, автоматизування процесу аналізу та визначення загроз, можливо тільки за умови ретроспективи роботи всієї мережі.

Аналіз бізнес-процесів, надає структуровану послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу підприємства, що надає інформацію про необхідний моніторинг інформації:

— створення концептуальної ідеї на етапі підписання договорів;

— процес проектування, якій поступає в межах локальних сегментів;

— етап реалізації, обмін інформацією, обмін частинами кодам;

— етап результату, на якому інформація виходить за рамки локальних сегментів.

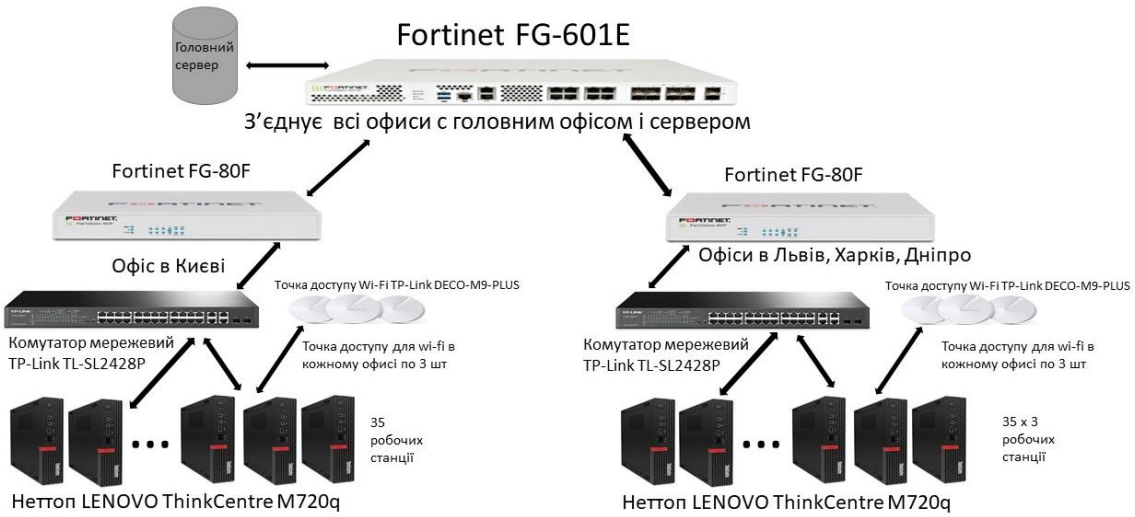


Рисунок 2.3 – Загальна структура мережі підприємства «ЮЛерн»

На рисунку 2.3, зображена загальна структура мережі підприємства «Юлерн», яка показує зв'язок між різними сегментами мережі, що надає інформацію про централізовані канали зв'язку і основні вузли, які можуть бути використані для захисту та аналізу безпеки мережі.

На кожному з вузлів комунікації, можливо впровадити систему моніторингу та аналізу безпеки мережі, завдяки якої виявляти шкідливу інфраструктуру всередині мережі та захистити внутрішні запити, в тому числі і з системою управління базами даних та запобігти небезпечного трафіку.

У рамках будь-якого бізнес-процесу, кінцевим результатом, є випуск продукції або послуги. У підприємстві «Юлерн», кінцевим рішенням, є інформаційний продукт, якій буде критичним для його пошкодження через недосконалі рішення кібербезпеки. Коли співробітники працюють безпосередньо з інстансами, в хмарному середовищі, важливим фактором є своєчасний аналіз небезпечних станів, для оперативного реагування. Таким чином треба використовувати інформацію про архітектуру всієї мережі, рішення безпеки в мережі, які доступні на даний час, ресурси доступні для моніторингу та аналізу безпеки мережі. Таким чином, для забезпечення аналізу безпеки мережі, необхідно визначати політику доступу до бізнес-процесів, тобто до набору бізнес-операцій підприємства та правила і параметри доступу, аутентифікації і видачі інформації на різні мережі і внутрішні ресурси.

2.2 Визначення вимог інформаційної безпеки компанії “Юлерн”

До функцій визначення вимог мережевої безпеки підприємства “Юлерн”, можна віднести формування політики безпеки програмних засобів, які налаштовуються як за допомогою властивостей самих програмних засобів, так і за допомогою додаткового налаштування прав доступу як до самих файлів, так і до запуску програми. Наступним кроком формування політики безпеки, є запобігання відмов апаратних засобів, для чого необхідно налаштовувати як апаратні засоби, так і доступ до всієї мережі. На кожному етапі формування вимог та налаштуванні, потрібно уточнення функцій захисту мережі і програмних засобів.

На рисунку 2.4 показана логічна схема визначення вимог мережевої безпеки, де показані етапи розроблення та застосування методів виявлення слабких місць у мережі, та оцінка досягнутої на певний час захищеності даних.

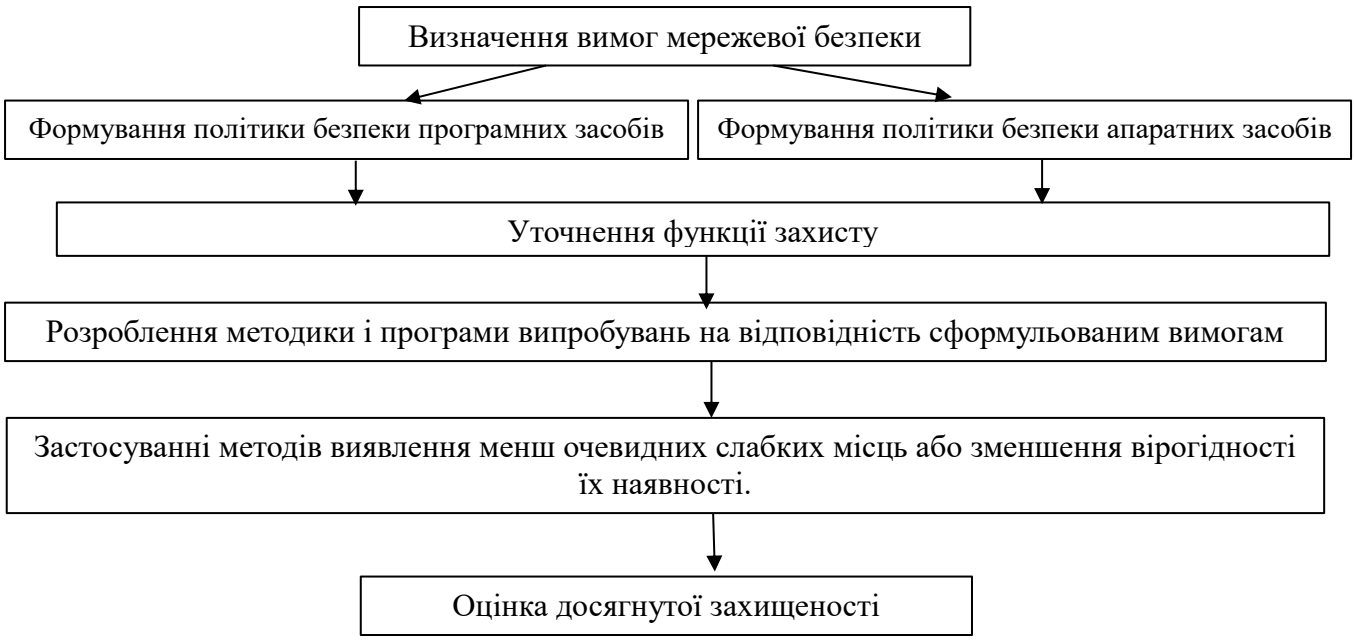


Рисунок 2.4 - Логічна схема визначення вимог мережевої безпеки.

На рисунку 2.5, показано вимоги за якими сформовано основні функції мережевої безпеки підприємства «Юлерн», які призначенні для зберігання внутрішніх ресурсів компанії та запобіганню вторгнень в мережу зовні.

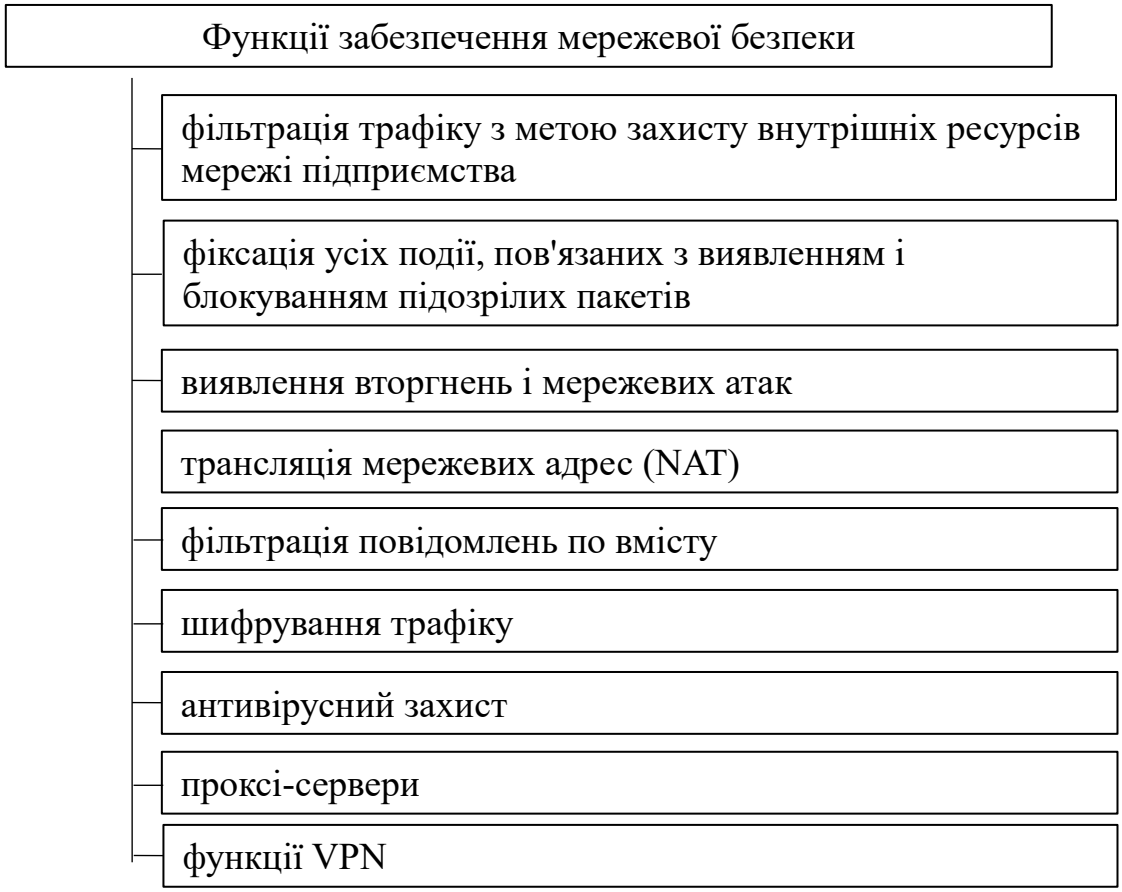


Рисунок 2.5 - Основні функції мережевої безпеки підприємства «ЮЛерн»

Для запобігання інфікування комп’ютерної мережі підприємства, інформаційна система ініціює запит з метою встановлення відповідності між звичайною роботою мережі, операційних систем, додатків з поточною. Використовуючи запит, інформаційна система встановлює на яких рівнях виникла підозра у небезпечній роботі мережі або одного з її вузлів. Модулю повідомлень надсилає серверу щодо дії запобігання небезпеки, в залежності від її типу. В разі успішного завершення боротьби з загрозою, інформаційна система забезпечення мережевої безпеки, здійснює логування даної інформації, для подальшого використання знань про небезпеку та отримання статистичних даних. В разі відсутності успіху у боротьбі з загрозою, інформація передається до відповідних модулів інформаційної системи, для подальшої роботи над урегулюванням небезпечної ситуації.

На відміну від впроваджених методів захисту мережевої безпеки, інформаційна система мережевої безпеки підприємства «ЮЛерн», направлена на налаштування протидії несанкціонованого доступу з урахуванням архітектури мережі компанії, та налаштуванням кожного елемента мережі, в залежності від вимог політики компанії. На рисунку 2.6, зображено дерево функцій захисту мережі «Юлерн»

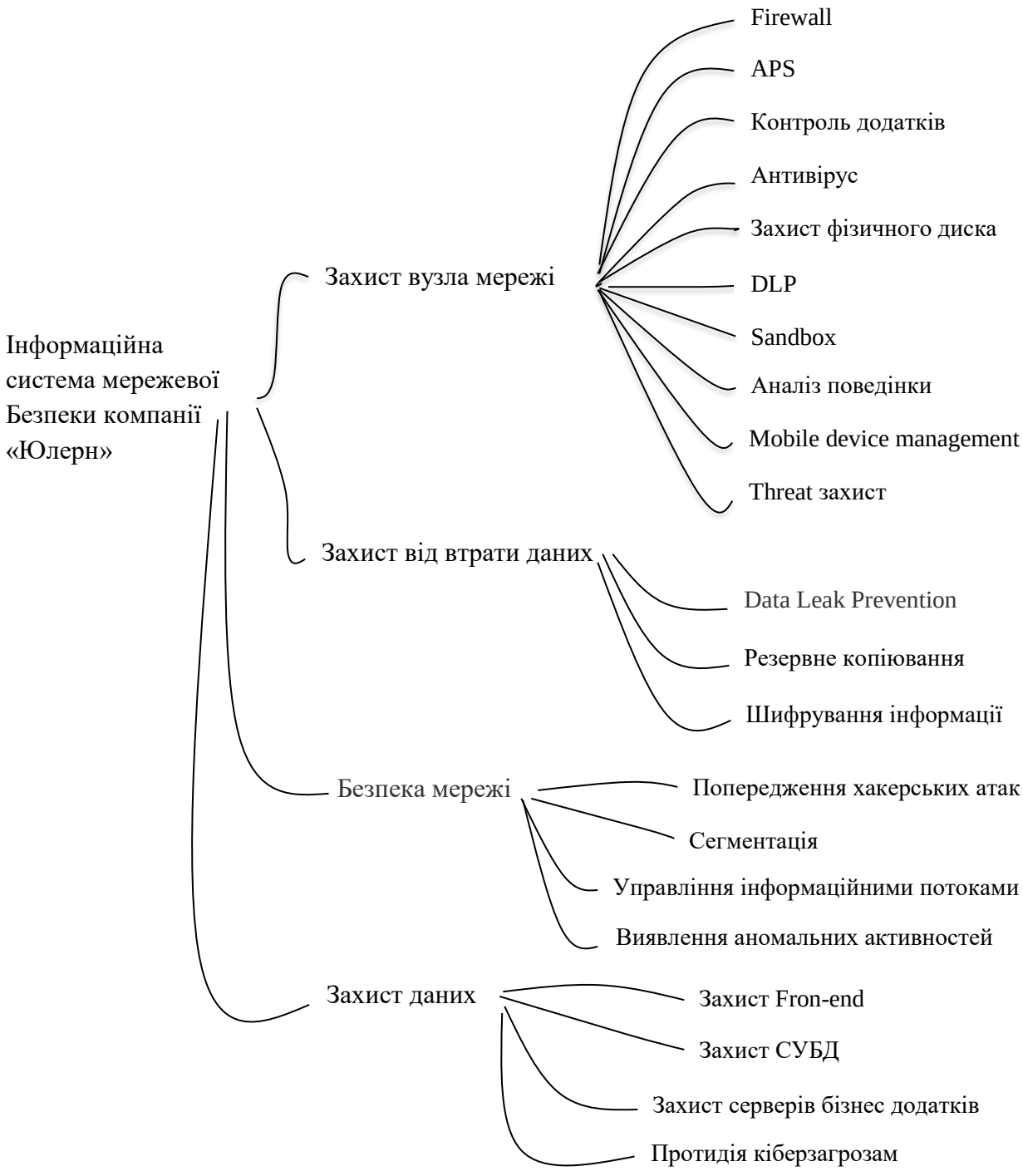


Рисунок 2.6 Схема інформаційної системи захисту мережі «Юлерн»

2.3. Декомпозиція опису інформаційної системи мережевої безпеки підприємства «Юлерн».

Методологія IDEF0 показує структуру системи, розбиваючи її на фрагменти. Для побудови діаграми, спочатку проводиться опис системи в цілому і її взаємодії з навколишнім світом, після чого проводиться функціональна декомпозиція, при якої їде розбивка на підсистеми, та кожна з підсистем наводиться окремо. На наступному кроці, кожна з описаних підсистем, розбивається на більш детальні і так далі до досягнення потрібного ступеня деталізації. [12] Дугами з'єднуються функціональні блоки системи, та дають представлення про взаємозв'язок між блоками. До функцій можуть бути віднесені як процеси, які проходять у системі, так і завдання, які необхідно виконати для отримання результату роботи моделюючого процесу.

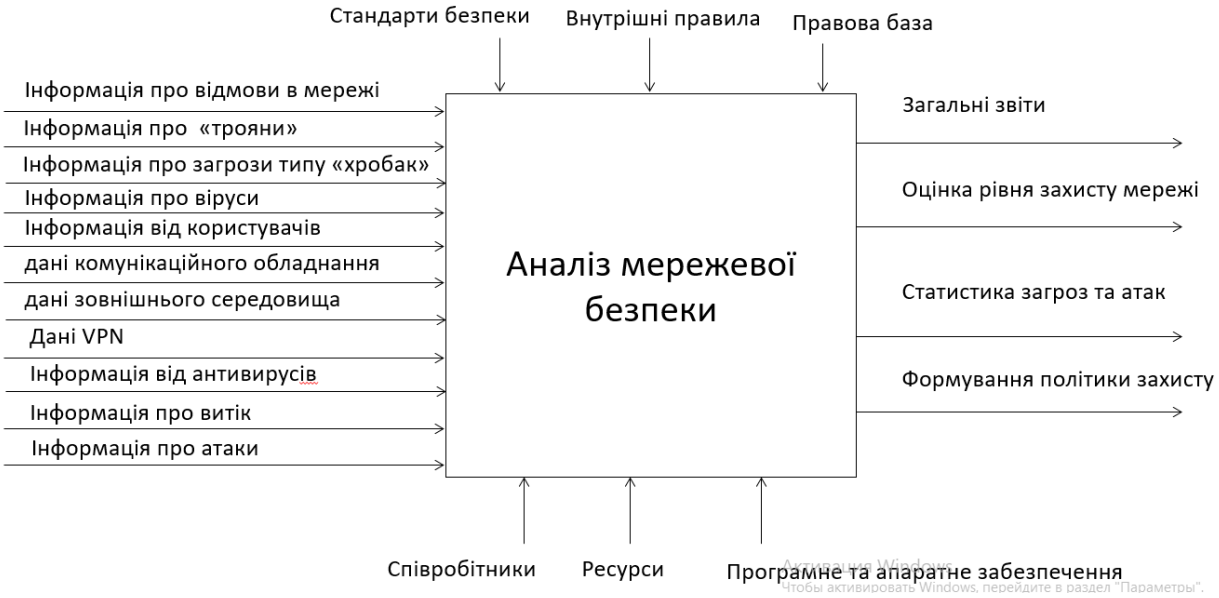


Рисунок 2.7 - Діаграма IDEF0 блоку аналізу мережевої безпеки компанії «Юлерн».

На рисунку 2.7, представлена діаграма IDEF0 блоку аналізу мережевої безпеки компанії «Юлерн», яка відображає перелік вхідних даних до системи аналізу, таких як відомості про події в мережі, інформацію з антивірусного програмного забезпечення, дані які були зрівнянні з сигнатурами окремо від антивірусного програмного забезпечення, інформацію про дії користувачів на рівні операційної системи, прав доступу та роботи з прикладних програмним забезпеченням, інформацію про витік, роботу з зовнішніми ресурсами та відомості

про атаки. До інформації, яка приходить від різних модулів системи, додається правова база, внутрішні правила налаштування безпеки та прав доступу і стандартне налаштування мережевих правил безпеки. На події у мережі компанії, велике значення має архітектура та фізичні вузли мережі, включаючи комунікаційне обладнання. Для формування подальшої політики захисту мережі, необхідно зберігати і аналізувати отриману інформацію, в процесі аналізу мережевого трафіку, для цього необхідно формувати загальні звіти, зберігати статистику загроз та атак, а також постійно оцінювати рівень захисту комп'ютерної мережі компанії «Юлерн».

Впродовж опису інформаційної системи мережевої безпеки компанії «Юлерн», на рисунку 2.8 представлена декомпозиція моделювання процесу аналізу мережевої безпеки.

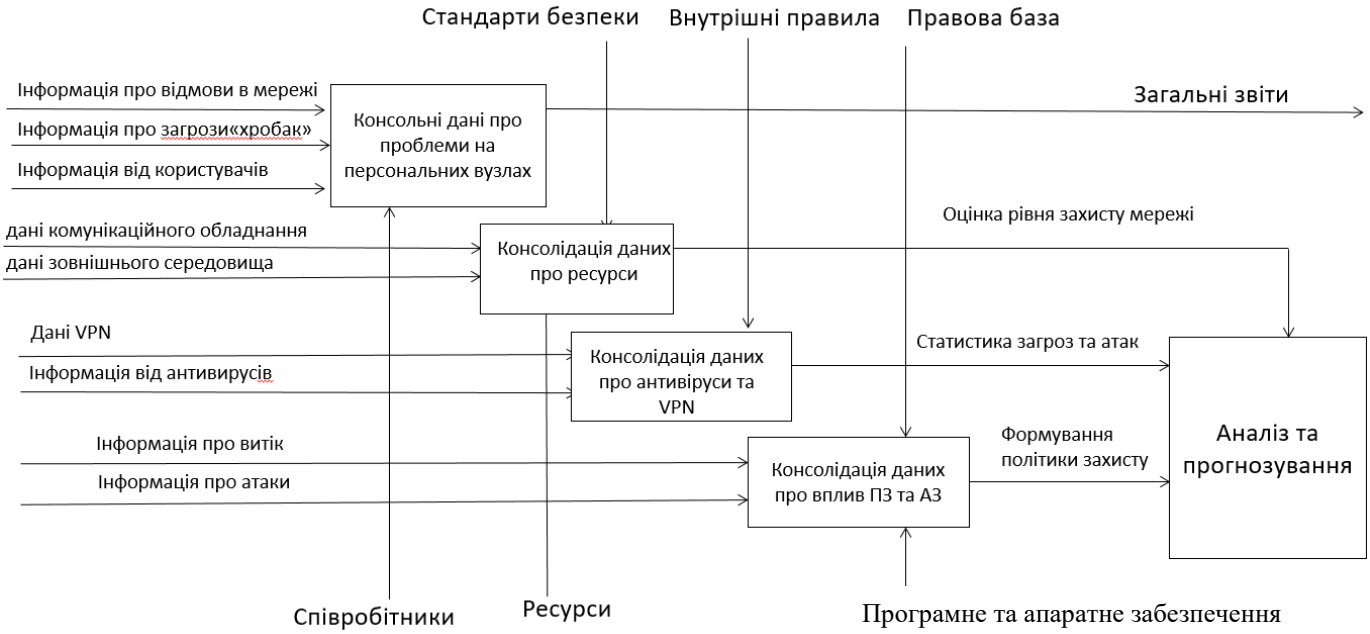


Рисунок 2.8 - Декомпозиція моделювання процесу аналізу мережевої безпеки «Юлерн».

Таким чином, враховуючи всі можливі джерела вхідних даних про можливі відхилення в роботі мережі або операційних систем, або комунікаційного обладнання або програмного забезпечення, можливо вчасно попередити вторгнення та врахувати недоліки поточного налаштування безпеки в мережі.

До ключових етапів аналізу мережевого трафіку, можна віднести:

- збір всієї можливої інформації про стан роботи мережі;
- збір всієї можливої інформації про стан роботи операційних систем;
- збір всієї можливої інформації про стан роботи програмного забезпечення;
- збір всієї можливої інформації про стан роботи комунікаційного обладнання;
- збір всієї можливої інформації про стан роботи з видаленими ресурсами, в тому числі GitHub;
- аналіз та формування звітів, логування, обробка та візуалізація статистики;
- процес прогнозування небезпечних станів, загроз, атак, вторгнень;
- переналаштування критичних вузлів комп'ютерної мережі, в тому числи комунікаційних і видалених.

До ключових вузлів мережі компанії «Юлерн», відносяться сервера, які підтримують збереження даних та налаштування мережі у п'яти філіалах, головний сервер, на якому зберігаються поточні інстанси сайтів замовників та комунікаційні вузли мережі, які підтримують зв'язок між всіма філіалами компанії. На рисунку 2.9 наведена декомпозиція побудови статистики та аналізу небезпечних станів в мережі.

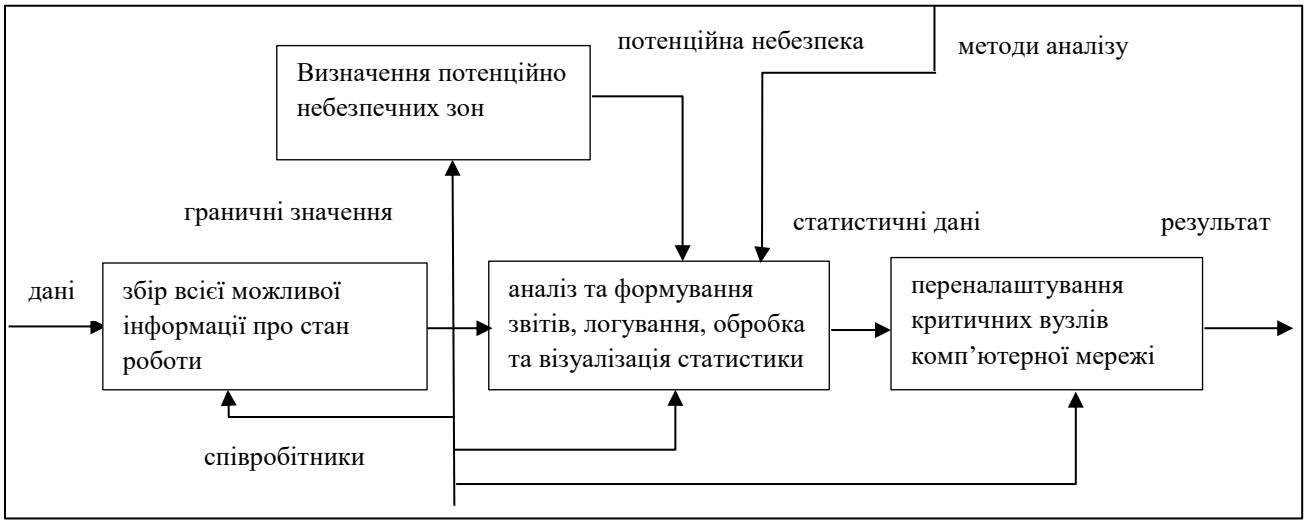


Рисунок 2.9 Декомпозиція побудови статистики і аналізу небезпечних станів.

3. РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ БЕЗПЕКИ КОМПАНІЇ ЮЛЕРН

3.1. Планування структури інформаційної системи розширеного моніторингу робочих станцій

Для планування інформаційної системи мережевої атаки, необхідно визначети основні блоки системи. На рисунку 3.1 предствлена загальна схема інформаційної системи мережевої безпеки «ЮЛерн». До першого блоку відносяться ті інформаційні ресурси компанії, від яких йде збір інформації, а саме це програмні сервера для налаштування прав доступу користувачів та систем і служби політики. Після збору даних, йде блок обробки статистичних даних, які можуть були отримані на попередньму кроці. Після аналізу даних, вони можуть бути направлені або в блок виявлення зловмисної активності, якщо це загроза або атака або в разі коли незрозуміло який тип небезпеки, то дані попадають до блокуц виявлення анамаотної активності. Враховуючи тип потенційно небезпечних програм, приймається рішення, або атоматично без людини, або з власником та приймається рішення в подальших кроках. Після цього система готова до видачі звітів та для прийняття подальших дій.

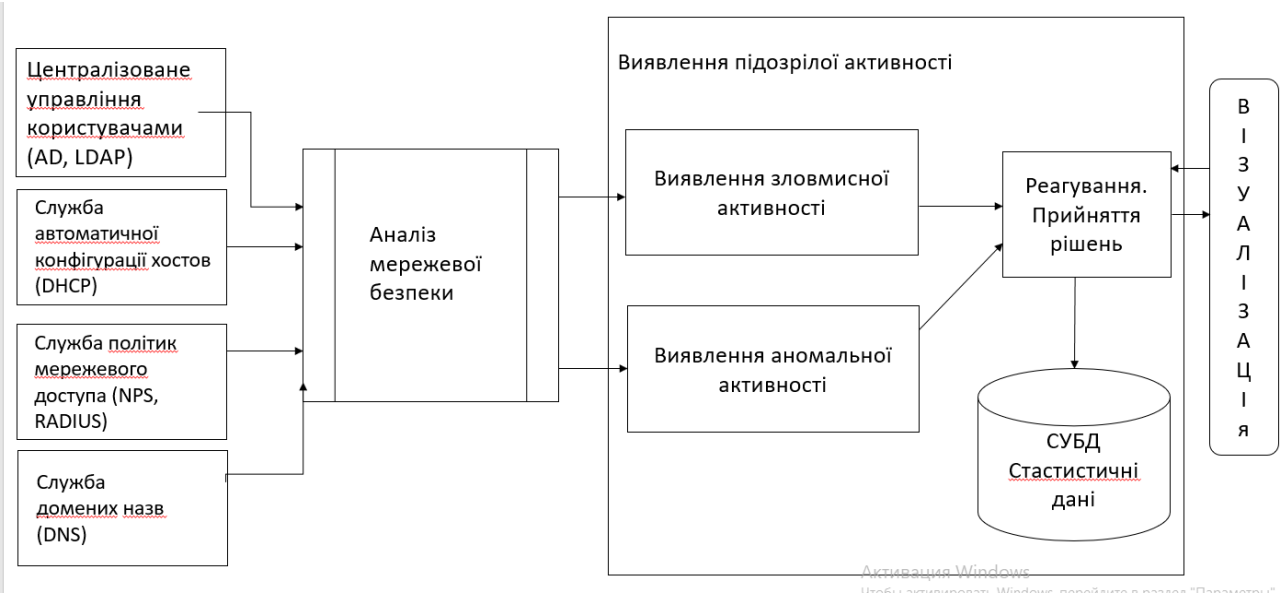


Рис. 3.1 Архітектура інформаційної системи мережевої безпеки «ЮЛерн»

На рисунку 3.2. представлена загальна схема функціонування модуля перевірки прав доступу до мережевих ресурсів.

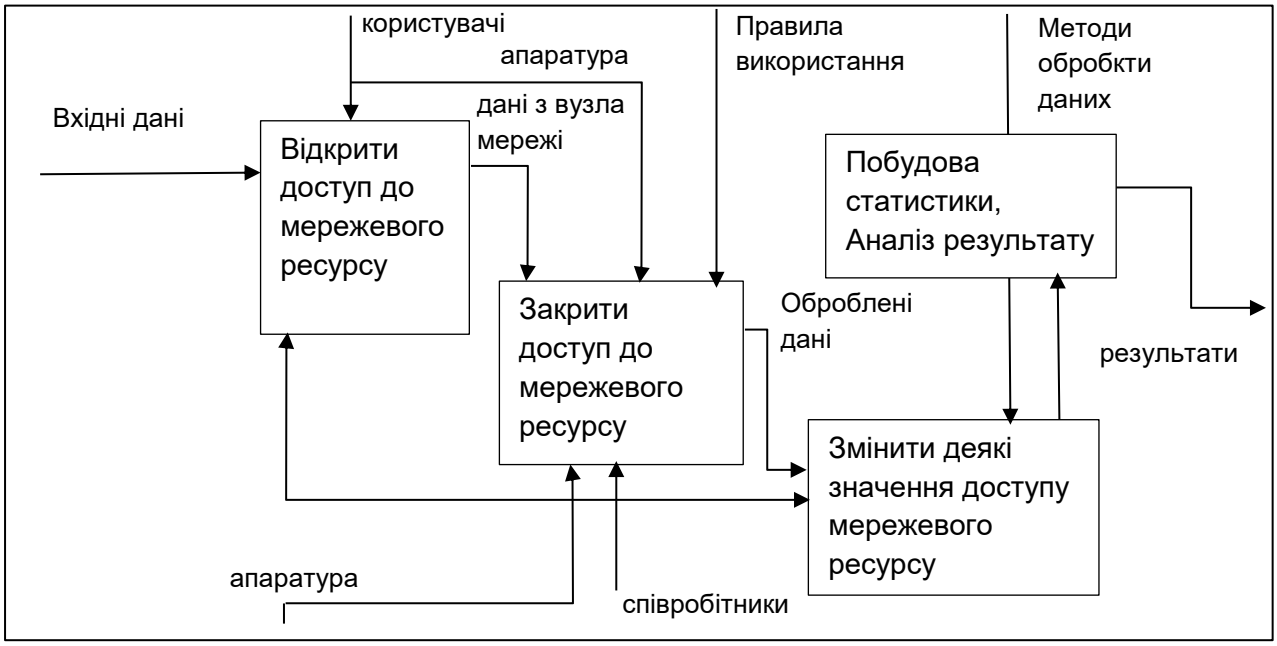


Рисунок 3.2. - Загальна схема функціонування модуля перевірки прав доступу до мережевих ресурсів.

При вдосконаленні системи захисту мережі, головним елементом виступає налаштування прав доступу користувачів до вузлів мережі, зовнішніх ресурсів якими в компанії «Юлерн» виступає ресурс Github. Також велику роль відіграє налаштування операційних систем, програмного забезпечення, комунікаційного обладнення у тому числі і мережевих екранів, таблиць маршрутизації. Для цього необхідно виконувати постійний мониторинг налаштування прав доступа та можливих вразливостей у системі захисту ресурсів. Загальна схема функціонування модуля перевірки прав доступу до мережевих ресурсів відображає процес моніторинга доступа до мережевого ресурсу та в результаті роботи, показує кількість і властивості ресурсів з відкритим доступом або з вразливостями у налаштуванні доступу. Використану інформацію про відкритий мережевий ресурс необхідно використовувати як для збереження статистики так і для усунення вразливого місця. Для цього необхідно підключитись до ресурса за допомогою відповідної до типа вузла функції, з аргументами назви вузла мережі, порта підключення та перевірки необхідного аргумента права доступу. :

Способ передачі данних між модулем і вузлом мережі можи бути як через стек, так і за допомогою бібліотек, або власного налаштування. Це залежить від типа вузла, а саме:

— серверне обладнення
— комп’ютер або ноутбук
— сервер баз даних
— сервер зберіганння даних (Storage)
— коммунікаційне обладнення (комутатор, маршрутизатор)
— мережевий екран.

Аргументом мережевого імені, виступає як імя DNS, так і IP-адреса вузла або його Mac-адрес. Після отримання доступу до ресурсу, модуль отримує інформацію до діректорій операційної сиситеми або файлів комунікаційного обладнення. Перевіряючи вразливі місця системи, модуль має змогу змінити доступ до директорії, або файлів. Для визначення структури до якої будуть застосовуватись зміни, використовується покажчик до ресурсу. На рисунку 3.3. показана схема елементів модуля:

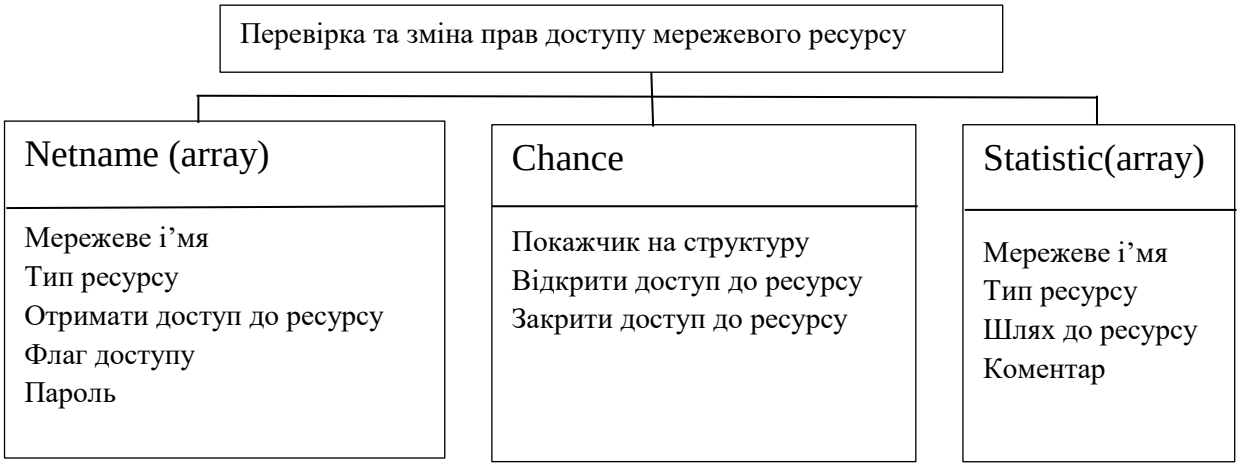


Рисунок 3.3 - Схема елементів модуля перевірки та зміни прав доступу до мережевого вузла компанії «Юлерн»:

3.2 Реалізація інформаційної системи мережевої безпеки компанії “Юлерн”-

Для створення системи розширеного моніторингу робочих станцій використовується ряд модулів, реалізуючих систему мережевої безпеки компанії «Юлерн», такі як модуль відповідаючий за перевірку потоків, модуль для форми системи і модуль для збереження інформації про назву робочих станцій, їх IP і MAC-адреси. Візуалізація в системі потрібна для взаємодії користувача з системою. На рисунку 3.4. представлена загальна схема структури функцій інформаційної системи забезпечення мережевої безпеки.

Рисунок 3.4. Загальна схема функції інформаційної системи забезпечення мережевої безпеки.

Головний модуль включає в себе всі інші модулі. Так само він містить в собі форму системи розширеного моніторингу. У цьому модулі описуються різні типи даних, що використовуються в процесі отримання необхідної інформації. В кожному модулі є опис процедур і функцій на події в мережі і її компонентів, а також додаткові характеристики і функції для перетворень або отримання даних, якщо формат не співпадає.

Модуль бази даних використовуються для безпосередньої взаємодії бази з системою розширеного моніторингу. У цьому модулі описані технологія доступу до даних бази через компоненти інформаційної системи, а також компоненти доступу до даних, компоненти відображення і редагування даних в таблиці.

В інформаційної системи забезпечення мережевої безпеки, використовується процес розширеного моніторингу з подальшим занесенням отриманої статистики до бази даних, що складається з наступних таблиць:

— інформація про відмови в мережі;

— інформація про «трояни»;

— інформація про загрози типу «хробак»;

— інформація про віруси;

— інформація від користувачів;

— дані комунікаційного обладнання;

— дані зовнішнього середовища;

— дані VPN;

— інформація від антивирусів;

— інформація про витік;

— інформація про атаки.

. Таблиці які місцять інформацію з інших пристроїв, мають наступні поля:

- поле key - ідентифікатор, це ключове поле. Розмір поля - «Довге ціле». Індексовані поле - «Так (Збіги не допускаються)».

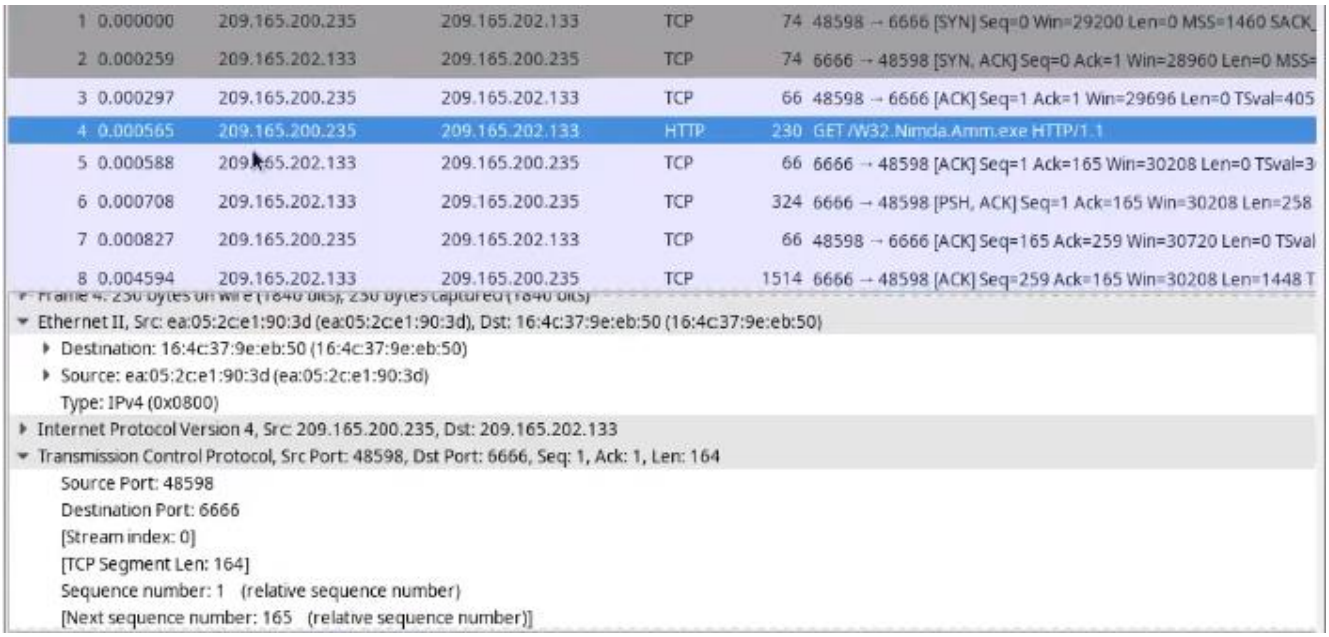
- поле host, яке відповідає за тип вузла в мережі, тобто комунікаційне обладнення, сервер або робоча станція. Тип - текстовий. Розмір поля - 255. Індексовані поле - «Так (Допускаються збіги)».

- поле ip, поле яке відповідає за адресу вузла в мережі. Тип - текстовий. Розмір поля - 16. Індексовані поле - «Так (Збіги допускаються)».

- поле mac, поле яке відповідає за Mac-адресу вузла в мережі Тип - текстовий. Розмір поля - 18. Індексовані поле - «Так (Збіги допускаються)».

З'єднання між інформаційною системо та сервером бази даних відбувається за допомогою мережевого доступу. Доступ до створеної бази даних здійснюватися за допомогою бібліотеки db.models. Для відображення даних з використується компонент DataSource. У цьому ж компоненті можна буде додавати, видаляти і редагувати рядки таблиці, якщо буде необхідно.

У базу даних надходить інформація про вузли мережі, такі як робочі станції працівників, сервера та комунікаційне обладнення, у яких визначені IP і MAC - адреси. Так як перевірка їх зміни, залежить від їх наявності, якщо при перевірці, в таблиці не виявилося такого комп'ютера, то цей хост додоється до неї. При виявленні невідповідності імені робочої станції з одним з його адрес, система автоматично виведе повідомлення, в якому буде вказано, який саме комп'ютер поміняв адресу.



.Рисунок 3.5 Приклад роботи модуля інформаційної сисктми безпеки.

Модулів відповідає за отримання списку всіх робочих станцій, які функціонують в локальній мережі. У модулі переглядається потік даних у мережі, за допомогою процесу знаходження всіх робочих станцій, що вимагає значного проміжку часу, за який може знадобитись в критичній ситуації безпеки, надати від системи інші дані. Додатковими підпрограмами в цьому потоці є процедури виведення отриманої інформації на засоби сповіщення.

Модуль розширеного моніторингу в системі, відповідає за отримання інформації про віддаленні комп'ютери в мережі. Як і перший модуль, він відповідає за потік даних, враховуючи велику затрату часу. IP-адреса віддаленої робочої станції допомагає визначити наявність потоку несанкціонованої інформації та визначає ім'я комп'ютера, імена користувачів зареєстрованих на даному хості, ім'я робочої групи, сервер домену, коментар про віддалений комп'ютер або мережевий хост, назву мережевої групи, до яких належить користувач та хост. На рисунку 3.6 представлено приклад інформації про мережевий вузел.

```
In [2]: sw3.execute('show vlan brief')
+++ SW3: executing command 'show vlan brief' +++
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Gi1/0
101  LAN1                             active
102  LAN2                             active
103  EDGE                             active    Gi0/3

In [3]: new_vlan_cfg = ['vlan 110', 'name new_vlan']
In [4]: sw3.configure(new_vlan_cfg)
+++ SW3: config +++
config term
SW3(config)#vlan 110
SW3(config-vlan)#name new_vlan
SW3(config-vlan)#end

In [5]: sw3.execute('show vlan brief')
+++ SW3: executing command 'show vlan brief' +++
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Gi1/0
101  LAN1                             active
102  LAN2                             active
103  EDGE                             active    Gi0/3
110  new_vlan                         active
```

Рисунок 3.6 – Інформація про вузол мережі.

Також інформаційна система безпеки, зберігає інформацію про MAC-адреса віддаленої робочої станції і доступні мережеві ресурси. Так само як і в першому модулі, в мережевому потоці перевіряється отримана інформація віпро наявні в мережі адреси та доступність до них та ведення отриманої інформації на форму, де вказується отримані при мониторингу вихідні дані. Для роботи модуля використовуються бібліотеки для перерахування залогінених користувачів, для визначення належності користувача до груп, для визначення доступних мережевих ресурсів.

Модуль перевірки мережевого потоку даних відповідає за перевірку співвідношень імені комп'ютера з його IP і MAC - адресами. У разі невідповідності одного з параметра система сповіщає про це адміністратора. Модуль працює в потоковому режимі, тому що перевірка на доступність вузлів мережі необхідна для попередження простою роботи компанії і вимагає для виконання перевірки великого проміжку часу, модуль буде повторювати перевірку через заданий інтервал часу. Під час перевірки буде або нічого не відбуватися, або видане повідомлення про виникнення підміни одного з адрес робочої станції, або додавання нового хоста в базу даних, при його відсутності в ній.

Використання бази даних полягає в тому, що отримані адреси хостів, при чергової перевірки локальної мережі, потрібно порівнювати з уже наявними адресами цих же хостів. Таку інформацію легше і доцільніше зберігати в таблиці. Так само з таблиці можна буде легко і швидко дістати адреси, цікавиться нами, хоста. У таблиці легше організувати пошуки і сортування. База даних в системі розширеного моніторингу робочих станцій буде містити таблицю, в якій буде знаходитися інформація про імена робочих станцій, їх IP і MAC - адреси.

Dідображається інформація по запиту адміністратора або при винекненні небезпечної ситуації. Перша сторінка потрібна для відображення інформації про мережеві ресурси надані локальним комп'ютером, з можливісттю переглядати їх; додавати нові ресурси з вибором прав доступу:

— на читання,

— на запис,

— на виконання,

— на повний доступ

— на комбінований доступ; з

— закривати вже відкриті ресурси.

В модулі є можливість отримати список поточних сесій, а також завершувати сесію, обрану за бажанням. Також є відображення списку відкритих файлів, так само з можливістю закриття відкритого файлу. На рисунку 3.7 показана функція перевірки доступності заданого вузла мережі.

```
[GCC 5.4.0 20160609] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pexpect
>>> child = pexpect.spawn('telnet 172.16.1.20')
>>> child.expect('Username')
0
>>> child.sendline('cisco')
6
>>> child.expect('Password')
0
>>> child.sendline('cisco')
6
>>> child.expect('iosv-1#')
0
>>> child.sendline('show version | i V')
19
>>> child.expect('iosv-1#')
0
>>> child.before
b'show version | i VrnCisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M), Version
>>> child.sendline('exit')
5
>>> exit()
```

Рисунок 3.7 Функція перевірки доступності заданого вузла мережі.

Сторінка відображає вихідні дані, пов'язані зі списком мережевих імен, список робочих груп кожного з співробітників, а також отримання повного списку робочих станцій локальної мережі із зазначенням підмережі і робочої групи. Проводитися контроль процесу виконання цих пошуків для того, щоб адміністратор міг візуально визначити його закінчення. Так само на цій сторінці мрожливо отримати інформацію про комп'ютер на основі його IP - адреси.

В інформацію про вузол входие:

— IP – адреса;

— ім'я робочої станції;

— імена залогінених користувачів на даному комп'ютері;

— локальна мережа, в якій обслуговується дане з'єднання;

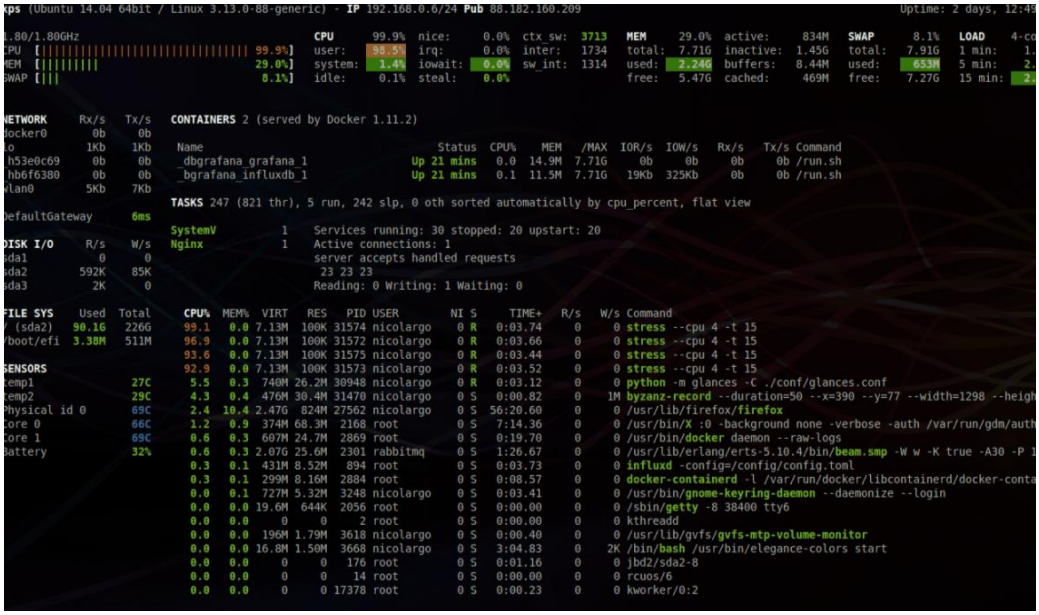
— коментарі до даної робочої станції, якщо такі будуть матися;

— ім'я робочої групи;

— MAC – адреса;

— мережеві ресурси надані цим комп'ютером з коментарями до них.

Також відображаєся таблиця з інформацією про імена робочих станцій, їх IP і MAC - адресами. На рисунку 3.8 наведено приклад дій вкладці, на якій є можливість створити або перебудувати таблицю з новою інформацією про хостах, можливість очищення таблиці. Також виводитися статус процесу виконання заповнення таблиці.



У головному модулі використовуються наступні функції:

— function GetMAC (MacAddress; Name), допоміжна функція, яка перетворює MAC - адреса до виду «00-00-00-00-00-00», використовується для перетворення адреси за допомогою отримання функції такого виду адреси «00-00-00-00-00-00» і для виведення MAC адреси інтерфейсу при визначення вхідного і вихідного трафіку.

— function IsNT (Value) Boolean, функція потрібна для визначення операційної системи на якій встановлена система віддаленого розширеного моніторингу робочих станцій.

— function SelectDirectory, використовується для виведення діалогу вибору папки. Вона потрібна при відкриті локального ресурсу в загальний доступ.

— function cardinaleoeimeStr, допоміжна функція, завдання якої буде перетворювати кількість секунд в більш звичну форму відображення «дні: годинник: хвилини: секунди».

— function netcontainerdist, функція повертає список мережевих імен з підрівня ListRoot. Кожен елемент списку TList - це PNetRec, де поле RemoteName визначає відповідно мережеве ім'я елемента списку.

— function netIPFromtame (DNS), функція потрібна для отримання IP - адреси по імені робочої станції, використовується для відображення інформації про повний список хостів в локальній комп'ютерній мережі. А також для заповнення поля ip в таблиці бази даних.

— function netьacaromIP, необхідна лдя отримання MAC - адреси по IP - адресу комп'ютера та потрібна для перетворення інформації та пошуку вузлів вне залежності від типа адреси, а також для заповнення поля mac в таблиці бази даних.

— function Database, функція потрібна для роботи з базою даних.

ВИСНОВКИ

Всі задачі, поставлені під час виконання бакалаврської роботи, було виконано в повному обсязі.

1. Проведено аналіз існуючих рішень, де було розглянуто такі системи як ЛАНІТ, Detwig, M3 і NetPing. Розглянуто всі можливості сучасних систем та їх недоліки. Описано наскільки автоматизація моніторингової системи буде вигідна для банків.

2. Розроблено систему підтримки прийняття рішення із використанням Бази даних та Системи управління базою даних. Кожен етап розробки системи супроводжувався схемами систем, наведеними частинами коду та результатів системи.

3. Проведено порівняльний аналіз розроблених систем із визначенням ефективності кожної із систем. Було визначено, що автоматизована система на базі даних є більш ефективною ніж сучастні не автоматизовані системи.

4. Перспективою розвитку системи буде скорочення часу простою банкоматів, що допоможе банкам нести набагато менше збитків та знизить поріг знань для працівників моніторингу.