МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Модель програмно-апаратного комплексу кіберзахисту підприємства»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Лаврик Т.В.**

Студента групи КБ – 61 — **Устика Д.С.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____2020 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-61 спеціальності "Кібербезпека" денної форми навчання Устика Дмитра Сергійовича.

Тема: "**Модель програмно-апаратного комплексу кіберзахисту підприємства**"

Затверджена наказом по СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки: 1) аналіз систем інформаційної безпеки підприємства; 2) характеристика моделі комплексу кіберзахисту підприємства; 3) розробка моделі програмно-апаратного комплексу кіберзахисту інформаційних ресурсів підприємства.

Дата видачі завдання "_____"_____2020 р.

Керівник випускної роботи _____ Лаврик Т.В.

Завдання прийняв до виконання _____ Устик Д.С.

РЕФЕРАТ

Записка: 63 стор., 14 рис., 5 табл., 57 джерел.

Об'єкт дослідження — системи захисту інформаційних ресурсів.

Мета роботи — проектування моделі програмно-апаратного комплексу на основі аналізу можливостей існуючих систем і засобів захисту, які задовільнять безпечну роботу та експлуатацію систем невеликого підприємства (до 30 робочих станцій).

Методи дослідження — метод аналітичного огляду, метод функціонально-статистичних випробувань.

Результати — проаналізовано відомі загрози інформаційним ресурсам підприємства, існуючі моделі захисту і описано системи захисту на прикладному, апаратному та мережевому рівнях, їх основні принципи роботи та здійснено порівняльну характеристику існуючих продуктів захисту; розроблено модель програмно-апаратного комплексу кіберзахисту підприємства на основі аналізу можливостей існуючих систем і засобів захисту. Сформовано інструкцію з базового налаштування програмно-апаратного комплексу кіберзахисту.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, КОМПЛЕКС КІБЕРЗАХИСТУ, АПАРАТНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ПРОГРАМНИЙ ЗАХИСТ ІНФОРМАЦІЇ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, СИСТЕМА РОЗМЕЖУВАННЯ ДОСТУПУ, МОНІТОРИНГ, АНТИВІРУС.

ЗМІСТ

ВСТУП

Кібербезпека зосереджена на захисті комп'ютерних систем від несанкціонованого доступу або їх пошкодження чи іншому недоступі ресурсів системи в результаті впливу шкідливих чинників. Відповідно до Закону України про основні засади забезпечення кібербезпеки України (2163-VIII) кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Інформаційна безпека - це більш широка категорія, яка спрямована на захист усіх інформаційних активів, як в паперовій, так і в цифровій формі. В останні роки кібербезпека потрапила під ретельний контроль ЗМІ. Це можна пояснити як швидким зростанням атак, так і значним впливом на організації. Витрати на порушення кібербезпеки зростають. Нові закони про конфіденційність можуть означати значні штрафи для організацій. Також слід врахувати нефінансові витрати, як, наприклад, шкода репутації.

Кіберзлочини стають все складнішими. Кібератаки продовжують зростати у вишуканості, зловмисники використовують постійно зростаючу різноманітність тактик. Сюди входить соціальна інженерія, зловмисне програмне забезпечення та програми-вимагачі, наприклад Petya, WannaCry та NotPetya).

Згідно з джерелом [1] більшість компаній зосереджуються на вдосконаленні системи кіберзахисту лише після того, як стикнулися з втратами через недоліки в даних системах. Найбільшим джерелом загроз вбачаються недбайливі робітники - 34%, застарілі системи контролю - 26%, можливість несанкціонованого доступу - 13% та використання хмарних сервісів - 10%. Як показали результати опитування, більшість компаній (87%) не мають достатніх ресурсів для підтримання достатнього рівня захисту і

стабільності систем від кіберінцидентів. 54% респондентів, які представляли організації малого бізнесу відмітили, що в недостатній мірі виділяли ресурси для фінансування кібербезпеки своїх інформаційних систем.

1. АНАЛІЗ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Загальна характеристика побудови системи інформаційної безпеки підприємства

Згідно з ресурсом [2], за даними експертів – чим менше бізнес та чим менше уваги в ньому приділяється кібербезпеці внутрішньої інфраструктури – тим більше шанс, що даний об’єкт буде атакований та використаний в подальших атаках на більш крупні цілі.

Основною метою систем захисту підприємтсва є попередження збитків, нанесених діяльності підприємства за рахунок несанкціонованого доступу до інформації, попередження викрадення цінної інформації а також порушення роботи виробничих процесів підприємства. Принципами побудови системи захисту є постійне вдосконалення існуючої системи, а також комплексне використання існуючих засобів захисту критично важливих процесів.

При побудові системи варто враховувати такі рекомендації:

- Забезпечення безпеки не є одноразовим актом. Це постійний процес реалізації методів, способів і шляхів створення, вдосконалення і розвитку системи безпеки, неперервного контролю і виявлення потенційних загроз підприємству;
- Безпека може бути забезпечена лише при комплексному використанні засобів захисту всередині структурних елементів виробничої системи;
- Ніяка система безпеки не може забезпечити бажаний рівень захисту без відповідної підготовки робочого персоналу і користувачів виробничої системи та дотримання ними правил, направлених на забезпечення захисту;
- Функціонування комплексу повинне здійснюватися на основі наступних принципів:

- Забезпечення безпеки інформаційних ресурсів підприємства протягом всіх технологічних етапів їх використання і обробки;
- Своєчасна постановка задач по безпеці на ранніх етапах розробки системи безпеки;
- Безперервне функціонування комплексу захисту;
- Засоби захисту повинні бути обгрунтованими з точки зору заданого рівня безпеки та відповідати встановленим вимогам;
- Вдосконалення засобів захисту на основі власного досвіду, появи нових засобів захисту з урахуванням змін в методах і засобах розвідки та промислового шпіонажу, нормативно-технічних вимог;

Основним з етапів створення систем захисту є визначення ті постановка цілей, визначення задач та вимог до системи безпеки. Важливим моментом є визначення критичних інформаційних ресурсів підприємства та вимог до забезпечення захисту даних об’єктів. Загалом, об’єктами захисту від загроз на будь-якому підприємстві є інформація з обмеженим доступом, засоби і автоматизовані системи обробки інформації, технічні та програмно-апаратні системи захисту матеріальних та інформаційних ресурсів підприємства.

1.2 Опис підприємства і аналіз джерел загроз та вразливостей

Основними бізнес-процесами підприємства малого бізнесу є ведення облікової документації за допомогою спеціалізованих застосунків та загальний документообіг інформації з обмеженим доступом (ІзОД) та для службового користування (ДСК). Частина документації може отримуватися за допомогою мережі Інтернет, а також засобами електронного листування. Адміністрування, як правило, проводиться з єдиної точки системним адміністратором.

Розглянемо типові загрози, характерні для систем підприємств малого бізнесу. Під загрозою розуміються одиничні або комплексні, реальні або потенціальні, активні або пасивні прояви несприятливих можливостей

зовнішніх або внутрішніх джерел загроз створювати критичні ситуації, події та шкідливо впливати на об’єкти захисту. До інформаційних ресурсів з обмеженим доступом перелік загроз ширший, оскільки вони є об’єктом підвищеної уваги зі сторони зловмисників.

В результаті витоку інформація може стати власністю суб’єкта, який не має права на доступ до неї. Під зловмисником розуміється особа, яка діє в інтересах конкурента, противника або у власних інтересах. Метою та результатом оволодіння зловмисником даного роду інформації може бути не тільки доступ, але й модифікація або її знищення.

Загроза доступності, цілісності та конфіденційності практично реалізується через ризик виникнення каналу несанкціонованого отримання кимось цінних документів. Функціонування даного каналу завжди веде до втрати даних. Розглянемо властивості даних та загрози детальніше.

Властивості даних

Існують три основні властивості даних:

1. Конфіденційність:

Конфіденційність перешкоджає передачі інформації неавторизованим особам, ресурсам і процесам. Синонім конфіденційності - особисті дані. Організації обмежують доступ до даних або інші ресурси мережі, щоб гарантувати їх використання тільки авторизованими операторами. Наприклад, програміст не повинен мати доступ до персональних даних усіх співробітників.

Організації повинні ознайомити співробітників з кращими практиками для захисту конфіденційної інформації, щоб вони могли убезпечити себе і свою організацію від атак. Для забезпечення конфіденційності використовуються такі методи, як шифрування даних, аутентифікація і розмежування доступу.

Є такі типи інформації з обмеженим доступом [3]:

- Конфіденційна інформація, яка в свою чергу розділяється на такі види [5]:

– Конфіденційна інформація, що є власністю держави;

– Конфіденційна інформація, що не є власністю держави.

Такий тип означає будь-яку інформацію, включаючи, без обмеження, будь-яке дослідження, дані, розрахунки, носії програмного забезпечення для зберігання чи інший збір інформації, патент, заявку на патент, авторські права, торговельну марку, торгове найменування, марку послуги, назву послуги, "ноу-хау", торгові секрети, списки клієнтів, деталі контрактів з клієнтами або консультантами, цінова політика, операційні методи, маркетингові плани або стратегії, методи або плани розвитку продукту, плани придбання бізнесу або будь-яка частина або фаза будь-якої наукової або технічної інформації, ідей, відкриттів, дизайнів, комп'ютерні програми (включаючи джерела об'єктних кодів), процеси, процедури, формули, удосконалення або інша майнова або інтелектуальна власність компаній, будь-яка в письмовій чи матеріальній формі, чи зареєстрована чи не зареєстрована, включаючи всі файли, записи, посібники , книги, каталоги, меморандуми, замітки, резюме, плани, звіти, записи, документи.

- Службова інформація [4]

– Така, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– Зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

- Таємна інформація:

– Державна таємниця;

– Комерційна таємниця;
– Службова таємниця;
– Банківська таємниця;
– Інші види таємниць.

2. Цілісність.

Цілісність - це точність, узгодженість і достовірність даних протягом усього терміну експлуатації. Синонімом цілісності даних є їх якість. Дані піддаються таким операціям, як отримання, зберігання, вилучення, оновлення та передача. Під час всіх цих операцій дані повинні залишатися захищеними від несанкціонованого доступу.

Для забезпечення цілісності даних використовуються такі методи [6], як хешування, перевірка достовірності та узгодженості даних і засоби розмежування доступу. У системах для забезпечення цілісності даних можуть застосовуватися один або кілька методів, перерахованих вище, та інші існуючі методи.

3. Доступність.

Доступність має на увазі постійну підтримку доступності до різних систем і сервісів. Кібератаки і збої системи можуть перешкоджати доступу до інформаційних систем і сервісів. Наприклад, перериваючи доступність веб-сайту конкурента шляхом зупинки його роботи, інша компанія може забезпечити собі перевагу. Такі DoS-атаки ставлять під загрозу доступність системи, запобігають доступу і використанню інформаційної системи легітимними користувачами.

Для забезпечення доступності застосовуються такі методи, як резервування системи, резервне копіювання і підвищення відмовостійкості систем, технічне обслуговування обладнання, актуальні операційні системи і програмне забезпечення, а також готові плани швидкого відновлення в разі непередбачених збоїв.

Види атак

На сьогоднішній день існує багато видів кібератак. Оскільки бакалаврська робота передбачає побудову моделі системи кіберзахисту для комерційного підприємства, то розглянемо приклади поширених атак на дані (дані ДСК, комерційні таємниці, облікові записи тощо) [7].

Зловмисне програмне забезпечення (ПЗ) - це код, який створюється для потайного впливу на комп'ютерну систему без відома користувача. Зловмисне програмне забезпечення відрізняється тим, що воно може поширюватися мережею, спричиняти зміни та пошкодження, залишатися невиявленим та залишатись в зараженій системі. Це може зруйнувати мережу і знизити її продуктивність.

Вірус “Троянські коні” - це шкідливе програмне забезпечення, яке хибно представляє себе корисним (тобто потрапляє до мережі під виглядом легітимного ПО). Вони поширюються, виглядаючи як звичайне програмне забезпечення та переконують жертву їх інсталювати (їх розробники користуються такими методами, як соціальна інженерія). Трояни вважаються одними з найнебезпечніших типів усіх зловмисних програм, оскільки вони часто призначені для крадіжки фінансової інформації.

SQL-ін’єкція, відома як SQLI, є різновидом атаки, яка використовує зловмисний код для маніпулювання базами даних, що надаються для отримання доступу до інформації, яка не призначена для відображення. Це може включати численні елементи, включаючи приватні дані про клієнтів, списки користувачів або конфіденційні дані компанії. SQLI може мати руйнівні наслідки для бізнесу. Успішна атака SQLI може призвести до видалення цілих таблиць, несанкціонованого перегляду списків користувачів, а в деяких випадках зловмисник може отримати адміністративний доступ до бази даних. Вони можуть бути дуже згубними для бізнесу. Розраховуючи ймовірну вартість SQLI, слід враховувати втрату довіри клієнтів у разі викрадення особистих даних, таких як адреси, дані кредитної картки та номери

телефонів. Хоча SQLI може використовуватися для атаки на будь-яку базу даних SQL, злочинці часто націлюються на веб-сайти.

Існує багато інших видів атак, окрім наведених вище.

Типи злочинців

Кіберзлочинність – це великий бізнес. У 2018 році економіка кіберзлочинності була оцінена на суму 1,5 трильйона доларів, згідно з дослідженням, замовленим Bromium. Зловмисники можуть також керуватися політичними, етичними чи соціальними стимулами.

Існують такі типи кібезлочинців [8]:

– Непрофесіонали

Непрофесіонали або «скрипт-кідді» мають обмаль навичок або ж не мають їх взагалі і для атак використовують існуючі інструменти бо інструкції, знайдені в мережі Інтернет. Деякі з них роблять це з цікавості, інші намагаються продемонструвати свої навички та нанести шкоду. Не зважаючи на те, що вони використовують базові інструменти, результат все одно може бути спустошливим.

– Хакери

Ця група злочинців проникає в комп'ютери або мережеві інфраструктури з різних причин. Згідно причин злому хакери класифікуються як «білі», «сірі» або «чорні». «Білі» хакери проникають в мережеву інфраструктуру або комп'ютерні системи з метою виявлення вразливостей і підвищення безпеки цих систем. Злом здійснюється з дозволу власників системи, а потім власники системи отримують результати тесту. «Чорні» хакери використовують уразливості для незаконного отримання особистої, фінансової або політичної вигоди. «Сірі» хакери знаходяться десь посередині між «білими» і «чорними» хакерами. «Сірі» хакери можуть знаходити уразливості і повідомляти про них власникам системи, якщо подібна дія узгоджується з їх планами. Деякі «сірі» хакери публікують інформацію про уразливість в Інтернеті, щоб інші зловмисники могли використовувати її.

– Організовані хакери

Включають організації кіберзлочинців, хактивістів, терористів і хакерів, спонсорованих державою. Кіберзлочинці, як правило, представляють собою групи професійних злочинців, націлених на владу і багатство. Злочинці добре організовані і можуть навіть пропонувати вчинення кіберзлочинів як послуги. Хактивісти роблять політичні заяви з питань, які важливі для них, щоб привернути до них увагу. Хактивісти роблять публічно доступною компрометуючу інформацію про своїх жертв. Спонсоровані державою хакери збирають розвідувальні дані або здійснюють акти саботажу від імені свого уряду. Такі кіберзлочинці, як правило, добре навчені і добре фінансуються. Їх атаки спрямовані на конкретні цілі, які вигідні для їх уряду. Деякі хакери, спонсоровані державою, навіть служать в збройних силах своєї країни.

1.3 Постановка задачі

З розвитком технологій та впровадженням різних технічних рішень внутрішні мережі підприємств являють собою деяку структуру програмних, програмно-апаратних та апаратних рішень задля їх функціонування.

Основними інформаційними ресурсами, які потребують захисту на визначеному підприємстві є:

– внутрішні технологічні мережі;

– бази даних;

– конфіденційна інформація (контракти, ДСК тощо).

Метою даної бакалаврської роботи є проектування моделі програмно-апаратного комплексу на основі аналізу можливостей існуючих систем і засобів захисту, які задовільнять безпечну роботу та експлуатацію систем невеликого підприємства (до 30 робочих станцій).

2. ХАРАКТЕРИСТИКА МОДЕЛІ КОМПЛЕКСУ КІБЕРЗАХИСТУ ПІДПРИЄМСТВА

2.1 Опис моделі

У даній бакалаврській роботі буде розроблятися модель системи для компанії типу малого та середнього бізнесу, в якій загальна кількість робочих станцій не перевищуватиме 30. За основу моделі комплексу захисту буде взято елементи моделей, які відносяться до комплексної системи захисту інформації (КСЗІ). Автор праці [9] розглядає такі моделі комплексу захисту: кібернетична, функціональна, структурна та організаційна. Оскільки у бакалаврській роботі розглядається програмно-апаратне рішення, то вважаємо доцільним використовувати структурну модель.

Структурна модель відображає склад таких компонентів КСЗІ, як кадровий, організаційно-правовий та ресурсний. Кадровий та організаційно-правовий компоненти розглядатися не будуть. Ресурсний компонент представляється такими видами забезпечення, як технічне, математичне, програмне, інформаційне та лінгвістичне. Робота буде зосереджена на програмному та програмно-апаратному видах забезпечення.

Відповідно до складу інформаційних ресурсів підприємства, які потребують захисту, визначених у пункті 1.3, комплексна система захисту інформації може містити такі підсистеми:

- системи захисту на прикладному рівні;
- системи захисту на мережевому та апаратному рівнях.

Отже, визначаємо програмно-апаратний комплекс кіберзахисту підприємства як набір рішень, які містять програмне та апаратне забезпечення, що покликане повідомляти та перешкоджати проникненню і поширенню шкідливого ПЗ та інших типів атак всередині локальної мережі.

Вимогою до даного комплексу є забезпечення стабільної безперебійної роботи серверів, робочих станцій, мережевого апаратного забезпечення та користувацьких програм.

Оскільки комплекс розділений на підсистеми, то у кожної є свій ряд виконуваних функцій. Системи захисту прикладного рівня розділені на системи розмежування доступу, моніторингу і антивірусного захисту. Системи розмежування доступу регулюють процес перевірки даних, введених користувачем, на предмет відповідності існуючим записам в системі. Системи моніторингу, як говорить назва, покликані перевіряти загальний стан системи та за можливості сповіщувати уповноважену особу в разі виявлення підозрілих змін у системі. В свою чергу, система антивірусного захисту перевіряє програмне середовище комп'ютера на предмет змін файлів, налаштувань, підозрілої поведінки та при можливості лікує заражені елементи або заносить їх до ізольованого середовища – "Пісочниці" (Sandbox).

Системи захисту апаратного та мережевого рівнів поділені на такі підсистеми: мережеві екрани, засоби виявлення втручань, засоби запобігання втручань. Мережеві екрани – це перша лінія захисту. Її мета – блокування пакетів даних на вході та виході з внутрішньої мережі. Засоби виявлення та запобігання вторгнень працюють всередині мережі. Засоби виявлення вторгнень лише знаходять шкідливі пакети та надсилають сповіщення в разі виявлення, в той час як засоби запобігання надсилають сповіщення та блокують шкідливі пакети.

2.2 Системи захисту на прикладному рівні

Системи захисту на прикладному рівні включають в себе такі підсистеми [10]:

- системи розмежування доступу до інформації, ідентифікації, автентифікації, авторизації;
- системи моніторингу;
- системи антивірусного захисту.

2.2.1 Системи розмежування доступу до інформації, ідентифікації та автентифікації, авторизації

Розмежування доступу це комплексне поняття, що являє собою надання або відмова у наданні системою певних прав і привілеїв конкретному користувачу даної системи.

Існують такі моделі системи розмежування доступу до інформації відповідно до [11, 12]:

– Дискреційне розмежування доступу (Discretional access control, DAC).

– Мандатне керування доступом (Mandatory access control, MAC).

– Контроль доступу на основі ролей (Role-Based access control, RBAC).

Опис моделі розмежування доступу DAC:

Модель DAC - це управління доступом суб’єктів до об’єкта на основі матриці доступу. Для кожної пари “суб’єкт-об’єкт” повинен бути заданий чіткий перелік типів доступу, які має суб’єкт по відношенню до об’єкта системи, тобто санкціоновані. Всі суб’єкти (користувачі) системи повинні бути явно однозначно ідентифіковані. Для будь-якого об’єкта комп'ютерної системи визначений суб’єкт-власник. Власник має право надавати доступ до об’єкта зі сторони інших учасників системи. Також у системі існує привілейований користувач, який володіє правом повного доступу до об’єктів системи (або правом призначати себе власником об’єкта).

Перевагою цієї моделі розмежування доступу є проста реалізація, тобто перевірка прав доступу користувача до об’єкта виконується під час відкриття об’єкта (наприклад, файлу або директорії).

Недоліками даної моделі є:

– Статичність розмежування доступу, тобто права доступу до вже відкритого об’єкта не змінюються незалежно від поточного стану системи.

– Власник об’єкта має право надавати доступ до останнього, що є шкідливо у разі, якщо у файлі зберігається чутлива до розкриття інформація (що є порушенням конфіденційності).

Опис моделі розмежування доступу MAC

Модель MAC – це модель, яка заснована на присвоєнні мітки конфіденційності об’єктам системи та призначенні легального доступу(допуску) суб’єктам для звернення до об’єктів конфіденційності. Це означає, що кінцевий користувач системи не має можливості змінювати налаштування, які впливають на видачу міток та доступів. В свою чергу, дана модель розділяється на дві моделі безпеки, а саме, модель Біби і модель Белл-ЛаПадули [13].

– Модель безпеки Біби:

У моделі Біби, користувачі можуть створювати об’єкти на рівні нижче або рівному своєму рівню доступу. Навпаки, користувачі можуть переглядати контент з рівнем, рівним або вищим їх власного рівня доступу. Прикладом реалізації даної моделі є військове командування - генерал може написати наказ полковнику, який може видати накази майору. У випадку використання цього порядку оригінальні накази генерала зберігаються недоторканими, і місія є захищеною (таким чином забезпечується цілісність за рахунок властивості "немає читання знизу"). Навпаки, цивільний ніколи не може віддавати накази сержанту, який, ніколи віддає накази лейтенанту, що також захищає цілісність місії ("немає запису вгору").

– Модель безпеки Белл-ЛаПадули:

Принципи цієї моделі є оберненим до моделі Белла, оскільки суб’єкт з даним рівнем доступу може отримувати(зчитувати) інформацію з об’єкта тоді і тільки тоді, коли рівень доступу суб’єкта більший за рівень таємності об’єкта (принцип “немає читання зверху”). Властивість запису полягає у тому, що суб’єкт з даним рівнем доступу не може записувати інформацію в об’єкти, рівень таємності яких нижчий за рівень доступу користувача (принцип “немає запису знизу”).

Модель MAC має такі основні властивості:

– Всі суб’єкти системи однозначно ідентифіковані.

– Кожному об’єкту комп’ютерної системи присвоєна мітка конфіденційності.

– Кожному суб’єкту системи присвоюється ступінь допуску.

– Наявний лінійно-впорядкований набір міток конфіденційності та відповідних їм ступенів доступу.

– В системі наявний привілейований користувач.

– Понизити мітку конфіденційності може той суб’єкт, який має доступ до об’єкта та володіючий спеціальною привілегією.

Недоліками моделі є:

– Складність програмної реалізації.

– Зменшення ефективності роботи комп’ютерної системи оскільки перевірка прав доступу виконується як при відкритті об’єктів, так і перед виконанням дії з об’єктом (читання, запис).

Зазвичай ця модель застосовується до систем, в яких є обмін інформацією державного рівня, наприклад, державна таємниця, та до систем силових відомств.

Опис моделі розмежування доступу RBAC

Модель RBAC - це спосіб контролю доступу, визначений навколо ролей та привілеїв. Компоненти RBAC, такі як операції, правила, ролі та сесії спрощують виконання завдань користувача. Дослідження NIST [14] показало, що RBAC відповідає на багато потреб комерційних та урядових організацій.

Модель RBAC поєднує в собі властивості моделей MAC (Зв’язок “Суб’єкт-Об’єкт” в одному правилі) і DAC (Призначення ролі окремому суб’єкту/суб’єктам).

Згідно з ресурсами [15, 16, 17] , можна виділити такі компоненти моделі:

– Операції - набір можливих дій користувача, що вимагає дозволу або відмови у доступі;

– Правило - набір операцій, множини об’єктів, щодо яких можуть бути застосовані операції та ознака доступу або недоступу до операції;

– Роль - набір правил, згідно яким користувачу надається згода або відмова у доступі;

– Сесія - це набір ролей, які надаються користувачу при авторизації у системі.

Отже, враховуючи властивості, переваги і недоліки вищенаведених моделей доступу, можна зробити висновок, що найбільш гнучкою функціонально та безпечною з точки зору методів доступу до об’єктів є модель RBAC.

Нижче наведені приклади систем, які здатні реалізовувати модель RBAC:

- Microsoft Active Directory.
- Oracle Database.
- Postgre SQL.

Microsoft Active Directory

Microsoft Active Directory це LDAP-сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft для операційних систем родини Windows NT. Active Directory дозволяє адміністраторам використовувати групові політики для забезпечення подібного налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів (через групові політики або за допомогою Microsoft Systems Management Server 2003 або System Center Configuration Manager), встановлювати оновлення ОС, прикладного та серверного ПЗ на всіх комп'ютерах в мережі (із використанням Windows Server Update Services (WSUS)), Software Update Services (SUS)). Active Directory зберігає дані і налаштування середовища в централізованій базі даних [18]. Мережі Active Directory можуть бути різного розміру – від кількох сотень до кількох мільйонів об'єктів.

Oracle Database

База даних Oracle (зазвичай її називають Oracle RDBMS або просто як Oracle) – це багатомодельна система управління базами даних, що виробляється та продається корпорацією Oracle [19].

Вона зазвичай використовується для роботи в режимі онлайн обробки транзакцій та зберігання даних.

PostgreSQL

PostgreSQL – це об’єктно-реляційна система керування базами даних (далі - СКБД). Є альтернативою як комерційним СКБД (Oracle DB, Microsoft SQL server та інші), так і СКБД з відкритим кодом (MySQL, Firebird, MySQLite) [20].

Ідентифікація – це процедура розпізнавання суб’єкта за його унікальним ідентифікатором [21]. В свою чергу ідентифікатор - це ім’я об’єкта (або суб’єкта) в системі, яке однозначно визначає сутність.

Автентифікація – це перевірка суб’єкта системи на допуск до користування ресурсами даної системи [22].

Види автентифікації:

- Однофакторна автентифікація;
- Багатофакторна автентифікація.

Однофакторна автентифікація – це перевірка суб’єкта системи на знання (наявність) певного фактора – пароля (в даному випадку - фактор знання). Захист системи в даному випадку залежить від надійності (стійкості до зламу) даного пароля. Багатофакторна автентифікація ідентична однофакторній, за виключенням вимоги системи надавати два або більше факторів.

Ідентифікація та автентифікація разом являють собою процес авторизації, по завершенню якого система вирішує, давати чи не давати доступ до ресурсів даному користувачу.

Загальна схема процесу надання доступу наведена на рисунку нижче:

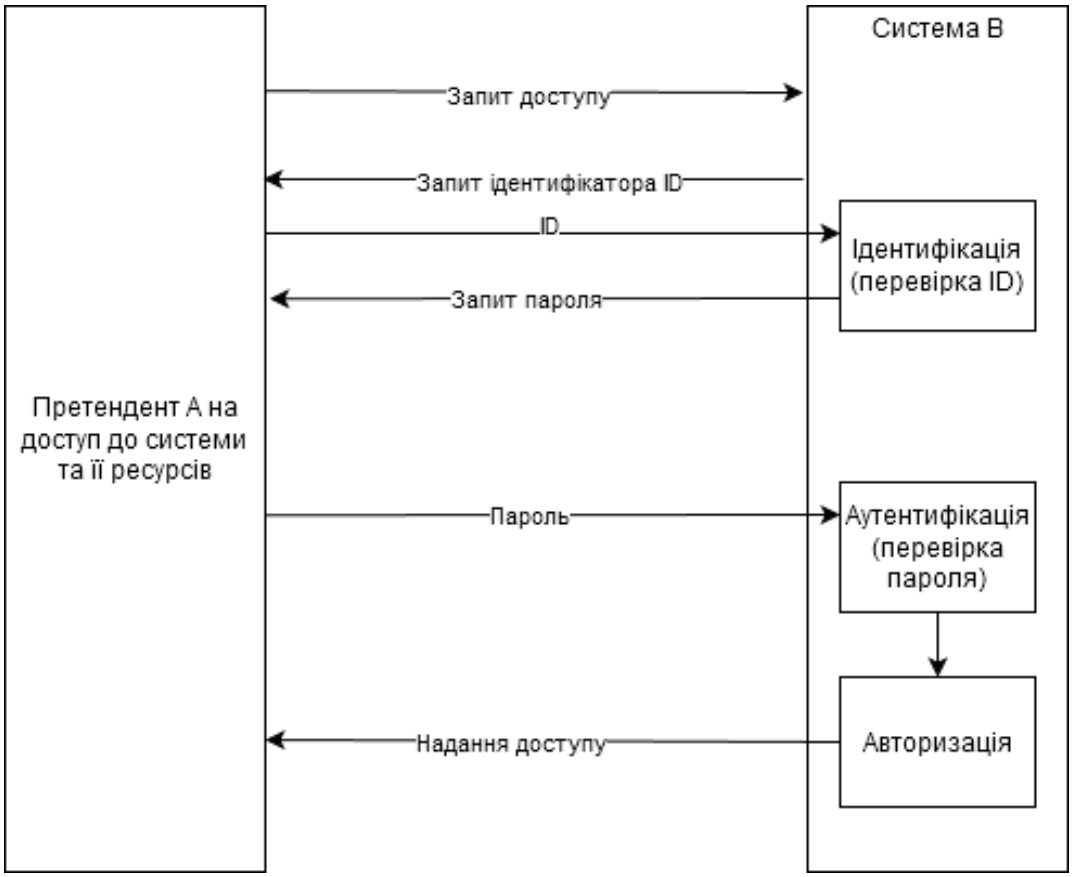


Рисунок 2.1 – Загальна схема процесу ідентифікації, автентифікації та авторизації.

Прикладами систем автентифікації та авторизації можуть бути протоколи RADIUS [23] (англ Remote Authentication in Dial-In User Service), Diameter [24] (подальший розвиток протоколу RADIUS), LDAP [25] (англ. Lightweight directory access protocol). Також існують вбудовані системи в ОС Windows та Linux (як приклад - запрошення вводу логіну та паролю при вході в систему).

2.2.2 Системи моніторингу

Моніторинг – це константний процес зчитування інформації, яка відображає загальний стан системи та можливе подальше сповіщення відповідального суб’єкта в разі виявлення інциденту. Проаналізувавши ресурс [26], можна виділити такі загальні види моніторингу:

- Моніторинг мережі та веб-сервісів;
- Моніторинг процесів операційної системи.

Спираючись на інформацію з ресурсу [27] можна зробити загальний висновок, що моніторинг мережі – це зчитування інформації, що передається комп'ютерною мережею з ціллю виявлення мережевих компонентів, що працюють неправильно або не працюють взагалі або які піддалися впливу небажаного або шкідливого програмного забезпечення. Моніторинг веб-сервісів потрібний для переконання, що веб-сторінки, веб-застосунки доступні для кінцевого користувача та працюють так, як очікується.

Моніторинг процесів операційної системи використовується для відстеження таких характеристик, як частота процесора його навантаження та температура, розмір вільної і зайнятої оперативної (ОЗП) та постійної (ПЗП) пам'яті, мережевої інформації (поточна IP-адреса, швидкість мережі тощо)[28].

Отже, спираючись на визначення понять, можна зробити висновок, що моніторингові системи можуть бути задіяні як одночасно, так і поодинці, в залежності від поставленої задачі безпеки. Прикладомm комплексного моніторингу систем та мережі є програмне забезпечення "Nagios". Програма "Nagios" пропонує такі функціональні можливості [29]:

- Моніторинг мережевих сервісів;
- Відстеження системних ресурсів;
- Відстеження стану апаратного забезпечення;
- Моніторинг через віддалено-запущені скрипти з допомогою Nagios Remote Script Executor;
- Віддалений моніторинг з допомогою SSH/SSL - туннелів;
- Можливість власноруч створити власний скрипт перевірки служб;
- Паралельна перевірка сервісів;
- Конфігураційні файли в форматі простого тексту;
- Можливість визначати елемент мережі за допомогою батьківських елементів, що дозволяє виявляти та відрізняти елементи, які є вимкнені або недоступні;

- Сповіщення про інцидент уповноважену особу;
- Автоматична обробка логів;
- Веб-інтерфейс для перегляду поточного стану мережі, сповіщень, історії інцидентів, файлів логів тощо.

Системи антивірусного захисту

Системи антивірусного захисту - це таке програмне забезпечення, яке допомагає захистити комп'ютер від зловмисних та потенційно загрозливих (небажаних) програм, відновити стан заражених файлів та регулярно перевіряти систему на наявність шкідливого програмного забезпечення. Антивірусне програмне забезпечення розглядає будь-які дані веб-сторінок, файлів, звичайного програмного забезпечення. Такі системи здійснюють пошук відомих загроз та відстежують поведінку всіх програм, відзначаючи підозрілу поведінку.

Існують різні методи виявлення потенційно небажаного програмного забезпечення [30]. Розглянемо детальніше основні з них.

- Метод сканування сигнатур

Метод заснований на пошуку у файлі унікальної послідовності байтів – сигнатури, яка є характерною для вірусу. Для кожного наступного знайденого вірусу визначається його сигнатура, яка вноситься до спеціальної бази даних, згідно якої потім антивірусне програмне забезпечення порівнює знайдені сигнатури у файлах. Головною перевагою даного методу є низький шанс помилкового спрацювання. Напроти, недоліком методу є неспроможність виявлення нового шкідливого програмного забезпечення через його відстутність у поточній базі даних.

- Метод контролю цілосності

Даний метод заснований на тому, що будь-яке несподівана та безпідставна зміна даних на носії є підозрілою подією, яка вимагає особливої уваги зі сторони антивірусної системи. Факт зміни даних, що є порушенням цілісності, встановлюється шляхом порівняння_контрольної суми, завчасно

підрахованої для початкового стану тестованого коду, та контрольної суми поточного стану тестованого коду. Якщо контрольні суми не співпадають, то для системи з’являється підстава провести додаткову перевірку, наприклад за методом сканування сигнатур.

Вказаний метод працює швидше за вищевказаний метод, оскільки операції підрахунку контрольних сум потребують менше обчислювальної потужності, ніж операції побайтового порівняння тестованих кодів.

- Метод сканування підозрілих команд

Також називається евристичним скануванням або евристичним методом. Заснований на виявленні в сканованому файлі підозрілих команд та/або ознак підозрілих кодових послідовностей (наприклад, команда форматування жорсткого диску диска або функція впровадження в виконуваний процес шкідливого коду). Цей метод, як і метод сканування сигнатур, не здатний реагувати на нові віруси.

- Метод відстеження поведінки програм

Цей метод заснований на аналізі поведінки програм в процесі виконання. Антивірусні засоби даного типу часто потребують активної участі користувача, який приймає рішення, як в майбутньому реагувати системі на підозрілу активність. Значна частина повідомлень може бути помилковою. Частота помилкових спрацювань при перевищенні певного порогу робить цей метод неефективним, а користувач може припинити реагувати на повідомлення. При використанні антивірусних систем, аналізуючих поведінку програм, був ризик виконання команд вірусного коду. Для усунення подібного недоліку був розроблений метод емуляції(імітації), який дозволяє запускати тестовану програму в штучній (віртуальній) області, яка називається “Sandbox”, без небезпеки пошкодження оточення.

Загалом, ринок даного типу систем захисту представлений багатьма комерційними та некомерційними (безкоштовними, але з можливістю апгрейду до комерційних версій) продуктами. Згідно ресурсу [31],

компаніями, які надали свої продукти в лабораторію на тестування, є Avast, Bitdefender, Cisco, CrowdStrike, Endgame, ESET, FireEye, Fortinet, K7, Kaspersky, McAfee, Microsoft, Panda, Seqrite, Sophos, SparkCognition, Symantec, Trend, VIPRE.

2.3 Системи захисту на апаратному та мережевому рівнях

Системи захисту на апаратному та мережевому рівнях покликані виявляти, сповіщати та за можливості перешкоджати просуванню шкідливого ПЗ через внутрішню мережу підприємства в разі його виявлення. Проаналізувавши ресурс [32] одними з основних систем будуть розглянуті наступні:

- Міжмережеві екрани;
- Системи виявлення втручань;
- Системи запобігання втручань.

2.3.1 Міжмережеві екрани

Мережевий брандмауер (брандмауер або міжмережевий екран) захищає комп'ютерну мережу від несанкціонованого доступу. Він може мати форму апаратного пристрою, програмного забезпечення або їх комбінації.

Міжмережеві екрани захищають внутрішню комп'ютерну мережу від несанкціонованого доступу ззовні, наприклад, заражених шкідливим програмним забезпеченням веб-сайтів або через вразливі відкриті порти мережі.

Брандмауер також може бути налаштований для обмеження доступу внутрішніх користувачів до зовнішніх з'єднань, як у випадку батьківського контролю чи блокування робочого місця.

Мережеві екрани [33, 34] поділені на два типи:

- Host-based встановлюється на кожній окремій робочій станції;
- Network-based встановлюється на робочій станції, що є виходом в мережу Інтернет.

Дані типи брандмауерів бувають програмним або апаратним забезпеченням.

Існують такі види фільтрації трафіку [35]:

- Фільтр пакетів (Packet filters)

Пакетні фільтри діють, перевіряючи пакети, передані між комп'ютерами. Якщо пакет не відповідає набору правил фільтрування, то фільтр або відкидає (тобто не генерує причину відмови) пакет, або відхиляє пакет (відкидає його та генерує повідомлення ICMP (internet control message protocol) відправнику пакета), інакше пропускає пакет до мережі.

Пакети можуть бути відфільтровані за мережевими адресами джерела та пункту призначення, протоколом, номерами джерела та пунктом призначення.

- З запам'ятовуванням стану (Stateful filters)

Брандмауери цього виду виконують роботу своїх попередників першого покоління, але також зберігають дані про конкретні сесії між кінцевими точками, запам'ятовуючи, який номер порту обидва IP-адреси використовують на рівні 4 (транспортний рівень) моделі OSI, що дозволяє перевірити загального обміну між вузлами. Цей тип брандмауера є потенційно вразливим до атак відмови в обслуговуванні (DoS - Denial of Service), які заповнюють буфер підключень брандмауера фальшивими з'єднаннями.

- Фільтрація даних застосунків

Основна перевага фільтрації даних додатків полягає в тому, що він може обробляти певні програми та протоколи (наприклад, протокол передачі файлів (FTP), система доменних імен (DNS) або протокол передачі гіпертексту (HTTP). Це дозволяє виявити, чи небажана програма чи послуга намагаються втрутитись у систему за допомогою забороненого протоколу на дозволеному порту, або виявити, чи скомпрометовані дані в пакеті протоколу.

2.3.2 Системи виявлення вторгнень

Система виявлення вторгнень (IDS - Intrusion Detection System) – це система, яка контролює мережевий трафік на предмет підозрілої активності та

видає сповіщення про виявлення такої активності [36]. Це програмне забезпечення, яке сканує мережу або систему на предмет шкідливих дій чи порушень політики. Про будь-яке небажану або підозрілу подію чи порушення зазвичай повідомляється або адміністратору, або збирається централізовано, використовуючи систему безпеки та управління подіями (SIEM). Система SIEM використовує методи фільтрації тривоги, щоб відрізняти зловмисну активність від помилкових тривог.

Хоча системи виявлення вторгнень контролюють мережі на предмет потенційно шкідливої активності, вони також піддаються помилковим сигналам тривоги. Отже, організаціям потрібно налагодити свої продукти IDS під час їх першого встановлення. Це означає, що належним чином налаштувати системи виявлення вторгнень, щоб визначити, як виглядає звичайний трафік у мережі порівняно зі шкідливою активністю.

Системи виявлення вторгнень також здійснюють моніторинг мережевих пакетів, які вводять в систему, щоб перевірити шкідливі дії, пов'язані з ними, і одразу надсилають попередження.

Класифікація даних систем включає такі типи:

– Мережева система виявлення вторгнень (NIDS)

Мережеві системи виявлення вторгнень (NIDS- Network intrusion detection system) встановлюються у центральній точці мережі для дослідження трафіку з усіх пристроїв у мережі. Він здійснює спостереження за пропущеним потоком даних і порівнює трафік, який передається по підмережах, з базою відомих атак. Після виявлення такої або спостерігається атипічна поведінка, попередження може бути відправлено адміністратору. Прикладом NIDS є встановлення його в підмережі, де розташовані брандмауери, щоб перевірити, чи хтось намагається зламати брандмауер.

– Система виявлення вторгнень на базі хосту (HIDS)

Такі системи працюють на незалежних пристроях у мережі. HIDS (Host intrusion detection system) відстежує лише вхідні та вихідні пакети з пристрою

та попереджатиме адміністратора, якщо буде виявлено підозрілу чи зловмисну активність. Система запам’ятовує стан існуючих системних файлів і порівнює його з попереднім станом. Якщо файли системи були відредаговані або видалені, адміністратору надсилається попередження для дослідження. Приклад використання HIDS можна побачити на критично важливих машинах, які, як очікується, не повинні змінювати свій стан.

– Система виявлення вторгнень на основі протоколу (PIDS)

Система виявлення вторгнень на основі протоколу (PIDS) складається з системи або агента, який контролює та інтерпретує дані протоколу між користувачем / пристроєм та сервером.

– Система виявлення вторгнень на основі протоколу додатків (APIDS).

Система виявлення вторгнень на основі протоколу додатків (APIDS) - це система або агент, який зазвичай знаходиться в групі серверів. Він ідентифікує вторгнення шляхом моніторингу та інтерпретації з’єднань на конкретних протоколах додатків. Наприклад, система може відстежувати протокол SQL.

– Гібридна система виявлення вторгнень.

Гібридна система виявлення вторгнень виробляється комбінацією двох або більше підходів системи виявлення вторгнень. У гібридній системі виявлення вторгнень хост-агент або дані системи поєднуються з мережевою інформацією для створення повного перегляду мережевої системи. Гібридна система виявлення вторгнень є більш ефективною порівняно з іншими системами.

IDS-системи використовують такі методи виявлення втручань:

– Метод на основі сигнатур

IDS на основі сигнатур визначає атаки на основі конкретних шаблонів, таких як кількість байтів або число 1 або число 0 у мережевому трафіку. Він також виявляє на основі вже відомих послідовностей коду, які використовуються зловмисним програмним забезпеченням. Виявлені

шаблони в IDS відомі як сигнатури. Недоліком цього методу є складність виявлення загрози, якщо відсутній запис про неї в базі.

– Метод на основі аномалій

IDS на основі аномалії був введений для виявлення невідомих атак зловмисного програмного забезпечення, оскільки нові шкідливі програми швидко розвиваються. У IDS на основі аномалії використовується машинне навчання для створення довірчої моделі поведінки, і дані, які проходять через мережу, порівнюються з цією моделлю, і оголошуються підозрілими, якщо вони не відповідають створеній моделі. Метод машинного навчання має кращу ефективність з IDS на основі сигнатур, оскільки ці моделі можуть бути навчені відповідно до програмних та апаратних налаштувань.

2.3.3 Системи запобігання вторгнень

Система запобігання вторгнень (IPS) – це форма захисту мережі, яка працює на виявлення та запобігання виявленим загрозам. Системи попередження вторгнень постійно контролюють мережу, шукаючи можливі шкідливі випадки та фіксуючи інформацію про них. IPS повідомляє про ці події системним адміністраторам і вживає запобіжних заходів, таких як закриття точок доступу та налаштування брандмауерів для запобігання майбутніх атак [37]. Рішення IPS можуть також використовуватися для виявлення проблем із політикою безпеки.

Аналогічно до систем IDS, системи IPS використовують такі методи запобіганню вторгнень:

– Метод на основі сигнатур

Підхід на основі сигнатур використовує попередньо визначені сигнатури відомих мережевих загроз. Коли ініціюється атака, яка відповідає одній з цих сигнатур чи зразків, система вживає визначені заходи.

– Метод на основі аномалій

Іншими словами - невідповідність даних в мережі моделі типової поведінки вже існуючого програмного забезпечення. Якщо виявлена аномалія, то система негайно блокує доступ до цільового хоста.

– Метод на основі політик безпеки

Цей підхід вимагає від адміністраторів налаштування політики безпеки відповідно до політик безпеки організації та мережевої інфраструктури. Коли відбувається діяльність, яка порушує політику безпеки, спрацьовує попередження та надсилається системним адміністраторам.

Системи запобігання вторгнень працюють шляхом сканування всього мережевого трафіку. Існує ряд загроз, проти яких призначені IPS:

– Атака відмови у службі (DoS - Denial of service);

– Атака розподіленої відмови в обслуговуванні (DDoS - Distributed denial of service);

– Різні види експлойтів (вразливості в ПЗ, які можна використати);

– Комп'ютерні віруси.

IPS здійснює перевірку пакетів у режимі реального часу, глибоко перевіряючи кожен пакет. Якщо виявлені будь-які зловмисні або підозрілі пакети, IPS може здійснити одну з наступних дій:

– Припинить сеанс, який використовується і заблокує IP-адресу або обліковий запис користувача, що порушує правила;

– Перепрограмує або переконфігурує брандмауер, щоб запобігти подібній атаці в майбутньому;

– Видалить або змінить будь-який шкідливий вміст пакету. Це робиться шляхом переупаковки корисних даних, видалення інформації заголовка та видалення заражених вкладень з файлів.

Основна відмінність IPS від IDS полягає в дії, яку вони вживають, коли виявлено потенційний інцидент. Системи запобігання вторгнень контролюють доступ до IT-мережі та захищають її від можливих атак. Ці системи призначені для моніторингу даних про вторгнення та вжиття необхідних заходів для

запобігання розвитку нападу. Системи виявлення вторгнень не розроблені для блокування атак і просто контролюють мережу та надсилають попередження системним адміністраторам у разі виявлення потенційної загрози.

3. РОЗРОБКА МОДЕЛІ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

3.1 Складові програмно-апаратного комплексу

Оскільки метою роботи є модель комплексу кіберзахисту підприємства малого розміру (кількість робочих станцій до 30 шт.), то розгляд безкоштовних засобів є доцільнішим, оскільки платні версії засобів розраховані саме на велику кількість робочих станцій для масштабних проєктів. Перейдемо до розгляду і порівняння існуючих рішень.

3.1.1 Системи захисту на прикладному рівні

Системи розмежування доступу до інформації, ідентифікації та автентифікації, авторизації

Оскільки найпопулярнішою операційною системою робочих станцій є Windows (згідно з джерелом [38]), то доцільно використовувати систему розмежування доступу Active Directory.

Служби Active Directory (AD) – рішення від компанії Microsoft, яке дає можливість об'єднати об'єкти мережі (комп'ютери, сервери, принтери) в єдину систему. AD виступає в ролі каталогу (бази даних), в якому зберігається інформація про користувачів, ПК, сервери, мережеві і периферійні пристрої.

Для реалізації даного рішення, необхідний спеціальний сервер – контролер домену. Він виконує функції аутентифікації користувачів і пристроїв у мережі. При спробі використати будь-який з об'єктів (ПК, сервер, принтер) мережі, виконується звернення до контролера домену, який або дозволяє цю дію (є необхідні права), або блокує її.

Всі дані користувачів (логіни та паролі) зберігаються в єдиній базі даних, що істотно спрощує роботу з ними. При авторизації всі комп'ютери звертаються до цієї бази даних, завдяки чому внесені зміни будуть застосовані до всіх комп'ютерів мережі. Також за допомогою AD реалізуються політики

безпеки, завдяки яким можна обмежити (або дозволити) доступ до певних серверів.

Оскільки база даних зберігається на контролері доменів, тому в разі його відмови, вся система буде недоступною. Для забезпечення відмовостійкості слід розгорнути один або більше дублюючих контролерів доменів і налаштувати автоматичну реплікацію (тобто синхронізацію даних між серверами). У даному випадку, при виході з ладу одного з контролерів працездатність мережі не порушується.

Щодо СКДБ, то існують комерційні і некомерційні продукти. Перевага віддається саме некомерційним. Нижче наведена таблиця порівняння СКДБ.

Таблиця 3.1 Порівняння СКДБ

Параметр	Oracle	MySQL	PostgreSQL
Тип	Об’єктно-реляційна СКБД	Реляційна СКБД	Об’єктно-реляційна СКБД
Мова	Java, C, C++	C, C++	C
Операційна система	Кроссплатформенна	Кроссплатформенна	Кроссплатформенна
Ліцензія	Комерційна/Некомерційна (Express Edition)	Комерційна/Некомерційна	Некомерційна
Остання версія	19c (13 лютого 2019)	8.0.9 (9 грудня 2019) 5.7.29(18 грудня 2019)	12.2(13 лютого 2020)

Варто звернути увагу на характеристики некомерційної версії Oracle Express Edition – максимальный розмір бази даних – 11 ГБ, а з версії 18c максимальний розмір бази даних – 12 ГБ. Враховуючи те, що потенційний розмір баз даних підприємства до 100 робочих станцій може перевищувати даний обсяг – ця СКБД відкидається зі списку тих, що можуть використовуватися на заданому типі підприємства.

Відповідно до ресурсу [39], PostgreSQL має безпекову модель, засновану на ролях, в той час як безпека MySQL заснована на списках контролю доступу. Оскільки рольова модель є більш гнучкою, перевага віддається PostgreSQL.

Системи моніторингу

На даний момент ринок даних засобів моніторингу умовно розділяється на дві категорії: моніторинг декількох пристроїв для безкоштовних версій програмного забезпечення з обмеженим функціоналом та моніторинг великої кількості мережевих об’єктів, але з коротким безкоштовним пробним періодом та подальшою купівлею корпоративної ліцензії (її часто називають Enterprise edition) – в залежності від кількості мережевих вузлів.

Оскільки в бакалаврській роботі розглядається мережа до 30 робочих станцій (невелике підприємство), то купівля корпоративної ліцензії недоцільна, як і безкоштовні продукти з обмеженим функціоналом.

Варто зазначити, що системи моніторингу можуть бути вбудовані в корпоративні версії систем антивірусного захисту. Із огляду на те, що підприємство може володіти обмеженими фінансовими ресурсами, то доцільніше використовувати системи, які мають змішаний функціонал.

Системи моніторингу мережі, як було описано в п. 2.2, потрібні для відслідковування споживання мережевого трафіку програмами. Сучасний ринок представлений багатьма програмами [40, 41]: Total Network Monitor, Observium, Nagios, Cacti, PRTG Network Monitor, Kismet, WireShark, NeDi, Zabbix, Icinga, Network Olympus Monitoring та інші, але ми будемо розглядати Windows-сумісні. Такими є Network Olympus Monitoring, WireShark,

Observium, Kismet, Cacti. Серед них безкоштовними є WireShark, Network Olympus, Kismet та Cacti. Kismet є рішенням для аналізу безпровідного трафіку (Wireless), тож його ми розглядати не будемо. Cacti вимагає наявність бази даних MySQL та не підтримує PostgreSQL, тож цей продукт також не буде розглядатися в порівнянні. Функціонал безкоштовної версії Observium надає дуже обмежений набір опцій. NeDi не підтримує ОС Windows. Аналіз продукту Network Olympus Monitoring на сайті виробника показав, що програмне забезпечення не надає детальної документації, також продукт не розглядається в порівняльних списках на сайтах англомовного сегменту. Звернемо увагу на продукт Wireshark. Відповідно до ресурсу [42] Wireshark надає такі можливості:

– Захоплення пакетів з мережевого з'єднання або перегляд вже захоплених пакетів зі збереженого файлу.

– Зчитування даних з таких інтерфейсів, як Ethernet, IEEE 802.11, PPP та loopback.

– Захоплені дані можна переглядати на графічному інтерфейсі.

– Вибір фільтру для відображення захоплених пакетів.

– Можливість захоплення VoIP-з'єднань та їх відтворення.

– Захоплення USB-трафіку.

– Захоплення бездротових з'єднань.

– Можливість перегляду статистики.

Як, видно, з функціоналу, Wireshark відноситься до програм-аналізаторів трафіку. Програма повністю безкоштовна та не має обмежень на кількість робочих станцій у мережі. Функціонал даної програми є достатнім для відстеження проблем у мережі.

Системи антивірусного захисту

Ринок антивірусних систем представлений антивірусними програмами таких компаній, як Avast, Bitdefender, Cisco, CrowdStrike, Endgame, ESET, FireEye, Fortinet, McAfee, Symantec та інших. Вибір продукту буде

проводитись за допомогою звітів, складених лабораторією “AV Comparatives” у 2019 році, відповідно до яких були перевірені саме корпоративні версії антивірусного програмного забезпечення.

Процедура тестування продуктів відбувалася за такими показниками:

- Тест захисту в реальному часі.
- Була проведена перевірка захисту на 844 тестових сценарії.
- Тест захисту на шкідливе ПЗ.
- Перевірка реакції захисту на 1278 різних вірусів.
- Тест продуктивності системи з працюючим антивірусним ПЗ.

Відповідно до результатів тестів, продукт від компанії Avast (Business Pro Plus) зайняв першу позицію. Згідно з описом продуктів ПЗ на сайті виробника [43], для корпоративного використання є три версії – Avast Business Antivirus, Avast Business Antivirus Pro, Avast Business Antivirus Pro Plus. Функціонал версії Avast Business Antivirus має оптимальний набір можливостей для того, щоб не задіювати системи моніторингу як окремий клас систем захисту для даного розміру підприємства.

3.1.2 Системи захисту апаратного та мережевого рівнів

Мережевий екран

Мережеві екрани (брандмауери, фаєрволи) є у вигляді програмного забезпечення та апаратного забезпечення. Аппаратне забезпечення ми не беремо до уваги, оскільки воно занадто коштовне. Платні версії фаєрволів також не мають сенсу для маленького підприємства. Безкоштовні версії мережевих екранів надають приблизно схожий функціонал, але деякі можуть постачатися разом з антивірусом [44]. Такі фаєрволи ми теж оминаємо, оскільки є окреме антивірусне ПЗ.

Прикладами безкоштовних мережевих екранів є GlassWire, NetDefender та TinyWall. Використаємо порівняння методом експертних оцінок [45]. Експертна група буде складатись з 4 чоловік. Метод експертних оцінок полягає в тому, що кожний з експертів надає оцінку кожному з об’єктів

порівняння (в нашому випадку об’єктом є ПЗ). Для більш точного результату будуть використані наступні методи:

– безпосереднього призначення коефіцієнтів ваги;

– коефіцієнтів ваги важливості в балах.

Метод безпосереднього призначення коефіцієнтів ваги означає, що кожен експерт окремо дає свою оцінку кожному з параметрів, що в сумі оцінка за параметрами не перевищує 1. Нижче наведена таблиця результатів з використанням даного методу.

Таблиця 3.2 – Метод безпосереднього призначення коефіцієнтів ваги.

Експерт	Параметр			Сума
	GlassWire	NetDefender	TinyWall	
1	0.5	0.2	0.3	1
2	0.5	0.3	0.2	1
3	0.2	0.4	0.4	1
4	0.2	0.3	0.5	1
Коеф.ваги	0.35	0.30	0.35	

За результатами першого методу продукти від GlassWire та TinyWall отримали однакові коефіцієнти ваги, тож скористаємось іншими методами. Метод призначення коефіцієнтів ваги в балах виконується шляхом призначення експертами оцінки кожному з порівнюваних параметрів в межах від 1 до 10. Далі записується сума оцінок в рядку для кожного з експертів і будується таблиця з такими ж полями, як в табл. 3.2, але в значеннях для параметрів записуються коефіцієнти відносні до суми за рядком. Далі наведені таблиці, які це показують.

Таблиця 3.3 – Метод безпосереднього призначення коефіцієнтів. Експертні оцінки параметрів.

Експерт	Параметр			Сума
	GlassWire	NetDefender	TinyWall	
1	9	7	6	22
2	8	6	7	21
3	5	6	4	15
4	6	5	7	16

Далі порахуємо коефіцієнт ваги кожного з параметрів відносно суми для кожного з експертів (табл. 3.4).

Таблиця 3.4 – Коефіцієнти ваги за методом безпосереднього призначення ваги в балах.

Експерт	Параметр		
	GlassWire	NetDefender	TinyWall
1	0.409091	0.318182	0.272727
2	0.380952	0.285714	0.333333
3	0.333333	0.4	0.266667
4	0.333333	0.277778	0.388889
Коеф. ваги	0.36	0.32	0.32

Як, видно, за результатами порівнянь, продукт від GlassWire в середньому набрав вищу вагу, ніж інші. Тестові запуски програм показали, що GlassWire не завжди запускається, а також NetDefender є застарілим. Отже, продукт TinyWall буде використаний як міжмережевий екран.

Системи виявлення і запобігання вторгнень

Ринок IDS/IPS систем загалом ділиться на 2 категорії – апаратні рішення та програмні рішення. Апаратні рішення являють собою свого роду комп'ютери, які підключаються безпосередньо до точки в локальній мережі. Програмні рішення в свою чергу потребують платформу для встановлення – локальний комп'ютер.

Будуть розглянуті дві найпопулярніші системи IDS/IPS на ринку програмного забезпечення з відкритим вихідним кодом (тобто безкоштовні). Це Snort та Suricata.

Snort – мережева система виявлення вторгнень (NIDS), яка написана мовою програмування C. Вона була розроблена у 1998 році Мартіном Рошем. Зараз програма викуплена та розробляється компанією Cisco. Це безкоштовне програмне забезпечення з відкритим кодом [46]. Вона також може бути використана як сніффер пакетів для моніторингу системи в режимі реального часу. Адміністратор мережі може використовувати продукт для перегляду всіх вхідних пакетів та пошуку небезпечних для системи. Вона заснована на інструменті бібліотек захоплення пакетів. Правила досить легко створювати та впроваджувати, і можуть бути розгорнуті в різних ОС. Перевагами цього ПЗ є:

- Монітор трафіку в реальному часі.
- Логування пакетів.
- Аналіз протоколів.
- Співставлення вмісту пакета.
- Створює логи (журналювання).
- Відкритий вихідний код.

– Правила легко імплементуються.

В свою чергу недоліками є те, що Snort не спроможний підтримувати функцію IPS під Windows-системами та застарілий програмний движок. Це означає, що Snort використовує лише одне ядро або один поток центрального процесору, що відбивається на ефективності аналізу великого об’єму мережевого трафіку.

Suricata – це система виявлення вторгнень (IDS) та система запобігання вторгнень (IPS) на основі відкритого джерела. Вона була розроблена Фондом відкритої безпеки (OISF). Бета-версія була випущена в грудні 2009 року, а перший стандартний реліз з’явився в липні 2010 року.

Можливості цього продукту подібні до можливостей Snort, але движок підтримує багатоядерність/багатопотоковість, що позитивно впливає на аналіз великого обсягу трафіку. Також Suricata може реалізувати функціонал Network Security Monitoring (NSM).

Обидві системи є NIDS/NIPS, що означає, що їх не потрібно встановлювати на кожну окрему робочу станцію, а лише у точці входу в локальну мережу.

Задачі, що буде вирішувати цей комплекс

Відповідно до поставленого завдання, комплекс призначений захищати бізнес-процес підприємства засобами захисту прикладного, апаратного та мережевого рівнів. Системи захисту прикладного рівня контролюватимуть доступ до робочих станцій та контролюватимуть безпечність роботи шляхом сканування середовища на віруси. Системи захисту мережевого та апаратного рівнів знизять можливість несанкціонованого доступу до загальної внутрішньої мережі.

Системами прикладного рівня обрані:

– Система розмежування доступу до інформації – продукт Microsoft Active Directory.

– Система моніторингу – Wireshark.

– Система антивірусного захисту – Avast Free Antivirus.

Системами мережевого та апаратного рівнів обрані:

– Міжмережевий екран – TinyWall.

– Система IDS – Suricata.

– Система IPS – Suricata.

Опис технології налаштування на підприємстві системи кіберзахисту

Оскільки дані системи вводитимуться в експлуатацію перший раз у новій мережі, то потрібно ізолювати дану мережу від мережі Інтернет, оскільки на ній відсутній захист. У звязку з тим, що системи розмежування доступу, система моніторингу, міжмережевий екран та IDS/IPS є системами контролю та спостереження, то вони повинні бути встановлені у центральній точці або точці входу в локальну мережу.

Так як використовуються програмні рішення, які повинні встановлюватися безпосередньо на комп'ютер, то функцію маршрутизатора буде виконувати комп'ютер. Також цей комп'ютер буде контролером домену для Active Directory. Нижче наведена загальна схема мережі підприємства (рис. 3.1).

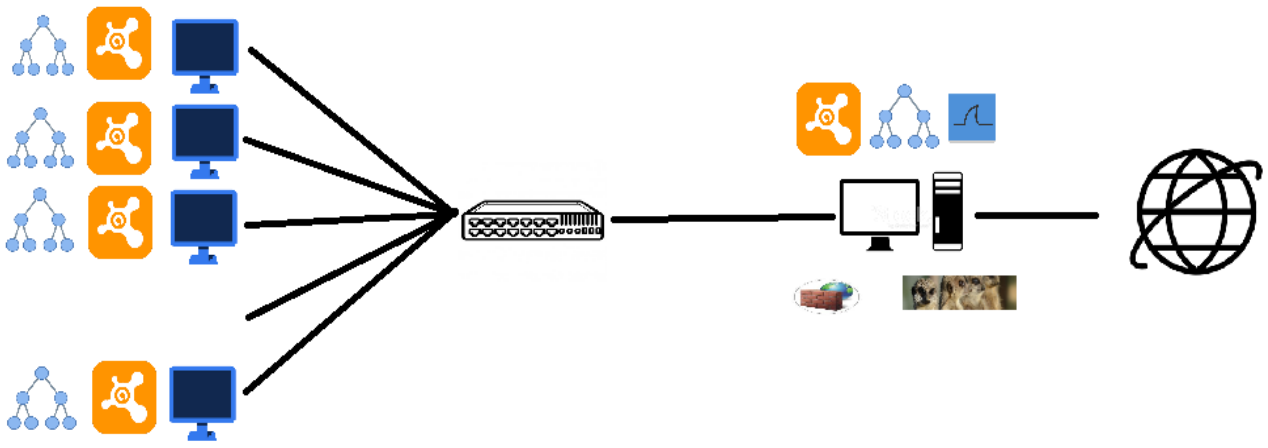
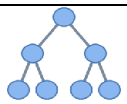


Рисунок 3.1 – Загальна схема мережі.

Умовні позначення наведені у таблиці 3.5.

Таблиця 3.5 – Умовні позначення на схемі мережі.

	Active Directory [47]
	Avast Free Antivirus [48]
	Wireshark [49]
	TinyWall [50]
	Suricata [51]
	Робоча станція [52]
	Головний комп’ютер в ролі роутера [53]
	Комутатор [54]
	Мережа Internet [55]

3.2 Налаштування програмно-апаратного комплексу

Налаштування програмно-апаратного комплексу починаємо з налаштування головної робочої станції. Вимогою до цього комп’ютера є наявність двох мережевих карт. Це потрібно для того, щоб з’єднати комутатор, до якого приєднані робочі комп’ютери, з головним комп'ютером, та приєднати головний комп’ютер до мережі Інтернет. Також варто звернути увагу на те, що рекомендована операційна система – Windows Server 2008 або вище.

Загальні налаштування Active Directory.

Додавання користувача та робочої станції в домен (виконуються на Контролері домена):

1. Створення облікового запису користувача для Адміністратора.

– Натискаємо кнопку «Пуск», переходимо в «Адміністрування», обираємо «Active Directory – користувачі і комп’ютери» (рис. 3.2);

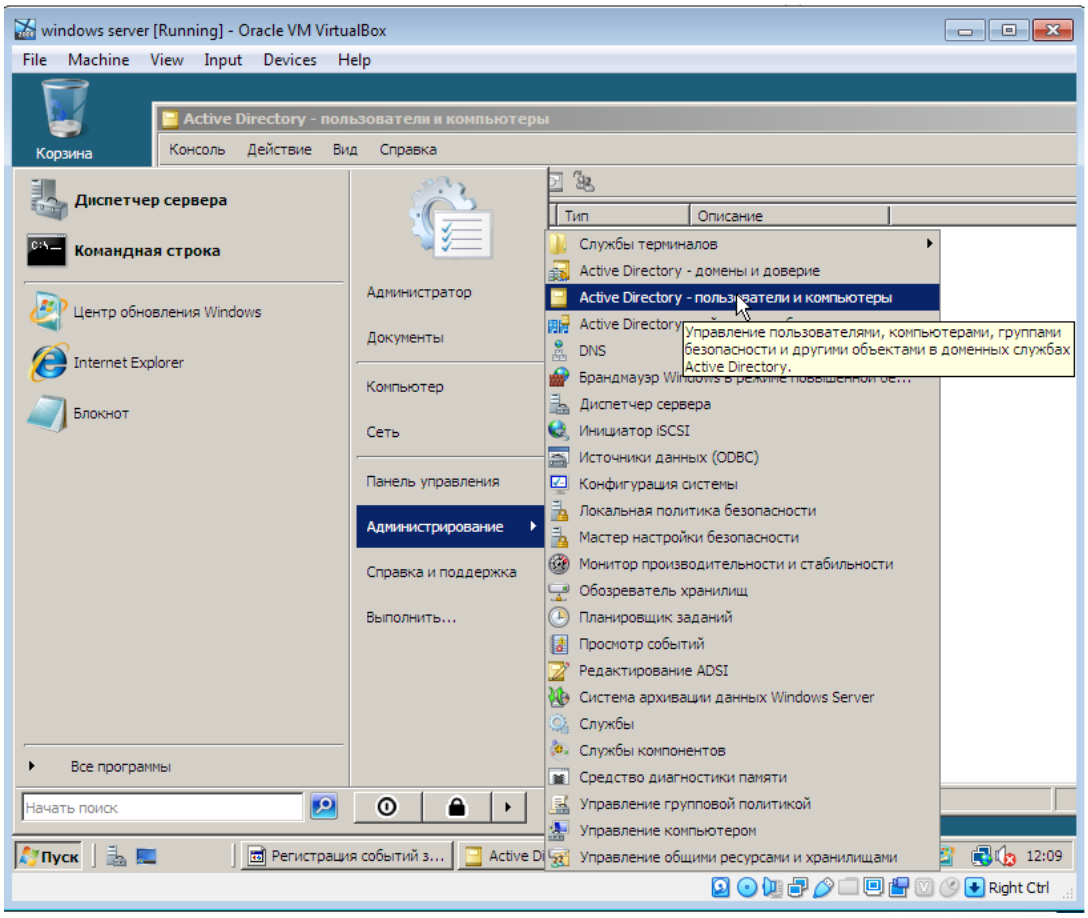


Рисунок 3.2 – Active Directory – користувачі і комп’ютери

– Відкриваємо створений домен, обираємо папку «Users», потім у контекстному меню обираємо команди «Створити» і «Користувач» (рис. 3.3);

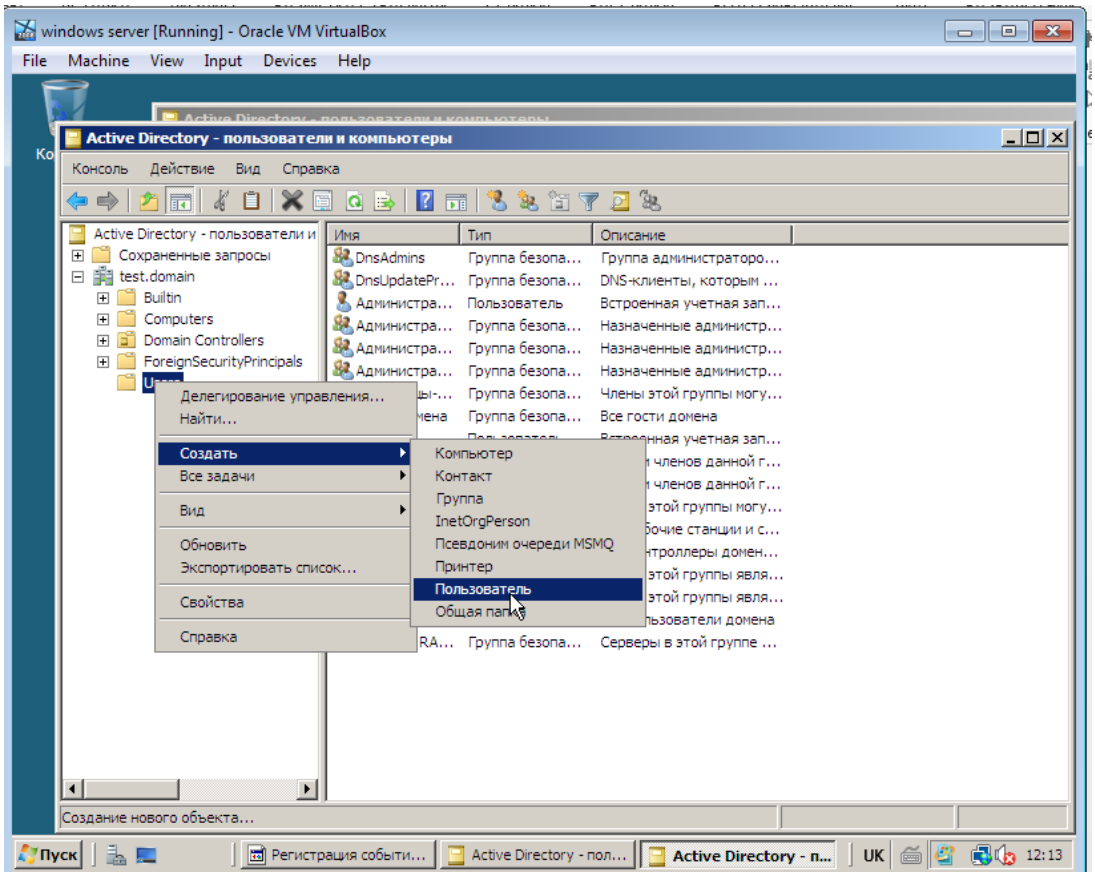


Рисунок 3.3 – Створення користувача

– У новому вікні вводимо “Ім’я - admin”, “Ім’я входу користувача - admin”, натискаємо “Далі”, вводимо і підтверджуємо пароль, натискаємо “Далі” і “Готово” (рис. 3.4);

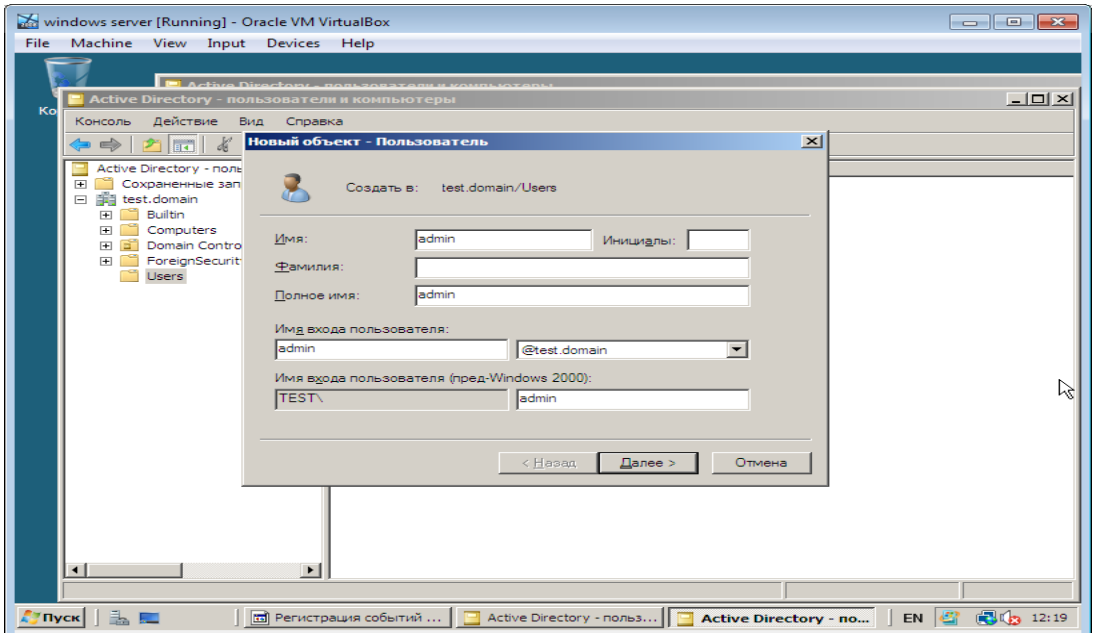


Рисунок 3.4 – Введення параметрів користувача

– Додаємо створеного користувача до всіх груп адміністраторів.

2. Додавання робочої станції до домена (безпосередньо на робочій станції).

– Переходимо до “Панель керування”, “Система та безпека”, “Система”;

– Натискаємо “Змінити параметри”;

– Переходимо до властивості “Ім’я комп’ютера” і обираємо “Ідентифікація”;

– Обираємо варіант “Комп’ютер входить до корпоративної мережі”, натискаємо “Далі”;

– Обираємо “Моя організація використовує мережу з доменами”, натискаємо “Далі”;

– Натискаємо “Далі”, вводимо ім’я користувача (адміністратора), пароль та назву домену;

– Обираємо “Додати наступний обліковий запис користувача в домені”, вводимо ім’я користувача і домен користувача, натискаємо “Далі”;

– Обираємо тип облікового запису як “Адміністратор”, оскільки далі потрібно буде встановити антивірусне ПЗ на робочу станцію.

Налаштування Avast Free Antivirus.

Налаштування Avast Free Antivirus здійснюємо за такою інструкцією [57]:

1. Завантажити файл установки
2. Запустити завантажений файл від імені Адміністратора.
3. При появі запиту на дозвіл робити зміни натиснути “Так”.
4. Дочекатися завершення процесу установки.
5. Прийняти або відхилити запит на анонімне відправлення та подальшу обробку користувацьких даних.
6. Відкрити інтерфейс антивірусної програми (рис. 3.5).

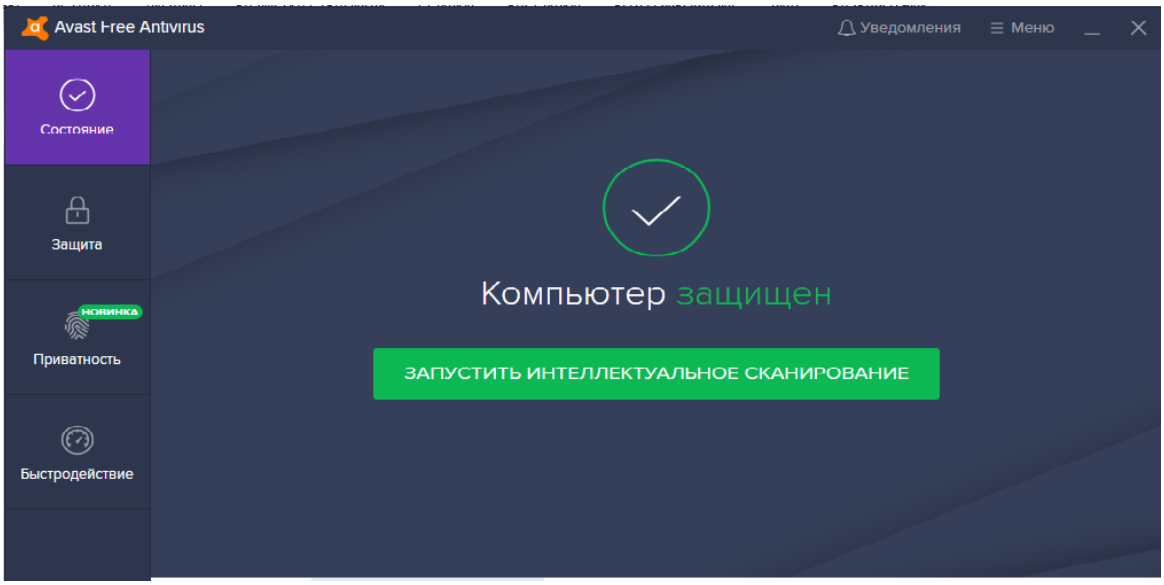


Рисунок 3.5 – Інтерфейс антивірусної програми

7. Обрати меню “Захист”, далі – “Основні компоненти захисту” (рис. 3.6).

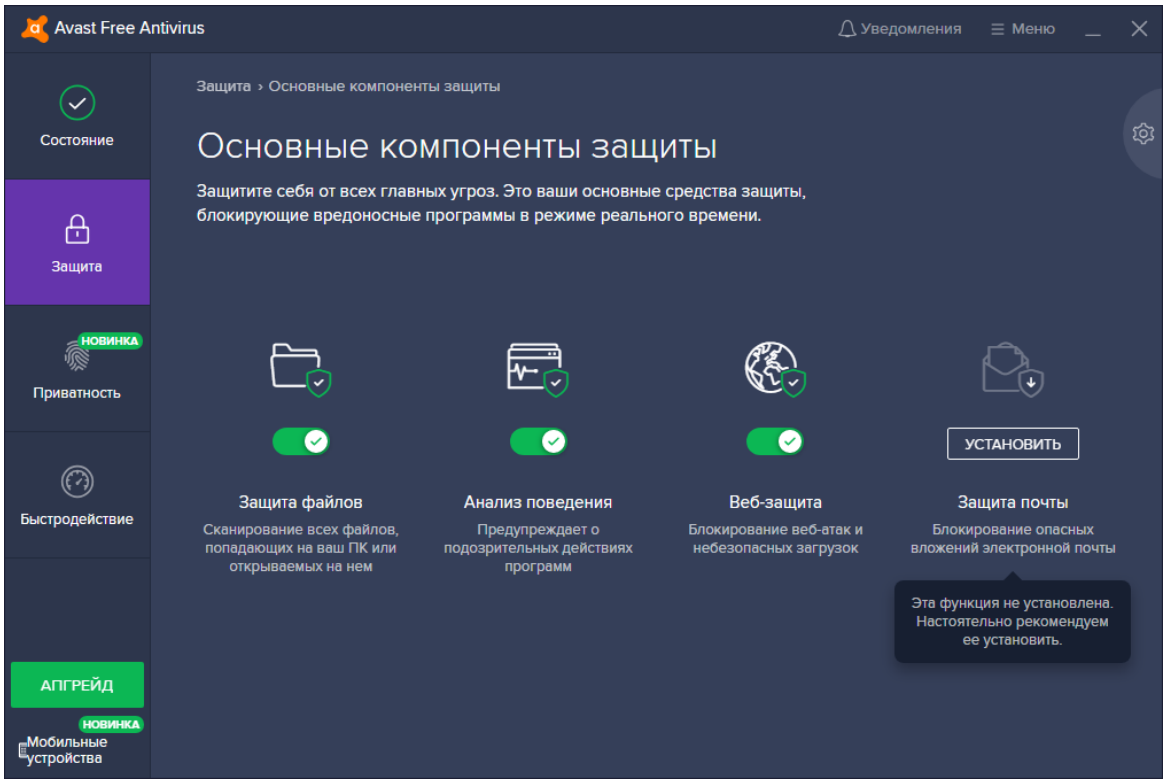


Рисунок 3.6 – Основні компоненти захисту

8. Увімкнути “Захист файлів”, “Аналіз поведінки”, “Веб-захист”, “Захист пошти”.

Налаштування Wireshark.

1. Завантажити та встановити Wireshark-win64-3.2.4.exe

2. При встановленні у вікні “Choose components” обрати потрібні компоненти.

3. Встановити Npcap і завершити встановлення.

4. Відкрити файл Wireshark.exe від імені Адміністратора.

5. При відкритті обрати інтерфейс зі списку, який буде відслідковуватись програмою (рис. 3.7, рис. 3.8).

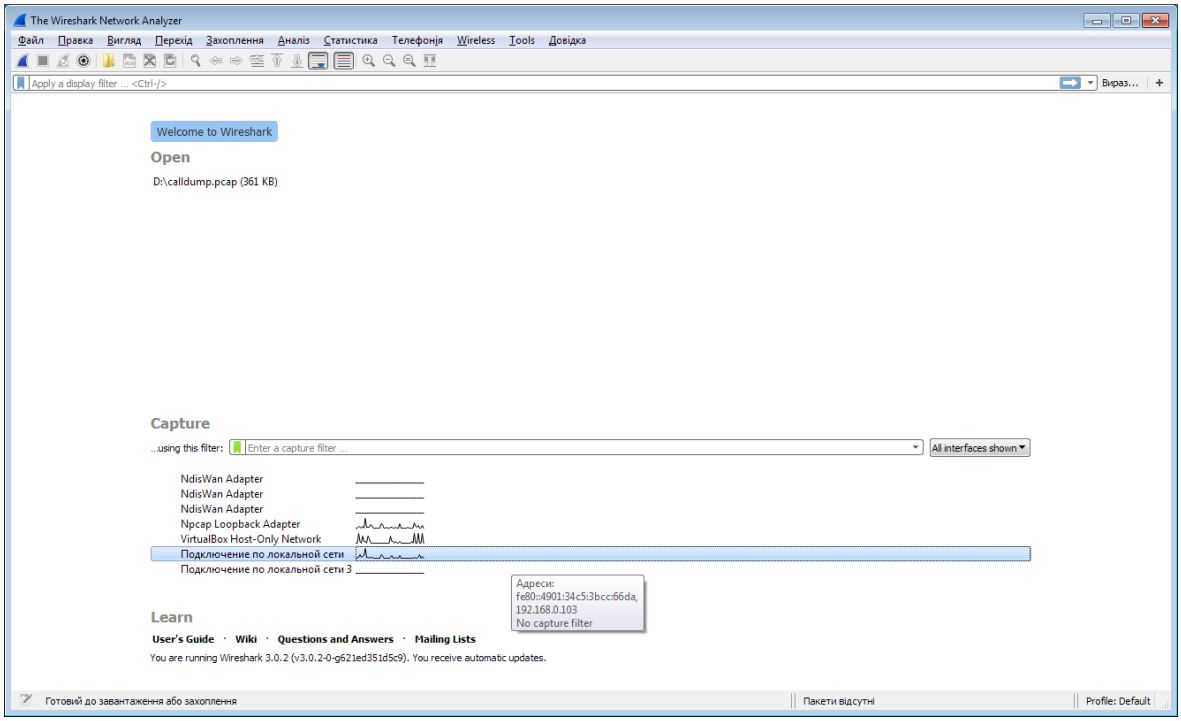


Рисунок 3.7 – Обрання інтерфейсу

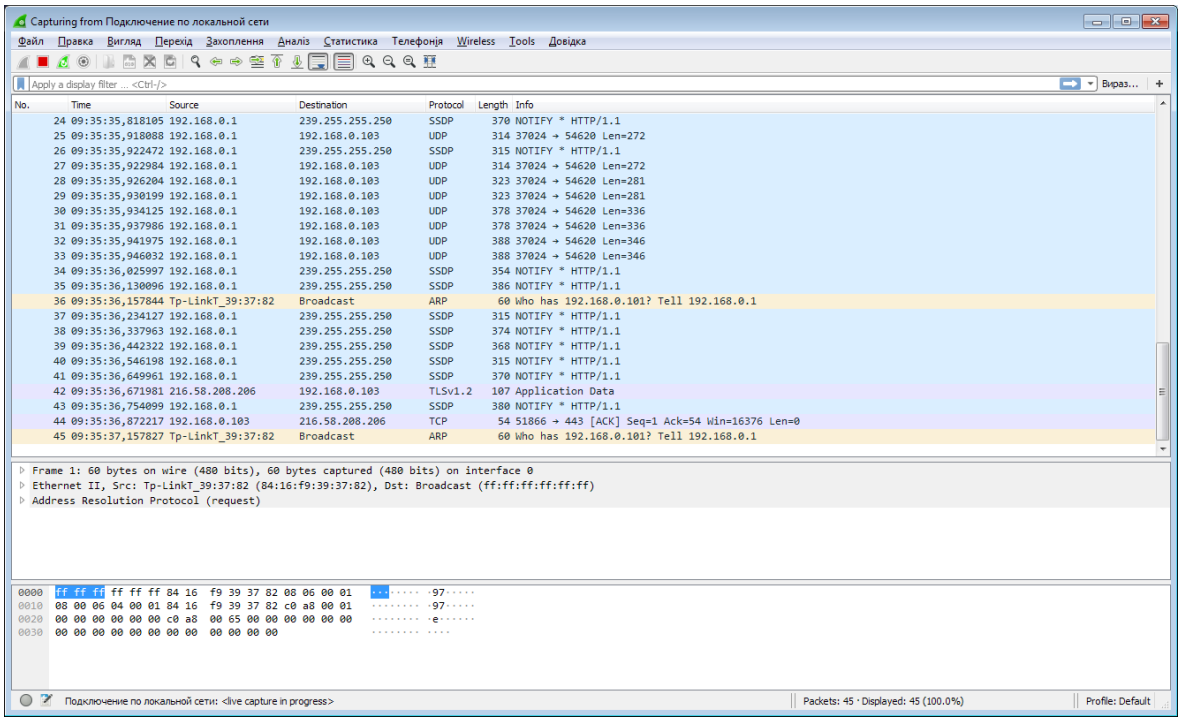


Рисунок 3.8 – Відслідковані пакети

Налаштування TinyWall.

1. Завантажити TinyWall-v3-Installer.msi, запустити TinyWall-v3-Installer.msi та встановити програму.

2. Запустити TinyWall Controller.

3. В статус-барі (справа знизу) натиснути правою кнопкою миші на іконку TinyWall та обрати підменю “Налаштування” (рис. 3.9).

4. В новому вікні обрати “Застосунки-виключення” і натиснути “Виявити” для того, щоб дозволити застосункам отримати доступ до мережі Інтернет (рис. 3.10).

5. Натиснути “Додати застосунок” і обрати “Обрати файл/процес/службу”. Цей пункт потрібен, якщо потрібно внести у виключення ті застосунки, які не були виявлені у п.4.

6. В статус-барі (справа знизу) натиснути правою кнопкою миші на іконку TinyWall та обрати підменю “Змінити режим” і навести на “Звичайний захист” (рис. 3.11).

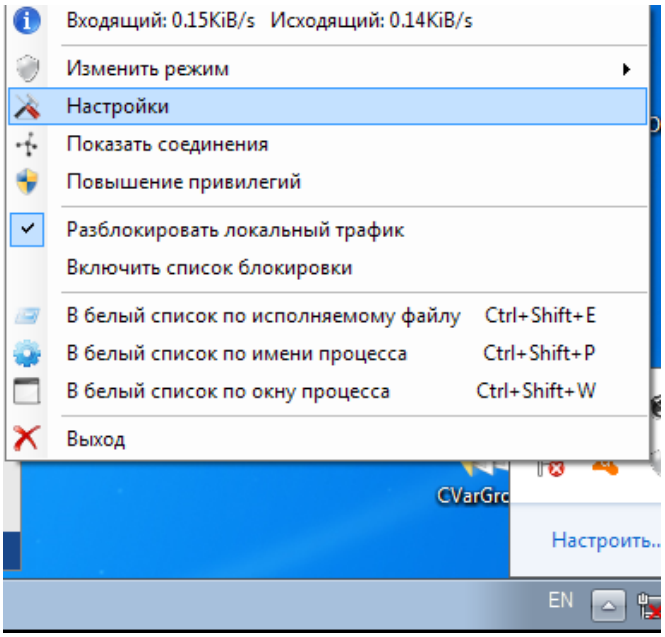


Рисунок 3.9 – Перехід у налаштування

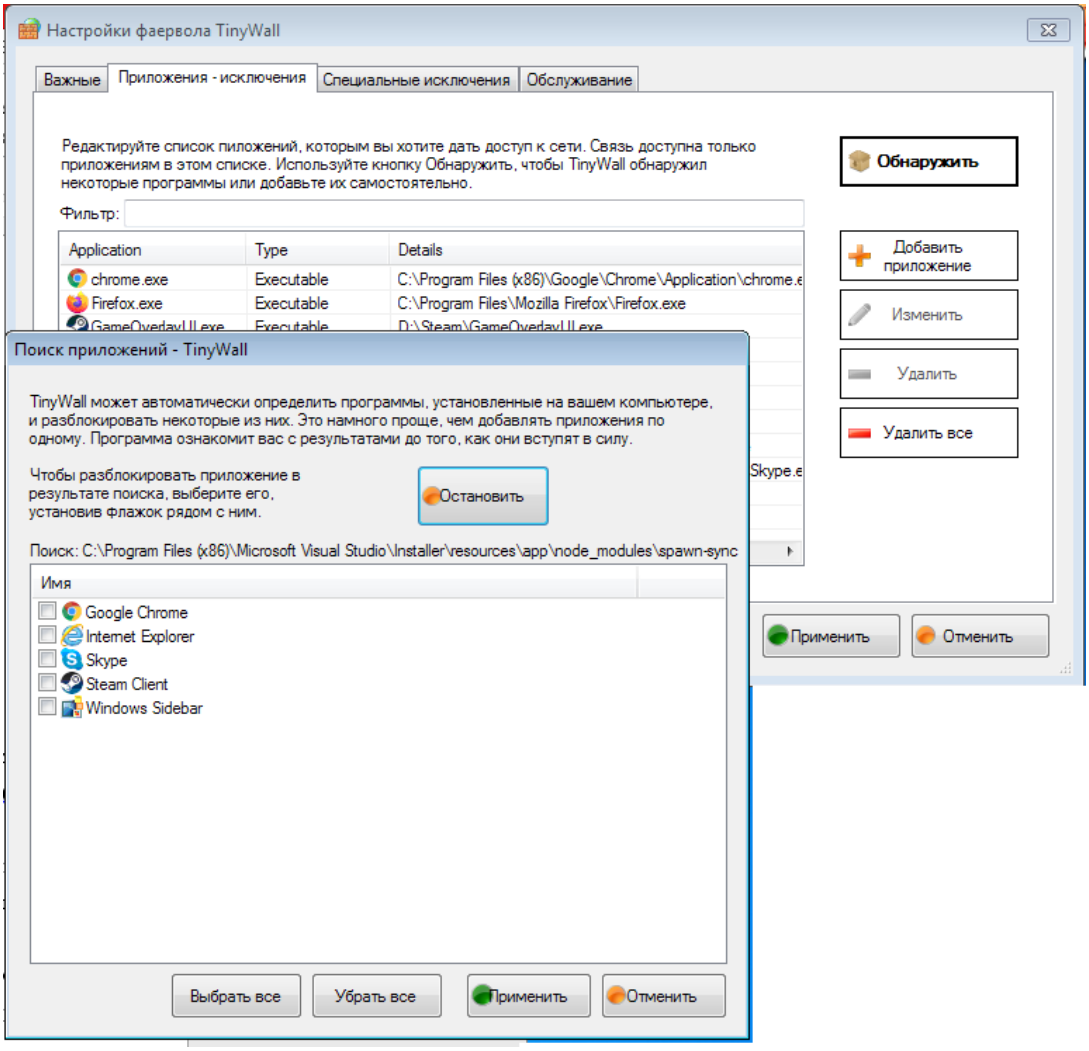


Рисунок 3.10 – Виявлення додатків

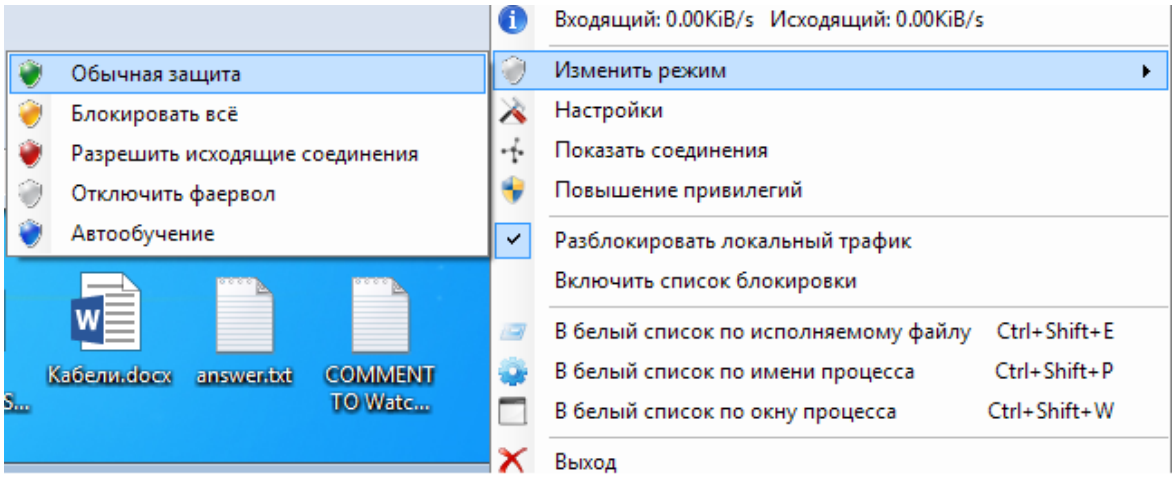


Рисунок 3.11 – Зміна режиму роботи

Налаштування Suricata

Налаштування IDS/IPS системи Suricata здійснюємо відповідно до наведеної інструкції [56].

– Завантажити та запустити файл Suricata-5.0.3-1-64bit.msi.

– Створити наступні каталоги:

· C:\Program Files (x86)\Suricata\log;

· C:\Program Files (x86)\Suricata\log\files;

· C:\Program Files (x86)\Suricata\log\certs;

· C:\Program Files (x86)\Suricata\rules;

– Скопіювати suricata.exe з папки C:\cygwin\tmp\oisf\src\.libs до C:\Program Files (x86)\Suricata.

– Скопіювати з C:\cygwin\bin наступні файли:

· cyggcc_s-1.dll;

· cygGeoIP-1.dll;

· cygluajit-5.1-2.dll;

· cygmagic-1.dll;

· cygnspr4.dll;

· cygnss3.dll;

· cygnssutil3.dll

· cygpcre-1.dll;

· cygplc4.dll ;

· cygplds4.dll;

· cygwin1.dll;

· cygz.dll у папку C:\Program Files (x86)\Suricata.

– Скопіювати файл C:\cygwin\usr\share\misc\magic.mgc в папку C:\Program Files (x86)\Suricata.

– Завантажити стандартні правила (Rules).

– Розпакувати архів за допомогою архіватора 7-Zip в папку C:\Suricata\rules.

– З папки C:\cygwin\tmp\oisf скопіювати:

· cygz.dll;

· classification.config;

· reference.config;

· suricata.yaml;

· classification.config;

· reference.config;

· suricata.yaml в папку C:\Program Files (x86)\Suricata.

– Внести наступні правки до файлу suricata.yaml у наступних місцях:

· Місце:

The default logging directory. Any log or output file will be
placed here if its not specified with a full path name. This can be
overridden with the -l command line parameter.
default-log-dir: C:\\Program Files (x86)\\Suricata\\log\\

· Місце:

Magic file. The extension .mgc is added to the value here.
#magic-file: /usr/share/file/magic
magic-file: C:\Program Files (x86)\Suricata\magic.mgc

· Місце:

outputs:

console: enabled: yes # type: json

file: enabled: yes

filename: C:\\Program Files (x86)\\Suricata\\log\\suricata.log

type: json

· Місце:

Set the default rule path here to search for the files.

if not set, it will look at the current working dir

default-rule-path: C:\\Program Files (x86)\\Suricata\\rules\\

rule-files:

· Місце:

classification-file: C:\Program Files (x86)\Suricata\classification.config

reference-config-file: C:\Program Files (x86)\Suricata\reference.config

· Місце:

vars:

Holds the address group vars that would be passed in a Signature.

These would be retrieved during the Signature address parsing stage.

address-groups:

HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]" (підставити відповідні значення адрес підмережі)

EXTERNAL_NET: "!$HOME_NET"

HTTP_SERVERS: "$HOME_NET"

SMTP_SERVERS: "$HOME_NET"

– Відкрити cmd.exe від імені Адміністратора, перейти в директорію C:\Program Files (x86)\Suricata та запустити команду “suricata.exe –build-info”.

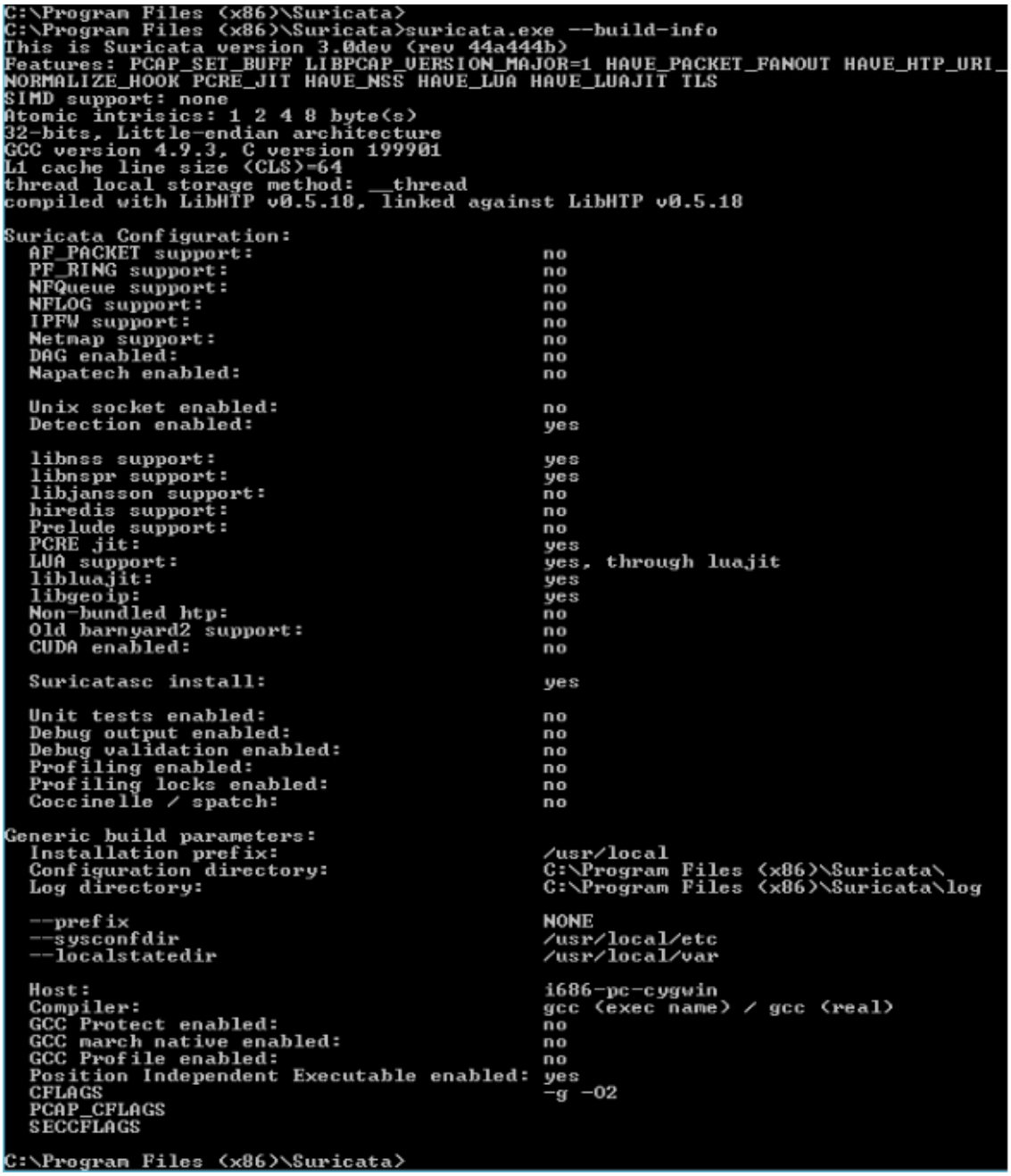


Рисунок 3.12 – Вивід команди “suricata.exe –build-info”

– Відкрити cmd.exe від імені Адміністратора, перейти в директорію C:\Program Files (x86)\Suricata та запустити команду “suricata.exe -c suricata.yaml -i X.X.X.X -v”, де “-i X.X.X.X” - адреса інтерфейсу(мережевої картки), який буде прослуховуватись IDS/IPS-системою.

Рисунок 3.13 – Вивід команди “suricata.exe -c suricata.yaml -i X.X.X.X -v”

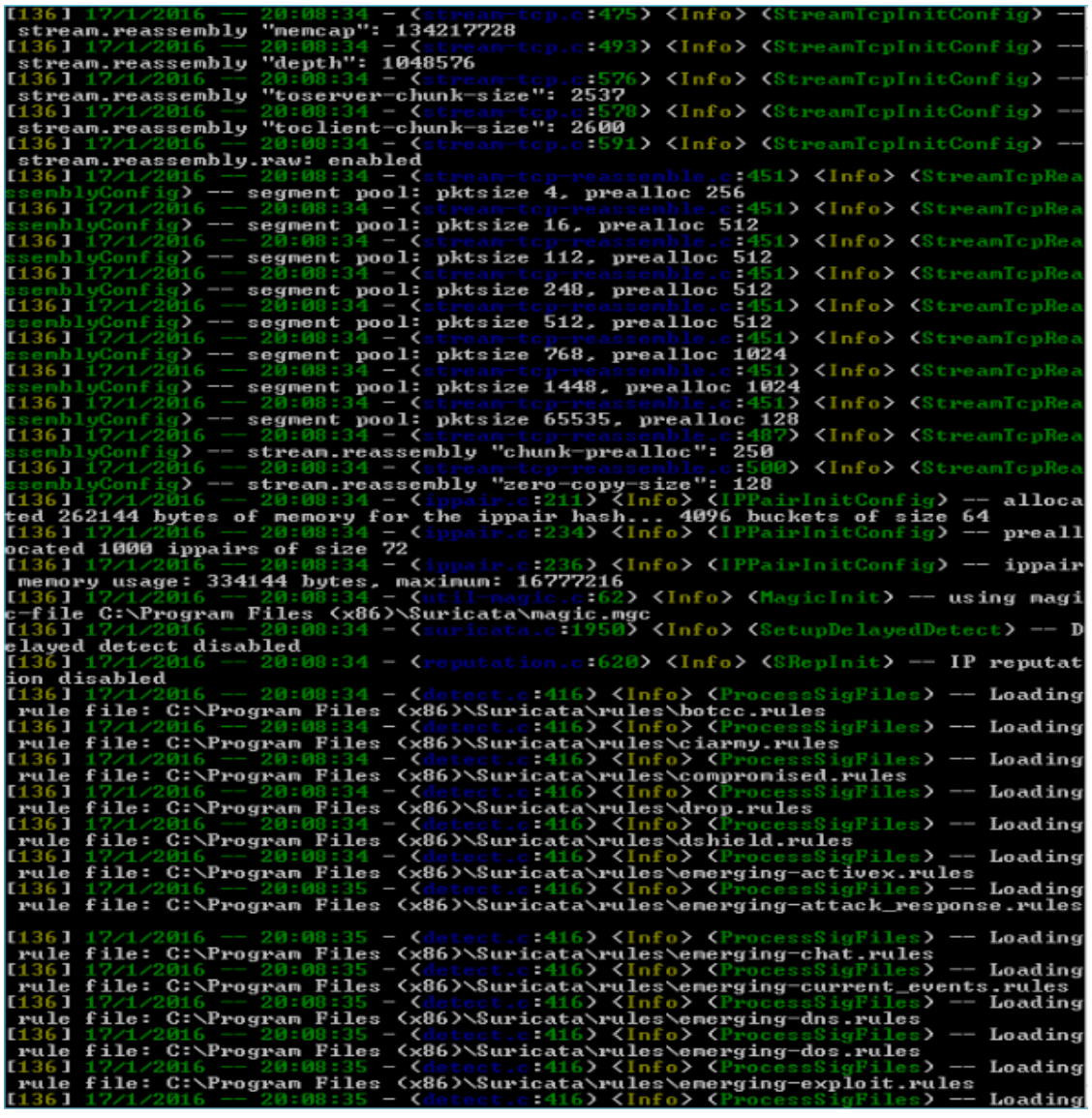


Рисунок 3.14 – Вивід команди “suricata.exe -c suricata.yaml -i X.X.X.X -v”

ВИСНОВКИ

Оскільки кібербезпека зосереджена на захисті комп’ютерних систем від несанкціонованого доступу або їх пошкодження чи іншому недоступі ресурсів системи в результаті впливу шкідливих чинників, існуючі системи дедалі частіше ризикують бути скомпрометованими, так як мають слабкий захист, або не мають його взагалі, то було прийняте рішення розробити модель кіберзахисту, яка надасть базовий рівень захисту для малого підприємства.

У роботі було проаналізовано поточний стан кібербезпеки на підприємствах за допомогою інтернет-ресурсів та були виділені потенційні загрози підприємству, що розглядається. Розглянуто існуючі моделі систем захисту та компоненти систем захисту, а саме – кібернетична, функціональна, структурна та організаційна моделі і компоненти систем захисту, такі, як системи прикладного, апаратного та мережевого рівнів; підсистемами яких є підсистеми моніторингу, антивірусного захисту, виявлення та запобігання втручань, міжмережевого екрану, системи розмежування доступу до інформації, ідентифікації та автентифікації, авторизації. Було розглянуто властивості систем захисту, їх принципи роботи та призначення.

На основі проаналізованих джерел проведена порівняльна характеристика та обрані програмні продукти для кожної з підсистем: Active Directory, Avast Free Antivirus, TinyWall, Wareshark, Suricata, які реалізують захисний функціонал. Також розроблено схему мережі з розташуванням кожного програмного продукту та практичну інструкції з їх встановлення та налаштування.

Розроблена модель кіберзахисту підприємства може бути реалізована на підприємствах, на яких відсутні захисні заходи прикладного, апаратного та мережевого рівнів. Також модель може бути доповнена апаратними засобами захисту, наприклад, апаратними IDS/IPS системами, системами розширеного моніторингу, антивірусного захисту, в залежності від фінансових можливостей підприємства.

СПИСОК ЛІТЕРАТУРИ

1. Исследование EY показало, что система кибербезопасности должна не только защищать организацию, но и стать ее конкурентным преимуществом [Електронний ресурс] // Ведомости. – 2018. – Режим доступу: https://www.vedomosti.ru/press_releases/2018/10/18/issledovanie-ey-pokazalo-chto-sistema-kiberbezopasnosti-dolzhna-ne-tolko-zaschischat-organizatsiyu-no-i-stat-ee-konkurentnim-preimuschestvom.

2. Кіберзащита для МСБ: как обезопасить вашу корпоративную сеть и не потратить деньги впустую [Електронний ресурс] // delo.UA. – 2019. – Режим доступу: https://delo.ua/special/kiberzaschita-dlja-msb-kak-obezopasit-vashu-korp-349691/.

3. Definition of Confidential Information [Електронний ресурс] // Law Insider – Режим доступу: https://www.lawinsider.com/dictionary/confidential-information?cursor=MTA%3D.

4. Закон України «Про доступ до публічної інформації», Стаття 9. Службова інформація [Електронний ресурс] // Протокол – Режим доступу: https://protocol.ua/ru/pro_dostup_do_publichnoi_informatsii_stattya_9/.

5. Сельченкова С. Діловодство Практичний посібник. / Сельченкова С. – К.: Інкунабула, 2009. – 480 с.

6. Цілісність інформації [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A6%D1%96%D0%BB%D1%96%D1%81%D0%BD%D1%96%D1%81%D1%82%D1%8C_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97.

7. Malware [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Malware.

8. Cisco Cybersecurity Essentials – розділ 1.2.1.1 [Електронний ресурс]. – Режим доступу: https://www.netacad.com/ .

9. Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

10. ТЗІ від НСД на прикладному і програмному рівні [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97.

11. Gentry S. Access Control: Models and Methods [Електронний ресурс] / Stuart Gentry. – 2018. – Режим доступу: https://resources.infosecinstitute.com/access-control-models-and-methods/#gref.

12. Carter S. RBAC vs ABAC Access Control Models - IAM Explained [Електронний ресурс] / S. Carter // Identity Automation – Режим доступу: https://blog.identityautomation.com/rbac-vs-abac-access-control-models-iam-explained.

13. Розмежування доступу [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D0%BC%D0%B5%D0%B6%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D1%83.

14. 16th National Computer Security Conference / David F. Frraiolo, Dennis M. Gilbert, Nickilyn Lynch // An examination of federal and commercial access control policy needs. – 1993.

15. Ролевое управление доступом (RBAC) [Електронний ресурс] // НОУ ИНТУИТ – Режим доступу: https://www.intuit.ru/studies/courses/73/73/lecture/2204?page=1.

16. Role-based access control [Електронний ресурс] // Wikipedia – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Role-based_access_control.

17. Управление доступом на основе ролей [Електронний ресурс] // Wikipedia – Режим доступу: https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B5_%D1%80%D0%BE%D0%BB%D0%B5%D0%B9.

18. Active Directory [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/Active_Directory.

19. Oracle Database [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Oracle_Database.

20. PostgreSQL [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/PostgreSQL.

21. Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов, обучающихся по специальностям 08050565, 21040665, 22050165, 23040165 / А.А. Гладких, В.Е. Дементьев. – Ульяновск: УлГТУ, 2009. – 156 с.

22. Переход на защищенные технологии идентификации [Електронний ресурс] // Techportal.ru – Режим доступу: http://www.techportal.ru/glossary/identifikatsiya.html.

23. RADIUS [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/RADIUS.

24. Diameter [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/Diameter.

25. LDAP [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/LDAP.

26. Monitoring [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Monitoring.

27. Network monitoring [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Network_monitoring.

28. System monitor [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/System_monitor.

29. Nagios [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Nagios.

30. Antivirus software [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Antivirus_software.

31. Business Security Test 2019 [Електронний ресурс] // AV Comparatives – Режим доступу: https://www.av-comparatives.org/tests/business-security-test-2019-august-november/.

32. ТЗІ на мережевому рівні [Електронний ресурс] // Wikipedia. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97.

33. Comparing Firewall Features [Електронний ресурс] // Techgenix – Режим доступу: http://techgenix.com/comparing_firewall_features/.

34. Bhardwaj R. Network Based Firewall vs Host Based Firewall [Електронний ресурс] / R. Bhardwaj // IPWITHEASE. – 2017. – Режим доступу: https://ipwithease.com/network-based-firewall-vs-host-based-firewall/.

35. Firewall (computing) [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Firewall_(computing).

36. Intrusion Detection System [Електронний ресурс] // GeekForGeeks – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/.

37. What is an Intrusion Prevention System (IPS)? [Електронний ресурс] // Forcepoint – Режим доступу: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips.

38. Юдин А. Самые популярные операционные системы [Електронний ресурс] / А. Юдин // Marketer. – 2017. – Режим доступу: https://marketer.ua/stats-operating-system-2017/.

39. PostgreSQL vs MySQL [Електронний ресурс] // 2ndQuadrant – Режим доступу: https://www.2ndquadrant.com/en/postgresql/postgresql-vs-mysql/.

40. 7 бесплатных программ для мониторинга сети и серверов [Електронний ресурс] // Networkguru.ru – Режим доступу: https://networkguru.ru/monitoring-seti-setevogo-oborudovaniia-serverov/.

41. Топ 10 лучших программ для мониторинга сети в 2019 [Електронний ресурс] // SoftintensiveLab – Режим доступу: https://www.softinventive.ru/best-network-monitoring-tools/.

42. Wireshark [Електронний ресурс] // Wikipedia – Режим доступу: https://en.wikipedia.org/wiki/Wireshark.

43. Рішення для захисту кінцевих точок компаній [Електронний ресурс] // Avast – Режим доступу: https://www.avast.ua/store#business-protection.

44. Top 10 BEST Free Firewall Software For Windows [Електронний ресурс] // Software Testing Help – Режим доступу: https://www.softwaretestinghelp.com/best-free-firewall/.

45. Метод експертних оцінок [Електронний ресурс] // Wikipedia – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%B5%D0%BA%D1%81%D0%BF%D0%B5%D1%80%D1%82%D0%BD%D0%B8%D1%85_%D0%BE%D1%86%D1%96%D0%BD%D0%BE%D0%BA.

46. What is SNORT [Електронний ресурс] // GeekForGeeks – Режим доступу: https://www.geeksforgeeks.org/what-is-snort/.

47. Active, directory, tree Free Icon [Електронний ресурс] // icons-icons.com – Режим доступу: https://icon-icons.com/icon/active-directory-tree/57383.

48. Avast Антивирус PNG фото [Електронний ресурс] // HOTPNG – Режим доступу: https://www.hotpng.com/search?q=avast+%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81.

49. Wireshark [Електронний ресурс] // icons-icons.com – Режим доступу: https://icon-icons.com/ru/%D0%B7%D0%BD%D0%B0%D1%87%D0%BE%D0%BA/%D0%BF%D0%BE%D0%BC%D0%BE%D1%89%D1%8C%D1%8E-wireshark/94067.

50. TinyWall Review [Електронний ресурс] // Slant – Режим доступу: https://www.slant.co/options/26943/~tinywall-review.

51. Suricata [Електронний ресурс] // Suricata – Режим доступу: https://suricata-ids.org/.

52. Иконки компьютер [Електронний ресурс] // Iconbird – Режим доступу: https://iconbird.com/search/?q=%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80.

53. Premium Stock Photo of Computer Icon [Електронний ресурс] // FreeImages – Режим доступу: https://www.freeimages.com/premium/computer-icon-844405

54. Ethernet switch icon, vector illustration - stock illustration [Електронний ресурс] // Depositphotos – Режим доступу: https://depositphotos.com/211031680/stock-illustration-ethernet-switch-icon-vector-illustration.html.

55. Internet Symbol free icon [Електронний ресурс] // flaticon – Режим доступу: https://www.flaticon.com/free-icon/internet-symbol_84517.

56. Windows Installation Guide forSuricata IDS/IPS/NSM [Електронний ресурс] // Suricata – Режим доступу:

https://redmine.openinfosecfoundation.org/attachments/download/1166/SuricataWinInstallationGuide_v1.4.2.pdf.

57. Установка Avast Free Antivirus [Електронний ресурс] // Avast – Режим доступу: https://support.avast.com/ru-ru/article/Install-Free-Antivirus.