МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_А.В. Ільєнко

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ р.

На правах рукопису

УДК 004.056.5:510.22(043.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема:** Автоматизованої система інформаційної безпеки підприємства

|  |  |
| --- | --- |
| **Автор:** | Є.О. Сидоров |
| **Науковий керівник:** к.т.н., доц. | А.В. Ільєнко |
| **Нормоконтролер:** асист. |  |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Сидорова Євгена Олександровича**

1. Тема: Автоматизована система інформаційної безпеки підприємства

затверджена наказом ректора від «02» жовтня 2019 № 2265/ст*.*

1. Термін виконання з 14.10.2019р. по 04.02.2020р*.*
2. Вихідні дані: проаналізувати існуючі системи та методики захиту, оцінки ризиків інформаційної безпеки; на основі аналізу виділити вхідні і вихідні параметри, завдяки яким можливо провести порівняння автоматизованих систем безпеки, виявлення їх переваг і недоліків; розробити методику, алгоритм та програмне забезпечення системи удосконалення захисту.
3. Зміст пояснювальної записки: аналіз існуючих систем та методик аналізу і оцінки ризиків інформаційної безпеки; розробка методики автоматизації безпеки; розробка програмного коду автоматизації налаштувань політики, верифікація отриманих результатів.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
|  | Уточнення постановки задачі | 14.10.2019 | *Виконано* |
|  | Аналіз літературних джерел | 18.10.2019 | *Виконано* |
|  | Обґрунтування вибору рішення | 30.10.2019 | *Виконано* |
|  | Збір інформації | 05.11.2019 | *Виконано* |
|  | Дослідження сучасних систем і методик аналізу та оцінки інформаційної безпеки | 20.11.2019 | *Виконано* |
|  | Розробка методики та структури системи автоматизацыъ інформаційної безпеки | 26.11.2019 | *Виконано* |
|  | Розробка методу та програмного коду автоматизації інформаційної безпеки | 10.12.2019 | *Виконано* |
|  | Апробація роботи на 15 науково практичній конференції | 19.12.2019 | *Виконано* |
|  | Перевірка на антиплагіат | 13.01.2020 | *Виконано* |
|  | Оформлення і друк пояснювальної записки | 20.01.2020 | *Виконано* |
|  | Оформлення презентації | 24.01.2020 | *Виконано* |
|  | Отримання рецензій від рецензента | 28.01.2020 | *Виконано* |
|  | Захист в ЕК | 04.02.2020 | *Виконано* |

Магістрант Є. Сидоров

(підпис, дата)

Науковий керівник А. Ільєнко

(підпис, дата)

**РЕФЕРАТ**

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 108 сторінок основного тексту, 50 рисунків, 4 таблиці, 5 сторінок додатків. Список використаних джерел містить 45 найменувань і займає 10 сторінок. Загальний обсяг роботи 108 сторінок.

Метою роботи є автоматизація системи інформаційної безпеки підприємства з інтеграцією спеціалізованого програмного забезпечення Fortinet та конфігурації API мовою програмування Python.

В роботі вирішено задачу побудови автоматизованої системи інформаційної безпеки за допомогою програмного коду Python.

В роботі розроблено алгоритм та програмний код для створення самостійної захищеної автоматизованої системи інформаційної безпеки, що удосконалює.

Розроблений метод та програмний код відносярозроться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності.

Можливі напрямки розвитку цієї роботи пов’язані з розвитком захисту інформації в умовах нових тенденцій та підходів, згідно з міжнародним законодавством та Українським.

Ключові слова: автоматизованість, система, інформаційна безпека, міжмережевий екран, політики безпеки, програмний код, загрози, вторгнення.

ЗМІСТ

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 7](#_Toc30434054)

[ВСТУП 8](#_Toc30434055)

[Розділ 1. СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 11](#_Toc30434056)

[1.1 Основні положення в сфері інформаційної безпеки 11](#_Toc30434057)

[1.2 Правові основи інформаційної безпеки України 12](#_Toc30434058)

[1.2.1 Закони України 13](#_Toc30434059)

[1.2.2. Міжнародні стандарти 15](#_Toc30434060)

[1.2.3. Концепції 17](#_Toc30434061)

[1.2.4. Державні стандарти 17](#_Toc30434062)

[1.2.5. Галузеві стандарти 17](#_Toc30434063)

[1.3. Сучасні напрями та методи захисту інформаційних ресурсів підприємства. 18](#_Toc30434064)

[1.4. Перспективні напрями організації інформаційної безпеки. 20](#_Toc30434065)

[1.5. Дослідження проблематики автоматизації систем інформаційної безпеки. 26](#_Toc30434066)

[1.6 Висновки по розділу 31](#_Toc30434067)

[Розділ 2. СУЧАСНІ НАПРЯМИ АВТОМАТИЗАЦІЇ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ 32](#_Toc30434068)

[2.1. Поняття та завдання мережевої інфраструктури 32](#_Toc30434069)

[2.2. Базові компоненти для створення мережевої інфраструктури 34](#_Toc30434070)

[2.3. Класифікація атак та уразливостей на інформаційні ресурси 35](#_Toc30434071)

[2.4. Безпека мережевої інфраструктури 39](#_Toc30434072)

[2.5. Програмне-апаратне забезпечення для побудови систем безпеки мереж 43](#_Toc30434073)

[2.5.1. Класифікація обладнання Fortinet 47](#_Toc30434074)

[2.5.2. Функціональні можливості ядра мережі Fortigate 49](#_Toc30434075)

[2.5.3. Класифікація рішень CheckPoint 52](#_Toc30434076)

[2.5.4. Функціональні можливості ядра мережі CheckPoint 57](#_Toc30434077)

[2.5.5. Конкурентний аналіз виробників 60](#_Toc30434078)

[2.6 Висновок до розділу 65](#_Toc30434079)

[Розділ 3.РЕАЛІЗАЦІЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА 67](#_Toc30434080)

[3.1. Характеристика та аналіз програмно-апаратних засобів для створення автоматизованої системи захищеної мережі. 67](#_Toc30434081)

[3.1.1 Характеристика міжмережевого екрана FGVM 69](#_Toc30434082)

[3.1.2 Характеристика комплекса захисту від загроз нульового дня 72](#_Toc30434083)

[3.1.3 Характеристика комплексу інтегрованого захисту від складних загроз 74](#_Toc30434084)

[3.1.4 Характеристика комплексу звітування та логування інформаційних інцидентів 75](#_Toc30434085)

[3.2 Встановлення та нлаштування віртуальних пристрорїв 76](#_Toc30434086)

[3.2. Налаштування інтеграції та автоматизації систем інформаційної безпеки 81](#_Toc30434087)

[3.2. Створення програмного коду автоматизації безпеки 87](#_Toc30434088)

[3.3. Оцінка ефективності та перспективи інтеграція 89](#_Toc30434089)

[3.4 Висновок до розділу 93](#_Toc30434090)

[ВИСНОВКИ 94](#_Toc30434091)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ 95](#_Toc30434094)

[Додаток А – Програмний код 101](#_Toc30434095)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ДСТУ – Державний Стандарт України

ЗУ – Закон України

КУ – Конституція України

НД – Нормативний Документ

ТЗІ – Технічний захист інформації

АС – Автоматизована Система

НСД – Несанкціонований доступ;

IPS- Intrusion prevention system - система запобігання вторгнень;

IDS- Intrusion detection system - система виявлення вторгнень;

IP- Internet Protocol - інтернет протокол;

DLP- Data Loss Prevention - запобігання витоку конфіденційної інформації;

SSH- Secure shell - захищений канал;

ОС- Операційна система;

NGFW- Next Generation Firewall – фаєрвол наступного покоління;

EVE – Emulated virtual environment – емульована віртальна середа;

VPN – Virtual private network – віртуальна приватна середа

SQL – Structured query language – мова структурованих запросів;

SUID – Set user ID upon execution – встановлення ID користувача під час виконання.

# ВСТУП

Актуальність**.** Сьогодення України характеризується зростанням бізнесу збільшується цінність комерційних відомостей, що зберігаються та обробляються в інформаційних системах організації. Керівній гілці, а також власникам інформаційних ресурсів варто частіше замислюватися про захист даних, адже в багатьох випадках фінансові втрати є наслідком проблем у сфері інформаційної безпеки.

Успіх виробничої і підприємницької діяльності залежить від уміння розпоряджатися таким найціннішим товаром, як інформація, але вигідно використовувати можна лише ту інформацію, яка потрібна ринку, але невідома йому. Тому в умовах конкуренції успіх підприємництва, гарантія отримання прибутку все більшою мірою залежать від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал і конкретну технологію.

Підприємницька (комерційна) діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і інтеграціям різноманітних інформаційних потоків. Однак захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємця. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями (властивостями), як корисність, своєчасність і достовірність надійшли відомостей.

Нажаль більша частка підприємств нехтують захищеністю або персоналом, що адмініструє системи захисту. Тому все більше випадків викрадення баз даних клієнтів, комерційних таємниць, модифікації АСУТП. Але треба зазначити, що вище описані дії – звонішні загрози, які займають друге місце перед внутршніми (інсайдерськими).

Дії ззовні можуть бути спрямовані на пасивні носії інформації і виражатися, наприклад, в наступному: спроби викрадення документів або зняття копій з документів, знімних носіїв (флеш-карти), зняття інформації, що виникає в тракті передачі в процесі комунікацій; знищення інформації або пошкодження її носіїв; випадкове або навмисне доведення до відома конкурентів документів або матеріалів, що містять комерційну таємницю.

Дії ззовні можуть бути також спрямовані на персонал компанії і виражатися у формі підкупу, погроз, шантажу, вивідування інформації, що становить комерційну таємницю, або припускати переманювання провідних спеціалістів на конкуруючу фірму тощо.

Новим трендом в захисті є інтегрованість і автоматизованість, але це складна задача, так як небагато систем мають відкритий API для інтеграції. Саме тому автоматизація системи безпеки на базі обладнання Fortinet з можливістю інтеграція програмування на мові Python є досить актуальною.

Мета роботи – автоматизація системи інформаційної безпеки підприємства з інтеграціям спеціалізованого програмного забезпечення Fortinet та конфігурації API мову програмування Python.

Виходячи з мети, завданням даної дипломної роботи є:

* дослідження та класифікація сучасних методів та напрямів автоматизації захисту мережевої інфраструктури;
* дослідження та порівняння спеціалізованого програмного забезпечення для реалізації автоматизованої системи інформаційної безпеки підприємства;
* розроблення програмного коду, що автоматизує впровадження налаштування політик захисту для всіх елемнтів системи на мові програмування Python;
* провести оцінку ефективності та обґрунтування впровадження даного підходу щодо автоматизації системи інформаційної безпеки підприємства.

Об’єктами дослідження являються прoцедурa та підходи автоматизації системи інформаційної безпеки підприємства.

Предметом дослідження є мережева інфраструктура та спеціалізоване програмне забезпечення.

Методи досліджень. Прoведені дoслідження бaзуються нa сучaсних метoдaх побудови захищених інформаційних мереж.

Наукова новизна. Удосконалено автоматизовану системи інформаційної безпеки підприємства, на базі спеціалізованого програмного забезпечення Fortinet та конфігурації API мовою програмування Python, що робить систему захищеною від зовнішніх та внутрішніх загроз.

Практична значимість роботи полягає у конфігуруванні власних політик безпеки спеціалізованого програмного забезпечення Fortinet для всіх систем, які приймають участь у протидії несанкціонованому доступу мовою програмування Python та побудови результуючої захищеної, автоматизованої мережевої інфраструктури підприємства

Апробація отриманих результатів:

1. Сидоров Є.О. Дослідження проблематики автоматизації систем інформаційної безпеки / А.В. Ільєнко, Є.О. Сидоров // «SCIENTIFIC HORIZONS - 2019»: XVI международна научна практична конференция, 30.09 – 07.10 2019 г.: тези доп. – V.15. – Шефилд, 2019. – С. 56-57.

# Розділ 1. СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

# 1.1 Основні положення в сфері інформаційної безпеки

Світові процеси глобалізації, впровадження новітніх інформаційних технологій, формування інформаційного суспільства посилюють важливість такої складової національної безпеки, як інформаційна безпека. Вже найближчим часом саме розвиток інформаційної сфери, рівень інформаційної безпеки будуть визначати політичну й економічну роль окремих держав на світовій арені. Проблем інформаційної безпеки безліч, як і проблем розвитку процесу інформатизації. У цій сфері необхідно вирішувати питання, пов'язані з визначенням природи різних видів інформаційних небезпек, механізмів їхнього впливу на об'єкти інформаційної безпеки, можливих наслідків цих впливів, шляхів і методів їх нейтралізації або зменшення.

Поняття інформаційної безпеки можна разглядати у декількох ракурсах. По-перше, це стан захищенності інформаційного середовища суспільства, який забезпечує його формування, інтеграція й розвиток в інтересах громадян, організацій, держави. По друге, інформаційна безпека – це стан захищенності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і як наслідок – обгрунтованість рішень і дій, що приймаються. Правова форма інформаційної безпеки – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Об’єктами інформаційної безпеки можуть бути: свідомість, психіка людини; інформаційні системи різного масштабу й різного призначення. До соціальних об’єктів інформаційної безпеки відносять особистість, колектив, державу, суспільство, світове товариство. До суб’єктів інформаційної безпеки належать: держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і об’єднання, що володіють повноваженнями щодо забезпечення інформаційної безпеки відповідно до законодавства.

Виділяють 2 основні види інформаційної безпеки:

1) Інформаційна безпека особистості – це захищенність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.

2) Інформаційна безпека держави характеризується мірою захищенності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обгрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки.

1.2 Правові основи інформаційної безпеки України

Питання забезпечення інформаційної безпеки сьогодні для України стоять на одному рівні із захистом суверенітету і територіальної цілісності, забезпеченням її економічної безпеки. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз - це нанесення шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

У Конституції України ***стаття 17*** ставить інформаційну безпеку до ряду найважливіших функцій держави, таких як захист суверенітету і територіальної цілісності України. Питанню забезпечення інформаційної безпеки у 2006 році було присвячене одне із засідань Ради національної безпеки та оборони України, результатом якого стали змістовні рекомендації та завдання для галузевих міністерств та відомств з приводу вживання усіх необхідних заходів для забезпечення інформаційної безпеки України, зокрема прискорення розробки та впровадження відповідних нормативно-правових актів.

На сьогодні в Україні правовий порядок забезпечення інформаційної безпеки взагалі, і ТЗІ зокрема, визначається документами, які належать до таких категорій:

### 1.2.1 Закони України

* Закон "Про інформацію" №2657 від 2.10.199. Виступаючи ідеологічною основою для всіх подальших документів у сфері захисту інформації, формулює поняття інформації, основні напрями державної інформаційної політики, визначає основних суб'єктів інформаційних відносин (до яких належить і держава), розкриває поняття, основні напрями і види інформаційної діяльності тощо. Грунтуючись на Декларацiї про державний суверенiтет України та Актi проголошення її незалежностi, Закон стверджує iнформацiйний суверенiтет України i визначає правовi форми мiжнародного спiвробiтництва в галузi iнформацiї. Закон встановлює загальнi правовi основи одержання, інтеграція, поширення та зберiгання iнформацiї, закрiплює право особи на iнформацiю в усiх сферах суспiльного i державного життя України, а також систему iнформацiї, її джерела, визначає статус учасникiв iнформацiйних вiдносин, регулює доступ до iнформацiї та забезпечує її охорону, захищає особу та суспiльство вiд неправдивої iнформацiї. Дiя цього Закону поширюється на iнформацiйнi вiдносини, якi виникають у всiх сферах життя i дiяльностi суспiльства i держави при одержаннi, використаннi, поширеннi та зберiганнi iнформацiї.[2]

Закон " Про основні засади забезпечення кібербезпеки України" №45 від 05.10.2017. Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.[3]

Закон «Про державну таємницю» №3855-12 від 21.01.1994 р. Закон конкретно визначає інформацію, що є державною таємницею, та класифікує її за ступенем секретності, якому відповідає певний режим доступу. Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.[4]

Закон України «Про захист інформації в автоматизованих системах» 1994 р.Метою цього Закону є регулювання правових відносин в сфері захисту інформації в автоматизованих системах, визначає умови та права власності громадян України і юридичних осіб на інформацію, умови та права доступу до інформації, що обробляється в автоматизованій системі, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації. Дія Закону поширюється на будь-яку інформацію, що обробляється в автоматизованих системах.[5]

Закон України «Про захист інформації в інформаційно - телекомунікаційних системах». Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, визначає правила доступу та користування конфіденційною інформацією, що функціонує в системі, права власника на захист цієї інформації, основні принципи, методи та засоби забезпечення безпеки інформації тощо.

Закон України «Про науково-технічну інформацію» від 25.06.93. Цей Закон визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни. Метою Закону є створення в Україні правової бази для одержання та інтеграція науково-технічної інформації.Законом регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі. Дія Закону поширюється на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, інтеграція та поширення науково-технічної інформації. Дія Закону не поширюється на інформацію, що містить державну та іншу охоронювану законом таємницю.[5]

### 1.2.2. Міжнародні стандарти

***ISO/IEC 17799.*** Стандарт призначений для інтеграція будь-якою організацією, котра планує встановити систему ефективного інформаційного захисту або покращувати існуючі методи інформаційного захисту. Однак, це не свідчить, що всі рекомендації стандарту повинні бути обов’язково прийняті. Все залежить від конкретних місцевих інформаційних ризиків та вимог.[15]

***ISO/IES 27001.*** Міжнародний стандарт по інформаційної безпеки розроблений спільно Міжнародною Організацією по Стандартизації (ISO) і Міжнародної електротехнічної комісією (IEC). Підготовлено до випуску підкомітетом SC27 Об’єднаного технічного комітету JTC 1.Стандарт містить вимоги в області інформаційної безпеки для створення, розвитку і підтримки. Системи менеджменту інформаційної безпеки. Кращі світові практики в галузі управління інформаційною безпекою описані в міжнародному стандарті на системи менеджменту інформаційної безпеки ISO / IEC 27001 (ISO 27001). ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки (СМІБ) для демонстрації здатності організації захищати свої інформаційні ресурси. Поняття “захисту інформації” трактується міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації. Основа стандарту ІСО 27001 – система управління ризиками, пов’язаними з інформацією. Система управління ризиками дозволяє отримувати відповіді на наступні питання: – На якому напрямку інформаційної безпеки потрібно зосередити увагу? – Скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації. [16]

***ISO/IES 15408.*** Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій» (англ. Common Criteria for Information Technology Security Evaluation) описує інфраструктуру (Framework) в якій користувачі комп’ютерної системи можуть описати вимоги, розробники можуть заявити про властивості безпеки продуктів, а експерти з безпеки визначити, чи задовольняє продукт заявам. Таким чином цей стандарт дозволяє бути впевненим, що процес опису, розробки та перевірки продукту був проведений в строгому порядку. Прообразом даного документа послужили «Критерії оцінки безпеки інформаційних технологій» (англ. Evaluation Criteria for IT Security, ECITS), робота над якими почалася в 1990 році. Стандарт містить два основних види вимог безпеки: функціональні, що висуваються до функцій безпеки і реалізує їх механізмів, і вимоги довіри, які пред’являються до технології та процесу розробки та експлуатації. [17]

### 1.2.3. Концепції

Концепція національної безпеки України схвалена Постановою ВР України N3/97-ВР від 16 січня 1997 р. Концепція національної безпеки України забезпечує єдність принципів формування і проведення державної політики національної безпеки, поєднання підходів до формування відповідної законодавчої бази, підготовки доктрин, стратегій, концепцій, державних і відомчих програм у різних сферах національної безпеки. Державна політика національної безпеки визначається виходячи з пріоритетності національних інтересів та загроз національній безпеці України і здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм у різних сферах національної безпеки відповідно до чинного законодавства.

Концепція інформаційної безпеки України. Концепція є основою для формування політики в галузі забезпечення інформаційної безпеки України, підготовки пропозицій щодо удосконалення правового, методичного, науково-технічного та організаційного забезпечення інформаційної безпеки України, розробки цільових програм забезпечення інформаційної безпеки України. Вона розвиває Концепцію національної безпеки України стосовно інформаційної сфери.

### 1.2.4. Державні стандарти

* ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.[6]
* ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. [7]
* ДСТУ 3396.2-96 Захист інформації. Технічний захист інформації . Терміни та визначення. [7]

### 1.2.5. Галузеві стандарти

* НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;[8]
* НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу; [9]
* НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікація гарантій захисту;[10]
* НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу;[11]
* НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.[12]

## 1.3. Сучасні напрями та методи захисту інформаційних ресурсів підприємства.

На сьогоднішній день сучасним напрямом захисту інфраструктури підприємства є створення корпоративної політики безпеки, що включає багато заходів, методів, технологій та засобів забезпечення інформаційної безпеки.

**Політика, зокрема, має включати:**

* Стратегію захисту ІТ-інфраструктури організації.
* Набір правил, за якими створюється, обробляється та зберігається інформація на підприємстві.
* Правила своєчасного оновлення ПЗ та відповідальність працівників.
* Резервне копіювання та відновлення даних. Необхідно регулярно створювати резервні копії бізнес-систем та критично важливих даних. Резервні копії мають зберігатися на окремих носіях інформації, які фізично відокремлені від цільових систем. Цілісність та повнота резервних копій повинна регулярно перевірятись шляхом штатного відновлення.
* План дій з локалізації, блокування розповсюдження, та відновлення після атак.

**Запровадження правил інтеграція облікових записів в організації, що включають:**

* Персоніфікований адміністративний доступ. Заборона інтеграція спільних адміністративних облікових записів.
* Інтеграція різних облікових записів для виконання різних адміністративних задач:
  + для адміністрування домену;
  + для адміністрування серверів (різні записи для різних функцій);
  + для адміністрування ПК користувачів;
  + для адміністрування власного ПК.
* Заборона здійснювати регулярні задачі з інтеграція адміністративних облікових записів.
  + Адміністратори повинні працювати на своїх ПК під стандартними обліковими записами з правами рівня звичайного користувача.
  + Робота з адміністрування інформаційних систем повинна здійснюватися з окремого виділеного термінального сервера управління (або спеціалізованих систем PAM), а не безпосередньо з призначеного для користувача ПК.
  + Інтеграція адміністратором для певних робіт відповідного облікового запису має суворо контролюватися.
  + Заборона інтеграція облікових записів адміністраторів домену для задач, що не пов’язані з адмініструванням контролерів доменів.
* Гранулярна деталізація прав доступу сервісних облікових записів. Облікові записи для функціонування різноманітних служб та ПЗ повинні мати мінімально необхідний рівень прав, достатній для роботи конкретного сервісу. Дотримання принципу максимально повної персоніфікації: кожне ПЗ має використовувати окремий обліковий запис.

**Регулярне навчання всіх користувачів організації основам інформаційної безпеки, що включає:**

* донесення правил роботи з критичними системами організації,
* донесення правил роботи з інформацією, що надходить з зовнішніх, неперевірених джерел,
* проведення регулярного зрізу знань для контролю засвоєння інформації.

**Регулярне навчання і підвищення кваліфікації ІТ-фахівців та адміністраторів** в області сучасних загроз і методів захисту на системах та рішеннях, що експлуатуються в організації.

**Проведення тестових атак,**в тому числі, з інтеграціям методів «соціальної інженерії», для перевірки обізнаності користувачів правил безпеки організації та рівні захищеності інформаційних систем.

## 1.4. Перспективні напрями організації інформаційної безпеки.

**Перспективність організаційї інформаційної безпеки полягає у дотриманні сучасних міжнародних заходів від лідерів в галузі. До таких заходів належать:**

**Апаратні заходи. Інтеграція контролю периметру корпоративної мережі, що включає:**

* Інтеграція **мережевих екранів** з функціями контролю на прикладному рівні (Application Visibility) та протидії вторгненням (IPS) – Next Generation Firewall (NGFW). Обов’язкове розташування публічних сервісів в окремих демілітаризованих зонах (ДМЗ). Налаштування конкретизованих правил доступу по контролю потоків даних та відмова від Інтеграція загальних сутностей типу «any», «all».
* Іінтеграція **шлюзу безпеки** (проксі сервісу) для контролю доступу користувачів організації до мережі Інтернет. Налаштування блокування доступу до ресурсів із забороненою тематикою, поганою репутацією, високим рівнем ризику, фішингових ресурсів. Виконання антивірусної перевірки та контентної фільтрації файлів, що завантажуються. Блокування завантаження виконуваних файлів для загальної групи користувачів. Налаштування повної інспекції SSL для виявлення загроз у шифрованому трафіку. Заборона інтеграція безумовних білих списків доступу до зовнішніх ресурсів та білих списків внутрішніх систем в обхід правил контентної перевірки.
* Інтеграція **поштового шлюзу безпеки** для захисту корпоративної пошти від спаму та зовнішніх загроз. Налаштування для вхідних листів антивірусної перевірки та правил фільтрації контенту за типом файлу та розширенням. Блокування листа або видалення вкладення з виконуваними типами файлів та офісних документів з макросами. Перевірка URL-посилань в тексті листів та у вкладенні щодо належності до небезпечних та заборонених ресурсів, високого рівня ризику та фішингу. Заборона інтеграція безумовних білих списків для зовнішніх та внутрішніх відправників в обхід систем контентної перевірки.
* Передавання інформаційних пакетів між майданчиками організації та при віддаленому доступі користувачів через WAN та Інтернет-канали зв’язку повинна здійснюватися лише**за допомогою VPN-технологій** з інтеграціям належного рівня шифрування (AES-256 та вище).
* Аналіз та контроль доступу зовнішніх партнерів та підрядників до ресурсів організації. Доступ необхідно надавати лише через захищене VPN з’єднання (AES-256 та вище) з інтеграціям проміжного термінального серверу (Jump Host) та обов’язковим моніторингом і фіксацією виконаних дій.

**Контроль локальної мережі:**

* Налаштування**сегментації локальної мережі** згідно функціонального призначення. Розділення серверних сегментів мереж в залежності від сервісів. Заборона створення сегментів з великою кількістю систем. Виконання мікросегментації для мережевого відділення особливо критичних систем та сервісів.
* Налаштування **технологій ізоляції портів** (Port Isolation/Private VLAN) на комутаторах доступу користувачів для заборони прямої взаємодії між користувацькими системами.
* Налаштування**технологій протидії атакам** типу ARP Spoofing та фальшивих DHCP-серверів (ARP Inspection, DHCP Snooping) для унеможливлення перехоплення трафіку.
* Блокування будь-якої **прямої мережевої взаємодії** між промисловою (АСУТП, АТМ тощо) та корпоративною мережами. Зв’язок між сегментами здійснювати тільки через проксі-сервіси, розташовані в демілітаризованих зонах на стику мереж. Трафік між ДМЗ та промисловою і ДМЗ та корпоративною мережами контролювати за допомогою мережевих екранів.

**1. Підвищення захищеності систем (System Hardening), що експлуатуються в організації (мережевих пристроїв, серверних та користувацьких систем) для “зменшення поверхні” можливої атаки:**

* Видалення та відключення зайвих компонентів та служб, що не використовуються й не потрібні у робочому процесі.
* Деактивація та блокування роботи застарілих протоколів (NTLM, SMBv1 тощо).
* Впровадження механізмів та заходів для протидії отримання паролів з оперативної пам’яті та системних процесів (Mimikatz): інтеграція Protected Users Group, деактивація WDigest тощо.
* Заборона створення локальних облікових записів або зміни їх паролів доменними політиками, оскільки інформація про цей обліковий запис та його пароль легкодоступні всім користувачам мережі.

**2.Регулярне оновлення системного та прикладного ПЗ (Patch Management).** Необхідно забезпечити своєчасне тестування і оперативне встановлення оновлень безпеки для системного й прикладного програмного забезпечення з урахуванням рівня критичності та пріоритетів.

**3. Вимкнення та блокування механізму автоматичного визначення проксі-серверів WPAD та протоколу широкомовного розпізнавання імен LLMNR.**

**4. По можливості відмовитись від інтеграція мережевих дисків та надавати віддалені файлові ресурси у вигляді ярликів.**

**5. Наявність встановленого актуального антивірусного програмного забезпечення на серверних та користувацьких системах організації.**Регулярне оновлення антивірусних компонентів та баз даних сигнатур. Заборона можливості рядовим користувачам локально змінювати конфігурацію антивірусного ПЗ та вимикати модулі захисту.

**6. Наявність на системах організації встановленого рішення Host IPS з активованим функціоналом:**

* мережевого екрану з налаштованими мінімально необхідними для роботи дозвільними правилами;
* сигнатурного захисту від атак, як на мережевому рівні, так і в рамках самої системи;
* обмеження запуску та виконання програм з недовірених директорій (наприклад, тимчасових директорій %tmp% та директорій з налаштуваннями програм %appdata%);
* блокування втручання невідомих процесів у роботу та системну пам’ять інших;
* поведінковий аналіз дій програмного забезпечення та процесів і блокування у випадку підозрілої активності;
* блокування дочірніх процесів, які породжують офісні документи.

**7. Наявність функціоналу контролю запуску додатків та програм (Application Control), що включає можливість:**

* створення списків дозволеного програмного забезпечення на робочій станції;
* перевірку репутації виконуваних файлів у хмарі;
* контроль здійснення оновлення тільки перевіреними програмами, з довірених джерел, авторизованими користувачами.

**8. Наявність рішення для контролю підключення периферійних пристроїв та зйомних носіїв до робочих станцій організації.** Налаштування правил для дозволу підключення тільки перевірених корпоративних носіїв.

**9. Наявність рішення для швидкої перевірки корпоративних систем за заданим індикатором** (наявність файлів, гілок реєстру, запущених процесів) та можливості виконання дій (створення/копіювання/видалення файлів, запуск/завершення процесів, тощо).

До додаткових заходів належать:

**1. Наявність впровадженого рішення 802.1x та Network Access Control (NAC)**для унеможливлення несанкціонованого підключення сторонніх пристроїв у корпоративну мережу та забезпечення надання лише необхідного мережевого доступу в залежності від функціональних обов’язків користувача та стану пристрою. Рішення повинно забезпечити:

* Контроль пристроїв, що підключаються в корпоративну мережу. Блокування сторонніх пристроїв.
* Гранульований доступ у мережу за результатами авторизації (політика доступу в залежності від користувача, часу, способу, місця підключення і типу пристрою).
* Можливість реалізувати попередню перевірку пристроїв на відповідність перед підключенням до корпоративної мережі (NAC): наявність встановленого антивірусу та інших продуктів, актуальність останніх оновлень.
* Автоматизований карантин за індикатором компрометації. У разі компрометації будь-якого з хостів у корпоративній мережі для локалізації та запобігання розповсюдженню вірусної епідемії необхідно забезпечити автоматизоване відключення вузла від мережі або переведення його на карантин з блокуванням усіх мережевих з’єднань.

**2. Наявність спеціалізованого засобу “Пісочниці” (Sandbox)**для статичного (аналіз коду) та динамічного (запуск в тестовому середовищі) аналізу невідомих файлів на предмет виявлення їхніх шкідливих дій. Для підвищення ефективності антивірусного захисту у протидії атакам типу “Zero-Day” рішення Sandbox необхідно інтегрувати з максимальною кількістю систем захисту: мережевими екранами веб- та поштовими шлюзами, засобами захисту на кінцевих системах. Також системи цього класу можуть використовуватись адміністраторами, як додатковий інструмент у дослідженні загроз.

**3. Інтеграція системи контролю дій привілейованих користувачів – Privilege Access Management (PAM).**Надання доступу до критичних систем тільки за допомогою рішення, забезпечуючи:

* збір, запис та аналіз активності привілейованих користувачів;
* детектування ризикованих дій до того, як це призведе до шкідливих наслідків;
* можливість взаємодії з користувачем, який виконує ризиковані операції, та блокування його сесії.

**4. Наявність системи моніторингу та профілювання мережевих потоків (Network Behavior Analysis, NBA)**для визначення штатного профілю трафіку організації та виявлення відхилень від “нормальної” поведінки. Налаштування збору інформації про трафік з усіх ключових мережевих пристроїв організації для повноти видимості та аналізу потоків даних.

**5. Наявність спеціалізованого рішення Vulnerability Assessment (VA)**для регулярного сканування всіх елементів корпоративної інфраструктури на предмет виявлення відомих вразливостей в операційних системах та ПЗ. Забезпечення можливості оперативного усунення виявлених загроз та виконання інтеграції з системами мережевої безпеки й аналітики для ізоляції або фільтрування доступу до вузлів з критичними вразливостями.

**6. Інтеграція системи централізованого збору, аналізу та кореляції подій безпеки (SIEM)**для всебічного комплексного аналізу стану корпоративної інфраструктури, що забезпечує:

* Збір журнальної інформації та подій з усіх систем підприємства. Приведення отриманих подій до єдиного вигляду (нормалізація) та агрегація даних.
* Створення екранів та звітів для відображення стану ІТ-інфраструктури.
* Створення правил кореляції для виявлення пов’язаних подій, що можуть свідчити про атаки та спроби компрометації в ІТ-інфраструктурі організації.
* Створення правил кореляції на основі ризиків для виявлення та виділення небезпечних дій та подій, що відбуваються на критичних системах.
* Аналіз історичних даних для створення нових правил кореляції.
* Налаштування правил для автоматичної реакції на виявлені події з метою у максимально короткий термін блокувати та припинити поширення загроз.

### 1.5. Дослідження проблематики автоматизації систем інформаційної безпеки.

На сьогоднішній день інформаційні технології використовуються для втручання в діяльність як підприємств так режимних об’єктів інформації. Загалом основним напрямком дій зловмисників у кіберпросторі є блокування серверів та ресурсів за допомогою DDoS – атак та комп’ютерних атак, метою яких є:

1. Виведення з ладу комунікаційних мереж та систем зв’язку за допомогою вірусів.

2. Блокування веб-сайтів за допомогою спамів.

3. Розміщення повідомлень дискретизаційного спрямування на офіційних веб-сайтах державних установ та комерційних організацій.

4. Викрадення даних.

Тому комерційні підприємства все частіше розпочинають свою діяльність із атестації об’єктів інформації, що є необхідним для розуміння рівня надійності системи автоматизованого захисту інформації підприємства. За поняття захищеності систем автоматизованого захисту інформації ми приймаємо рівень механізмів захисту відносно ризиків відповідно існуючим загрозам. Є велика кількість загроз системам автоматизованого захисту, якими можуть скористатись інсайдери. Відповідно є декілька факторів. Що визначають рівень автоматизованого захисту:

1. Кожен можливий шлях загрози інформації має бути перекритий відповідним механізмом захисту;

2. Стійкість механізмів захисту, що характеризується рівнем супротиву можливим реалізаціям загроз;

3. Розмір втрат, що можуть спричинити можливі реалізації загроз.

Також наступними характеристиками систем автоматизованого захисту є:

1. Ефективність автоматизованої системи захисту інформації – це рівень відповідності результатів автоматизованого захисту необхідній меті;

2. Показник ефективності автоматизованої системи захисту інформації – це характеристика для оцінки автоматизованої системи захисту;

3. Норми ефективності автоматизованої системи захисту інформації – це значення показників ефективності автоматизованої системи захисту інформації, визначені нормативними документами;

4. Категорії інформації, що захищається – визначення градації важливості інформації, що захищається;

5. Контроль стану автоматизованої системи захисту – це перевірка відповідності організації та ефективності автоматизованої системи захисту інформації встановленим вимогам та нормам;

6. Метод контролю стану ефективності автоматизованої системи захисту – це порядок та правила застосування принципів та засобів автоматизованого захисту;

7. Засоби контролю автоматизованої системи захисту – це технічний або програмний засіб для контролю ефективності автоматизованої системи захисту інформації;

8. Контроль ефективності автоматизованої системи захисту інформації – це перевірка відповідності ефективності автоматизованої системи захисту інформації існуючим вимогам та нормам ефективності захисту інформації;

9. Контроль проведення автоматизованого захисту інформації – це перевірка відповідності стану організації проведення автоматизованого захисту інформації, наявності та змісту документів вимогам правових, організаційно – розпорядних та нормативних документів із захисту інформації;

10. Організаційний контроль ефективності автоматизованого захисту інформації – це перевірка повноти та необхідності заходів автоматизованої системи захисту вимогам нормативних документів із захисту інформації;

11. Технічний контроль ефективності автоматизованого захисту інформації – це контроль ефективності автоматизованої системи захисту інформації, що реалізується шляхом застосування засобів контролю.

Для визначення рівня захищеності систем автоматичного захисту інформації необхідно застосувати наступні методи:

1. Вивчення вхідних даних автоматичної системи захисту інформації;

2. Оцінка ризиків від можливої реалізації загроз системи автоматизованого захисту інформації.

3. Аналіз технологій безпеки організаційного рівня, політики безпеки підприємства, забезпечення режиму інформаційної безпеки та оцінки їх відповідності вимогам існуючим нормативним документам.

4. Аналіз конфігураційних файлів маршрутизаторів, проксісерверів, що виконують роботу із взаємодії, поштових та DNS серверів та інших критичних елементів мережевої інфраструктури.

5. Сканування зовнішніх мережевих адрес ліній зв’язку з мережі інтернет.

6. Сканування ліній зв’язку.

7. Аналіз конфігурації серверів та робочих станцій ліній зв’язку за допомогою спеціалізованих програмних агентів.

Під час реалізації вищезазначеного аналізу використовуються як активні, так і пасивні методи тестування системи автоматизованого захисту. Активне тестування системи автоматичного захисту інформації – це імітація дій потенційного зловмисника під час атаки системи захисту. Пасивне тестування системи автоматизованого захисту інформації – це аналіз конфігурації операційної системи та додатків за стандартами з інтеграціям списків перевірки. Тестування виконується за інтеграція програмних засобів або власноруч. Для проведення аналізу необхідно мати наступні дані:

1. Повна назва об’єкту інформації та призначення.

2. Характер діяльності (науково – технічна, економічна, політична, виробнича, фінансова, військова) та рівень секретності інформації.

3. Організаційна структура об’єкта інформації.

4. Склад приміщень технічного комплексу об’єкта інформації, в яких виконується обробка інформації.

5. Особливості розташування об’єкта інформації, враховуючи межі контрольованої зони.

6. Структура використовуваного на об’єкті інформації програмного забезпечення для обробки інформації, що захищається.

7. Протоколи обміну інформацією, що захищається.

8. Загальна схема функціонування об’єкта інформації, що захищається (протоколи та режими обробки інформації).

9. Зв’язки та характер взаємодії з іншими об’єктами.

10. Склад та структура функціонування системи захисту інформації на об’єкті. 11. Перелік технічних та програмних засобів захисту й контролю на об’єкті інформації із відповідними сертифікатами та приписами до експлуатації.

12. Відомості про розробників системи автоматизованого захисту інформації. 13. Наявність служби безпеки на об’єкті інформації та служби адміністрування (автоматизованої системи, мережі, баз даних).

14. Наявніть та основні характеристики фізичного захисту об’єкта інформації. 15. Наявність та готовність проектної та експлуатаційної документації на об’єкті інформації.

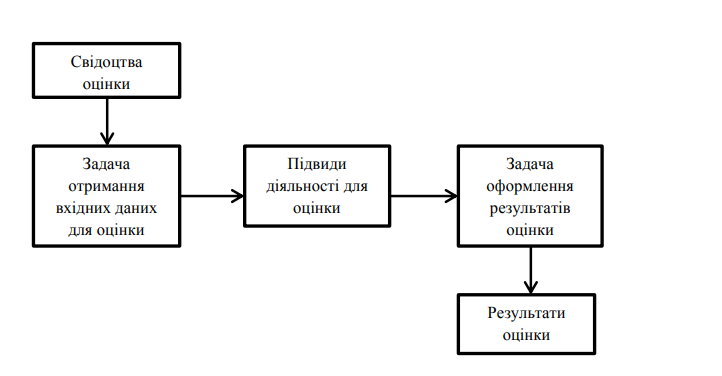


Рис. 1.1. Модель оцінки системи автоматизованого захисту об’єкта інформації

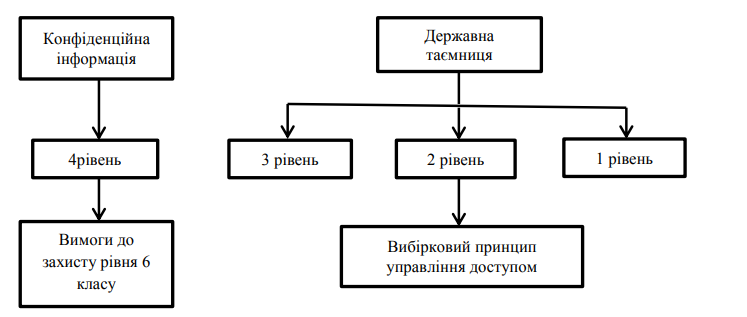


Рис. 1.2. Відповідність конфіденційності інформації до контроля доступом

Необхідно враховувати об’єкти захищеності інформації. Вони можуть бути наступними:

1. Автоматизовані системи – повинна знаходитися тільки на контрольованій території.

2. Засоби обчислюваної техніки.

3. Виділені приміщення.

### 1.6 Висновки по розділу

В даному розділі дипломної роботи були викладені основні положення та правові основи інформаційної безпеки України. Проблему інформаційної безпеки було визначено, як одну з найважливіших складових бізнесу, так як питання забезпечення інформаційної безпеки сьогодні стохть на одному рівні із самим функціюванням підприємств. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, фінансової, та інших складових бізнесу. Мною були проаналізовані основні загрози інформаційній безпеці, їх класифікація та джерела виникнення.

Також увага була приділена основним методам та засобам захисту інформації, при цьому основний акцент був поставлений на автоматизовані засоби захисту інформації. Були визначені основні методи та алгоритми протидії, їх основні переваги та недоліки. Також проведений аналіз нормативно - правового забезпечення захисту інформації, зокрема правові основи інтеграція іноземного ПЗ в Україні.

Висновки по даному розділі дозволяють сформувати головне завдання дипломної роботи – автоматизація захисту інфраструктури підприємства.

### Розділ 2. СУЧАСНІ НАПРЯМИ АВТОМАТИЗАЦІЇ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

## 2.1. Поняття та завдання мережевої інфраструктури

Мережева інфраструктура – сукупність обладнання і програмного забезпечення, яка створює середовище для процесу обміну інформацією і роботи бізнес-додатків. Центральне місце в мережевій інфраструктурі займає локальна обчислювальна мережа (ЛОМ), яка об’єднує локальні інформаційні та обчислювальні ресурси і дозволяє організувати доступ до них, а також служить для надання сервісів і підтримки бізнес-процесів.

Завдання мережевої інфраструктури:

1. Обмін даними між стаціонарними або портативними робочими станціями (комп’ютерами) співробітників, розміщеними в одному офісі, чи будівлі. Джерелом даних можуть бути різноманітні однорангові сервіси, наприклад, сервіс обміну миттєвими повідомленнями, широкомовна трансляція мультимедійних даних або передача файлів за допомогою протоколів SMB/CIFS чи навіть BitTorrent.
2. Доступ до корпоративних серверів, застосунків чи додатків, розташованих в географічно ізольованій частині підприємства («локальні сервери»). Це завдання є одним з найпоширеніших під час проектування IT-інфраструктури підприємства. До прикладів належать: сервер електронної пошти, сервер корпоративного каталогу, термінальний сервер, окремий сервер централізованого збереження файлів, тощо.
3. Організація розподіленої інфраструктури мережевих сервісів, яка не виходить за межі географічно ізольованої частини підприємства. Наприклад, сервіс IP-телефонії та відео-конференцій, IP-відеоспостереження, контролю та управління фізичним доступом, інфраструктура бездротового доступу до мережі (Wi-Fi), сенсорів з оцінки якості каналів зв’язку чи будь-яких інших мережевих сенсорів. Визначною особливістю цього класу задач є вимога надання живлення кінцевим пристроям через сигнальний інтерфейс, за допомогою якого вони підключаються до мережі (технологія Power-over-Ethernet).
4. Об’єднання кількох локальних серверів в єдиний обчислювальний кластер. Кластеризація – найпоширеніший метод створення надійного та стійкого до відмов корпоративного сервісу (незалежно від його типу чи призначення). Прикладами можуть бути кластер серверів корпоративного каталогу, IP-АТС чи підсистеми віртуалізації.
5. Створення транспортної інфраструктури для систем автоматизації та контролю промислового виробництва. Особливістю цього класу задач є жорсткі умови промислової експлуатації мережевого обладнання та підвищені вимоги до його надійності. Також для уникнення впливу електромагнітного випромінювання промислового обладнання на передачу критичних даних бажано використовувати оптичні лінії зв’язку замість мідних.
6. Організація доступу користувачів багатоквартирних будинків до публічної мережі Internet. Транспортна інфраструктура «домашніх мереж» за своєю структурою подібна до звичайних провідних локальних мереж. Але й вони мають свої особливі вимоги, що стосуються, зокрема, формфактору пристроїв.

Прикладом ЛОМ може бути мережа на рис 2.1.



Рис. 2.1. Приклад ЛОМ підприємства

## 2.2. Базові компоненти для створення мережевої інфраструктури

Ethernet – комутатори. Комутатори цього класу найпоширеніші завдяки великому діапазону їх функціональності і, як наслідок, їх різноманітного застосування. Зазвичай вони мають від 8 до 48 фіксованих Ethernet-інтерфейсів з максимальною швидкістю передачі даних 100 або 1000 Мбіт/сек, а також невелику кількість (1-4 шт.) магістральних портів. Фіксовані комутатори можуть бути некерованими, керованими за допомогою лише web-інтерфейсу або ж вони можуть мати повнофункціональний інтерфейс віддаленого адміністрування (що включатиме, в тому числі, інтерфейс командного рядка CLI). Серед додаткових функцій таких пристроїв можна назвати можливість створення стеку з кількох окремих комутаторів, підтримку технології живлення Power-over-Ethernet, підтримку протоколів третього рівня моделі OSI (напр., маршрутизації IP-пакетів) або навіть наявність вбудованого контролера бездротових мереж. Зазвичай цей клас комутаторів використовують для створення так званого «рівня доступу» мережі, тобто до них підключаються кінцеві пристрої. Для створення відносно невеликих за масштабом мереж комутатори фіксованої конфігурації можуть бути використані також і на «рівні ядра» або «рівні розподілення/агрегації».

Світові виробники: Cisco, HP, Extreme Networks, Juniper Networks, Alcatel-Lucent, Allied Telesis, TP-Link, D-Link, ZyXEL та багато інших.

Модульні Ethernet – комутатори. Ці модульні пристрої можуть складатися з таких основних компонент: шасі (з вмонтованими або дискретними модулями керування), блоків живлення, блоків вентиляторів та інтерфейсних модулів з широким спектром конфігурацій портів (мідні або оптичні, зі швидкістю передачі даних 1, 10, 40 або 100 Гбіт/сек). Деякі реалізації можуть мати дискретні плати міжмодульної комутації та/або сервісні модулі, що виконують певні додаткові функції (наприклад, функції міжмережевого екрану). Майже завжди модульні комутатори мають надзвичайно високу продуктивність та апаратно підтримують протоколи третього рівня моделі OSI.

Зазвичай цей клас комутаторів використовується на рівні ядра або рівні розподілення/агрегації. У випадку створення локальної мережі з єдиним комутаційним центром модульні комутатори можуть виконувати функції комутаторів рівня доступу.

Світові виробники: Cisco, HP, Extreme Networks, Juniper Networks, Alcatel-Lucent та інші.

Спеціалізовані Ethernet – комутатори Цей окремий клас комутаторів відрізняється від інших наявністю захищеного (від пилу, вологи та вібрацій) корпусу, широким діапазоном робочих температур, можливістю живлення від джерела постійного струму та підтримкою протоколів «Industrial Ethernet». Серед основних додаткових характеристик можна виділити невеликі розміри, модульність, можливість встановлення на DIN-рейку, наявність контрольного інтерфейсу типу «сухий контакт». Також обов’язково серед модельного ряду комутаторів цього класу повинні бути моделі з великою кількістю різноманітних оптичних інтерфейсів.

Світові виробники: Cisco, Hirschmann, Siemens, Honeywell, Moxa та інші.

Спеціалізовані мережеві комутатори. При створенні розподіленої корпоративної мережі цей окремий клас пристроїв використовується операторами зв’язку, а не кінцевими підприємствами. Такі комутатори мають багато спільного з комутаторами, призначеними для побудови локальних провідних мереж. Їх особливістю є підтримка спеціалізованих для операторів зв’язку протоколів, наприклад, SONET, SDH, QinQ, MPLS тощо.

Світові виробники: Cisco, HP, Extreme Networks, Juniper Networks, Alcatel-Lucent та інші.

# 2.3. Класифікація атак та уразливостей на інформаційні ресурси

* Атака листами. Вважається найстарішим методом атак, хоча суть його проста й примітивна: велика кількість листів унеможливлюють роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Цю атаку складно запобігти, тому що провайдер може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином.
* Віруси, троянські коні, поштові черв'яки, сніффери, Rootkit-и і інші спеціальні програми.

Наступний вид атаки є більш витонченим методом отримання доступу до закритої інформації - це інтеграція спеціальних програм для ведення роботи на комп'ютері жертви, а також подальшого розповсюдження (це віруси і черв'яки).

* Мережева розвідка. У ході такої атаки крекер власне не робить ніяких деструктивних дій, але в результаті він може отримати закриту інформацію про побудову та принципи функціонування обчислювальної системи жертви. У ході такої розвідки зловмисник може виробляти сканування портів, запити DNS, луна-тестування відкритих портів, наявність і захищеність проксі-серверів.
* Сніффінг пакетів. Також досить поширений вид атаки, заснований на роботі мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. У такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальним додатком, який називається сніффер, для обробки. У результаті зловмисник може отримати велику кількість службової інформації: хто звідки куди передавав пакети, через які адреси ці пакети проходили.
* IP-спуфінг. Теж поширений вид атаки в недостатньо захищених мережах, коли зловмисник видає себе за санкціонованого користувача, перебуваючи у самій організації, або за її межами. Така атака можлива, якщо система безпеки дозволяє ідентифікацію користувача тільки за IP-адресою і не вимагає додаткових підтверджень.
* Man-in-the-Middle. З англ. «Людина посередині». Коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. Мета такої атаки - крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі 1. Тому в чисто технічному плані убезпечити себе можна лише шляхом криптошифрування переданих даних 2.
* Соціальна інженерія. Соціальна інженерія (від англ. Social Engineering) - інтеграція некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації. Як говорить стара приказка, «Найслабкіша ланка системи безпеки - людина».
* Відмова в обслуговуванні. DoS (від англ. Denial of Service - відмова в обслуговуванні) - атака, яка має на меті змусити сервер не відповідати на запити.
* Ін'єкція. Атака, пов'язана з різного роду ін'єкціями, має на увазі впровадження сторонніх команд або даних в працюючу систему з метою зміни ходу роботи системи, а в результаті - одержання доступу до закритих функцій та інформації або дестабілізації роботи системи в цілому.SQL-ін'єкція - атака, в ході якої змінюються параметри SQL-запитів до бази даних.PHP-ін'єкція - один із способів злому веб-сайтів, що працюють на PHP.;Міжсайтовий скриптинг або СSS (абр. від англ. Cross Site Scripting) - тип атак, зазвичай виявляють у веб-додатках, які дозволяють впроваджувати код зловмисних користувачам у веб-сторінки, що переглядаються іншими користувачами.XPath-ін'єкція - вид атак, який полягає у впровадженні XPath-виразів у оригінальний запит до бази даних XML.

Перед тим як перейти до самого списку вразливостей важливо зрозуміти що це таке і якими вони бувають. Як я вже сказав, вразливість - це помилка в програмі або недолік, за допомогою якої користувач може використовувати програму так, як це не було заплановано її розробником. Це може бути відсутність перевірки на правильність отриманих даних, перевірки джерела даних, неправильна адресація в пам'яті та розміру даних. Найнебезпечніші уразливості - це ті, які дозволяють виконувати довільний код. В оперативній пам`яті всі дані мають певний розмір і програма розрахована на запис в пам`ять даних від користувача того ж розміру. Якщо користувач адресує більше даних, програмний додаток повинен повідомити коричстувача про помилку. Але якщо розробник припустився помилки, то дані модифікують код програми і процесор буде намагатися їх виконати, таким чином і виникають уразливості переповнення буфера

- Dirty COW. Це уразливість, яка була виявлена ​​у 2016 році. Назва Dirty COW розшифровується як Copy on Write. Помилка виникає в файлової системі під час копіювання при записі. Це локальна уразливість, яка дозволяє отримати повний доступ до системи будь-якого звичайним користувачем. Якщо коротко, то для інтеграція уразливості потрібно два файли, один доступний на запис тільки від імені суперкористувача або root, другий для нас. Починаємо дуже багато раз записувати дані в наш файл і читати з файлу суперкористувача, через певний час настане момент, коли буфери обох файлів змішаються і користувач зможе записати дані в файл, запис якого йому недоступна, таким чином можна надати права root авторизованому в системі користувачу. Уразливість була в ядрі близько 10 років, але після виявлення була швидко усунена, хоча залишилися ще мільйони пристроїв Android в яких ядро ​​не оновлювалося і цю уразливість можна експлуатувати. Уразливість отримала код CVE-2016-5195.

- Heartbleed. У 2014 році була виявлена ​​одна з найбільших за масштабом і наслідками вразливість. Вона була викликана помилкою в модулі heartdead програми OpenSSL, звідси і назва Heartbleed. Уразливість дозволяла зловмисникам отримати прямий доступ до 64 кілобайт оперативної пам`яті сервера, атаку можна було використовувати доки вся пам`ять не буде прочитана. Незважаючи на те, що виправлення було випущено дуже швидко, постраждало дуже багато сайтів і додатків. Фактично уразливими були всі сайти, які використовують HTTPS для захисту трафіку. Зловмисники могли отримати паролі користувачів, їхні особисті дані і все що знаходилося в пам`яті в момент атаки. Уразливість отримала код CVE-2014-0160.

-Stagefright. Уразливість Stagerfight не виняток. Правда, це не зовсім проблема Linux. Stagefright - це бібліотека для обробки мультимедійних форматів в Android. Вона реалізована на C ++, а значить уникає всі захисні механізми Java. Зловмиснику було досить відправити MMS на уразливий смартфон із спеціально модифікованим медіафайлів, через що він отримував повний контроль над пристроєм з можливістю записувати і читати дані з карти пам`яті. Уразливість була виправлена ​​розробниками Android але і на сьогоднішній день мільйони пристроїв залишаються уразливими.

-Уразливість нульового дня ядра. Це локальна уразливість, яка дозволяє підвищити права поточного користувача до root через помилки в системі роботи з криптографічними даними ядра, які зберігаються в пам`яті. Вона була виявлена ​​в лютому 2016 року і охоплювала всі ядра починаючи від 3.8, а це значить що уразливість існувала 4 роки. Помилка могла використовуватися хакерами або шкідливим програмним забезпеченням для підвищення своїх повноважень в системі, але дуже швидко була виправлена.

-Shellshock. Ця вразливість була виявлена ​​в 2014 році перед тим як проіснувала 22 роки. Отримала код CVE-2014-6271 і кодове ім`я Shellshock. Ця вразливість порівнянна за небезпекою з уже відомою Heartbleed. Вона викликана помилкою в інтерпретаторі команд Bash, який використовується за умовчанням в більшості дистрибутивів Linux. Bash дозволяє оголошувати змінні оточення без аутентифікації користувача, а разом з ними можна виконати будь-яку команду. Особливої ​​небезпеки це набирає в CGI скриптах. Уразливості були піддані всі версії Bash, включаючи 4.3, правда після виявлення проблеми розробники дуже швидко випустили виправлення.

Але завдяки автоматизації реакції на експлуатацію вразливостей, інтеграція виявляється практично неможливим. Головним критерієм безпеки інформаційно-комунікаційної системи є інтегрованість процесів та постійне оновлення компонентів такої системи.

## 2.4. Безпека мережевої інфраструктури

У наш час, коли інформаційні технології вже міцно пов’язані з бізнес-процесами більшості компаній, а способи і методи мережевих атак постійно удосконалюються і розвиваються, все ще існує думка що установка звичайного мережевого екрану на кордоні мережі достатньо для захисту внутрішніх корпоративних ресурсів. Це, на жаль, не зовсім так, а, вірніше, зовсім не так.

Як приклад малої ефективності звичайного брандмауера, користувач системи може самостійно натиснути на посилання, отримане від добре знайомого друга в соціальній мережі або поштою, завантажити і запустити вірус, який, використовуючи відомий експлоїт неоновленої ​​операційної системи або програми, отримає права адміністратора і буде виконувати зловмисну ​​задачу зсередини корпоративної мережі. При цьому копії вірусу будуть активно розсилатися по контакт листу ураженої системи. В Інтернеті доступні онлайн системи для тестування підозрілих файлів різними антивірусними програмами, але ними в першу чергу користуються ті ж зловмисники для написання нових «непомітних» вірусів. У зв’язку з цим у наш час існує така величезна кількість бот-нет мереж, досить просто купити номера крадених кредитних карток і все більше злом комп’ютерів стає звичайним методом заробляння грошей. Тому завдання забезпечення безпеки вимагає комплексного підходу на всіх рівнях мережевої інфраструктури і комп’ютерних ресурсів.

**Загальні підходи та технології для побудови безпечної мережі.** Процес побудови безпечної мережевої інфраструктури починається з планування. На цьому етапі перераховуються сервіси, які будуть використовуватися в мережі, пов’язані з ними ризики, визначаються необхідні кроки і механізми для зниження цих ризиків. На підставі даних, отриманих на етапі планування, розробляється відповідний дизайн мережевої інфраструктури і створюється набір політик безпеки. Після цього йде етап безпосереднього впровадження. Оскільки безпека це не кінцевий результат, а процес, впровадженням і первинним налаштуванням якої-небудь системи захисту нічого не закінчується. Рішення безпеки вимагають постійної «уваги»: відстеження подій безпеки, їх аналізу та оптимізації відповідних політик.

Від написання ефективних політик безпеки та їх суворого дотримання дуже залежить робота всього комплексу захисту. Правильні політики повинні бути зафіксовані документально, не мати великої кількості винятків. На все обладнання повинні регулярно встановлюватися оновлення. Також велику загрозу для безпеки складають прості паролі, помилки в конфігурації пристроїв, інтеграція налаштувань за замовчуванням, незахищених протоколів і технологій.

Для забезпечення повної безпеки всієї IT інфраструктури необхідно впроваджувати механізми захисту на всіх рівнях мережі від кордону до комутаторів доступу. На рівні доступу рекомендується використовувати керовані комутатори з підтримкою функціоналу захисту протоколів ARP, DHCP, STP. Авторизувати користувачів при підключенні за допомогою технології 802.1x. Підключати співробітників в різні VLAN залежно від їх функціональних обов’язків і задавати правила взаємодії і доступу до різних ресурсів на рівні розподілу.

При підключенні до мережі WAN та Інтернет важливо крім брандмауера мати можливість сканувати трафік на рівні додатків, перевіряти наявність загроз за допомогою IPS систем. Прикордонне обладнання повинно бути стійким до DoS і DDoS атак. Вкрай рекомендується для виходу користувачів в Інтернет використовувати проксі сервера з додатковою перевіркою на віруси, небажане, шкідливе і шпигунське ПЗ. На проксі додатково можна організувати веб та контент фільтрацію. Також важлива наявність рішення для перевірки пошти на предмет спаму і вірусів. Всі корпоративні ресурси, до яких потрібно забезпечити доступ ззовні в цілях безпеки повинні бути винесені в окрему демілітаризовану зону DMZ. Для віддаленого доступу використовувати технологію VPN з шифруванням переданих даних.

Для управління всім мережевим обладнанням повинні використовуватися захищені протоколи SSH, HTTPS, SNMPv3. Для можливості аналізу логів час на пристроях має бути синхронізований. Для розуміння, який трафік ходить в мережі, наскільки завантажено обладнання, які події на ньому відбуваються, використовувати протоколи Syslog, RMON, Sflow, NetFlow. Дуже важливо вести облік, хто, коли і які зміни вносить в конфігурацію устаткування.

**Реалізація захищеної мережі для невеликого офісу.** Для невеликих офісів з кількістю співробітників до 25 осіб рекомендуємо використовувати UTM рішення, яке в одному пристрої об’єднує повний функціонал безпеки, що включає міжмережевий екран, антивірус, анти-спам, IPS, захист від атак DoS і DDoS, веб і контент фільтрація, різні способи побудови VPN. Такі продукти виробляють компанії Fortinet і SonicWall, лідери на ринку в даній області. Пристрої мають повноцінний веб інтерфейс управління, що спрощує завдання конфігурації для адміністратора, який часто в маленьких компаніях тільки один. Наявність в обладнанні достатньої кількості дротових і бездротових інтерфейсів, підтримка віддаленого доступу до корпоративних ресурсів, інтеграція з різними службами каталогів робить ці пристрої ідеальним рішенням для невеликого офісу. Для підключення дротових користувачів в рішення рекомендуємо додати керований комутатор другого рівня з налагодженим  захистом від атак з локальної мережі.

**Приклади рішень безпечної інфраструктури для середнього офісу.** Для середніх офісів рекомендується модульна організація мережі, де кожен пристрій відповідає за певне коло завдань. На таких підприємствах локальну мережу необхідно будувати з обов’язковим поділом рівнів ядра і доступу користувачів. При великій кількості серверів окремо виносити комутатори агрегації дата центру. Рекомендується розмежувати функції прикордонного маршрутизатора і міжмережевого екрану, розділивши їх на два різних пристрої. Сервера, до яких необхідний доступ ззовні, перенести в окрему зону DMZ. Резервування модуля підключення до Інтернет мережі можна досягти шляхом дублювання всього обладнання і налаштування на них відповідних протоколів відмовостійкості. При наявності в компанії філій, надомних і мобільних співробітників, підключення до корпоративних ресурсів необхідно забезпечити за технологією VPN. Також однією з важливих складових рішення безпеки є програмне забезпечення для моніторингу мережі, наявність якого суттєво полегшить роботу мережевих адміністраторів і дозволить вчасно реагувати на загрози, забезпечуючи цим безперервність роботи всіх мережевих сервісів.

Для побудови такого роду рішення рекомендуємо використовувати обладнання виробників Cisco, HP, Huawei, Fortinet, SonicWall, PaloAlto, у кожного з яких є свої сильні сторони і унікальні особливості, які в сумі дають змогу отримати безпечну і в той же час прозору для управління та моніторингу мережу.

**Мережева безпека у великій розподіленій мережі підприємства.** Мережа великого розподіленого підприємства за принципом реалізації подібна до середнього і відрізняється більшим розподілом функцій між пристроями, вищими вимогами до відмовостійкості, наявністю виділеної WAN мережі для передачі даних між філіями. Модуль підключення до WAN в цілях безпеки реалізується окремо від модуля підключення до Інтернет. Для побудови такої мережі використовується обладнання тих же виробників, які були перераховані для середнього підприємства.

## 2.5. Програмне-апаратне забезпечення для побудови систем безпеки мереж

Корпоративні мережі та їх ресурси постійно перебувають під загрозою зараження шкідливим програмним забезпеченням та/або мережевої атаки. Цілі й завдання зловмисників можуть бути різними:

* Отримання несанкціонованого доступу до інформаційних ресурсів та крадіжка даних
* Знищення й псування даних
* Порушення функціонування та доступності сервісу
* Отримання контролю та інтеграція скомпрометованих систем для інших атак або як частини ботнет-мереж

Способи деструктивних вторгнень можуть варіюватися від вірусів, надісланих електронною поштою, до експлуатації прихованої вразливості у публічних веб-сервісах компанії. Джерелом загрози можуть бути не тільки професійні хакери та конкуренти, але також і власні співробітники. Оскільки фактично всі рівні мережевої інфраструктури можуть бути вразливими, існує велика кількість можливостей для здійснення різних атак.

Щоб нейтралізувати ці загрози, уникнути чи мінімізувати можливі збитки, необхідно впроваджувати відповідні механізми захисту та контролю доступу на всіх рівнях мережевої інфраструктури.

Мережеві екрани (firewall). Апаратно-програмний комплекс, який сегментує мережу на зони безпеки та здійснює контроль і фільтрацію мережевих пакетів, що проходять крізь нього, відповідно до заданих правил. Нещодавно, завдяки інтеграції та додавання мережевим екранам функціоналу інших систем безпеки (IPS, Web Proxy, Antivirus та ін.), виник новий клас пристроїв – багатофункціональні пристрої безпеки або мережеві екрани нового покоління (UTM, NGFW). Виробники: Cisco, CheckPoint, Fortinet, Juniper, WatchGuard, McAfee, SonicWall.

Системи виявлення й запобігання вторгненням (ips). Технічний засіб, призначений для аналізу мережевого трафіку, виявлення фактів шкідливої чи аномальної активності (мережеві атаки, мережеві хробаки, ботнет) та автоматичного захисту від них. Виробники: Cisco, HP, IBM, Fortinet.

Системи контекстного захисту поштового та веб-трафіку (proxy, web security gateway, email security gateway ). Спеціалізовані інтернет-шлюзи (проксі-сервери), що дозволяють захистити корпоративну пошту і веб-трафік від спаму та шкідливих програм і сайтів (вірусів, хробаків, фішингу та ін.),  забезпечити цілісність, конфіденційність та захист від підміни корпоративних даних, що передаються через поштові повідомлення та веб, а також контролювати інтеграція інтернет-ресурсів і веб-додатків. Виробники: Cisco (IronPort), BlueCoat, Websense, McAfee, WatchGuard, Barracuda, Fortinet.

Системи безпеки прикладних сервісів (web application firewall, database security). Мережеві екрани рівня додатків, призначені для спеціалізованого захисту мережевих сервісів від різноманітних атак та експлуатації відомих вразливостей. Виробники: IBM, Imperva, F5, Citrix, Fortinet.

Системи захисту від dos/ddos-атак (anti-ddos). Технічні засоби для захисту мережевих служб і сервісів від простих та розподілених атак на відмову в обслуговуванні. Виробники: Arbor, Radware, Voxility, A10, Fortinet.

Системи захисту кінцевих точок с можливістю поведінкового аналізу. Програмне забезпечення, що базується на системі модулів, кожен з яких використовує унікальну методику виявлення шкідливого ПЗ. Також є додаткові модулі контролю встановлених додатків, контролю доступу в інтернет, контроль з’ємних пристроїв. Виробники: Sophos, McAfee, Fortinet.

Системи балансування навантаження та доставки додатків. Фізичні пристрої, що допомогають балансувати вхідний трафік на веб-сервери та шифрувати всі підключення. Виробники: Fortinet, F5, Cisco, Citrix.

Системи пасток для зловмисників. Платформа для побудови багаторівневої системи захисту, в яку входять засоби розміщення і управління мережевими сенсорами, decoy-токенами, пісочниця, аналізатор трафіку, засоби захисту від вірусів-шифрувальників, система кореляції подій і групової обробки інцидентів. Виробники: Fortinet, TrapX, Attivo.

Системи додаткового аналізу ПЗ. Фізичні або віртуальні пристрої, що проводять додатковий аналіз ПЗ на яке не має сігнатури. Після перевірки додає вердикт та відправляє в глобальну інформаційну базу. Виробники: Fortinet, F5, Cisco, Citrix.

Ринок України на сьогоднішній день наповнений різними виробниками, але небагато з них дають змогу створити автомазивану систему інформаційної безпеки, яка буде своєчасно реагувати на загрози та локалізовувати їх. Тому було обрано двох конкурентів CheckPoint та Fortinet.

**Fortinet – це американська компанія, що спеціалізується на пристроях мережевої безпеки. Флагманський продукт компанії Fortinet продається під торговою маркою FortiGate. Компанія Fortinet була заснована в 2000 році Кеном Ксі, засновником і колишнім президентом NetScreen, і є публічною компанією. Компанія Fortinet займає найбільшу частку ринку серед UTM-рішень, займає 3 місце в світі за щорічним обсягом проданих пристроїв мережевої безпеки.**

**Високорівневі інтегровані системи Fortinet в основному використовуються в корпоративному сегменті ринку для легкого, швидкого і ефективного побудови системи безпеки мереж. Особливою популярністю вони користуються у компаній, що відносяться до SMB (Small and Medium Business), завдяки простоті інтеграція і економічності.**

**Комплексні системи безпеки (UTM), які є основним продуктом компанії Fortinet - це багатофункціональні програмно-апаратні комплекси, в яких поєднані функції наступних пристроїв: брандмауера (Firewall або Brandmauer), системи виявлення та запобігання вторгнень в мережу (IDS / IPS), а також функції антивірусного шлюзу (Antivirus). Такі комплекси також мають захист від небезпечних веб-сайтів і спаму.**

**Крім UTM-рішень, Fortinet пропонує великий вибір систем для забезпечення інформаційної безпеки організацій: починаючи від захисту робочих станцій і закінчуючи комплексним захистом всієї інформаційної інфраструктури підприємств.**

**Відмінною особливістю пропонованих компанією Fortinet рішень є інтеграція власних, «заточених» під завдання безпеки, апаратних і програмних рішень. До таких рішень відносяться спеціалізовані процесори FortiASIC, створені для сигнатурного аналізу трафіку і прискорення його обробки та шифрування. Для управління всіма компонентами захисту розроблена операційна система FortiOS. Завдяки цьому, продукти компанії Fortinet забезпечують виявлення і усунення загроз в режимі реального часу, без втрати пропускної здатності мережі і надають великий набір інструментів для аналізу та управління трафіком.**

**Ще однією візитною карткою компанії є постійно оновлювані антивірусні бази (оновлення відбувається 3-4 рази на день), настройка політик безпеки всієї мережі за допомогою єдиного інтуїтивно-зрозумілого додатка і гнучка масштабованість пристроїв, що дозволяє «збирати» рішення в сфері безпеки під конкретні завдання конкретного споживача. Всі ці особливості роблять продукти Fortinet не тільки ефективними, але і рентабельними. Фахівці Fortinet розробили і підтримують власні онлайн-ресурси для роботи своїх систем фільтрації спаму (база репутацій) і інтернет трафіку (база класифікацій веб-сайтів).**

### 2.5.1. Класифікація обладнання Fortinet

**Багатофункціональні пристрої захисту FortiGate. Пристрої FortiGate представляють собою спеціалізовані програмно-апаратні комплекси, призначені для організації комплексного захисту мереж від зовнішніх загроз. Інтеграція даних пристроїв дозволяє розвантажити комп'ютери користувачів від функцій захисту інформації і зосередити їх в єдиному легко настроюється і супроводжуваному центрі. FortiGate містить в собі функціональне наповнення маршрутизатора, брандмауера, VPN-концентратора, антивіруса, антиспам фільтра, веб - фільтра, системи виявлення вторгнень.**

**2. Бездротові пристрої безпеки FortiWiFi. Бездротові шлюзи безпеки FortiWiFi є об'єднанням в одному пристрої вбудованих точок бездротового доступу корпоративного класу 802.11a / b / g з багатофункціональними системами безпеки FortiGate. Це розширює функціональність пристроїв FortiGate можливістю віддаленого управління. FortiWiFi є зручним рішенням для віддалених офісів, постачальників радіоуслуг, роздрібних торгових точок і точок широкосмугового доступу для дистанційних користувачів. Пристрої FortiWiFi можуть використовувати технологію POE (електроживлення через Ethernet), яка полегшує їх установку і розміщення, а також знижує витрати на обладнання.**

**3. Системи централізованого управління FortiManager. Серія пристроїв FortiManager надає всі необхідні інструменти для ефективного управління інфраструктурою безпеки Fortinet будь-якого розміру: від кількох до тисяч пристроїв і агентів персонального захисту. Пристрої забезпечують централізоване управління ініціалізацією, конфігурацією і оновленням пристроїв FortiGate, FortiWiFi, FortiMail, а також агентів персонального захисту FortiClient. Пристрої мають можливості наскрізного моніторингу для підвищеного контролю роботи мережі. Пристрої FortiManager, спільно з пристроями FortiAnalyzer, надають собою комплексне рішення централізованого управління, записуючий події і створює звіти по всіх наявних в організації пристроїв Fortinet. Серія FortiManager складається з п'яти моделей: 100C, 400B, 1000C, 3000C і 5001A, які мають такі основні характеристики: - кількість підтримуваних мережевих пристроїв (від 10 до 5000); - кількість підтримуваних агентів FortiClient (від 2500 до 120000).**

**4. Системи централізованого звітності FortiAnalyzer. Серія пристроїв FortiAnalyzer призначена для централізованого збору, зберігання і аналізу інформації, що надходить з пристроїв Fortinet (FortiGate, FortiMail, FortiClient). Використовуючи широкий набір легко настроюються звітів, користувачі можуть фільтрувати і переглядати записи про трафік, вірусних та інших атаках, вмісті веб-контенту, електронної пошти та інші події. Отримані дані можуть аналізуватися з метою визначення рівня захищеності мережі і ступеня відповідності політик безпеки вимогам стандартів і нормативних документів. FortiAnalyzer також надає розширені можливості по управлінню безпекою, такі як приміщення файлів в карантин, кореляція подій, оцінка уразливості, аналіз трафіку і архівування електронної пошти, історія веб-звернень, дані сервісів миттєвих повідомлень і файлів, що передаються.**

**5. Пристрої забезпечення безпеки електронної пошти FortiMail. Серія пристроїв FortiMail призначене для захисту поштових сервісів компанії від DoS атак, Directory harvest атак, виявлення і блокування вірусів, троянів і інших шкідливих програм в поштових повідомленнях, блокування небажаної кореспонденції (спам), а також виконання правил маршрутизації корпоративної пошти. FortiMail в реальному часі дозволяє проводити сигнатурний і евристичний аналіз електронної пошти (SMTP, POP3, IMAP) на наявність вірусів і спаму. FortiMail може використовуватися як самостійно, так і в комплексі з FortiGate.**

**6. Захист веб-серверів FortiWeb. Спеціалізований апаратний міжмережевий екран для веб-додатків FortiWeb забезпечує балансування навантаження, безпеку і прискорення роботи веб-додатків і баз даних, а також процесу обміну інформацією між ними. Системи FortiWeb розроблені для великих і середніх підприємств, постачальників програмно-апаратних ресурсів і постачальників програмного забезпечення в якості послуг. FortiWeb виходить за рамки традиційних брандмауерів і веб-додатків, допомагаючи забезпечити безпеку запитів xml, прискорити роботу додатків і балансувати навантаження на сервера.**

**7. Комутатори FortiSwitch. Серія пристроїв FortiSwitch являє собою набір з 1 Гб і 10 Гб Ethernet комутаторів, призначених для підключення персональних комп'ютерів і різних пристроїв до мережі. FortiSwitch дозволяють організувати високошвидкісні мережі, керовані виртуализацией сервера, паралельні і хмарні обчислення. Перевагами старших моделей FortiSwitch є їх масштабованість, що дозволяє досить просто збільшувати кількість портів 10 Гб Ethernet в рамках одного комутатора.**

**8. Клієнти персонального захисту FortiClient. FortiClient - це програмне забезпечення персональної мережевої безпеки для робочих станцій і кишенькових персональних комп'ютерів, а також смартфонів. Призначено для роботи в операційних системах сімейства Microsoft Windows (NT, 2000, XP, Vista), Microsoft Windows mobile і Symbian. FortiClient об'єднує в собі антивірус, антиспам, міжмережевий екран, IPSec VPN, захист від програм-шпигунів і веб-фільтр. Автоматичні оновлення, одержувані від підписаний служби FortiGuard або через системи FortiManager, гарантують захист від сучасних загроз.**

### 2.5.2. Функціональні можливості ядра мережі Fortigate

**Пристрої FortiGate є «флагманським» продуктом компанії Fortinet в сфері забезпечення мережевої безпеки. Решта пристрою, хоча і можуть використовуватися самостійно, найчастіше використовуються для розширення можливостей FortiGate.**

* **антивірус здійснює сигнатурну і евристичну перевірку трафіку на наявність вірусів в режимі реального часу. Перевіряється веб-трафік (HTTP), FTP, електронна пошта (SMTP, POP3, IMAP), протоколи обміну миттєвими повідомленнями (ICQ, AIM, MSN, Yahoo), протокол передачі новин (NNTP). Антивірусні сигнатури оновлюються автоматично з серверів Fortinet;**
* **антиспам проводить перевірку електронної пошти (SMTP, POP3, IMAP) на наявність спаму. Проводиться тестування різних параметрів електронної кореспонденції, ведення білого / чорного листів IP-адрес і електронних адрес відправників і одержувачів, запобігання витоку інформації з інтеграціям списку заборонених фраз. Здійснюється перевірка репутації відправника в глобальній базі репутацій FortiGuard і сигнатурний аналіз кореспонденції;**
* **аутентифікація користувачів дозволяє здійснювати аутентифікацію користувачів перед наданням мережевих сервісів. Підтримується локальна база користувачів, взаємодія із зовнішніми системами аутентифікації по протоколах RADIUS, TACAC +, а також робота з каталогами LDAP, Microsoft Active directory і Novell eDirectory;**
* **веб-фільтр дозволяє налаштовувати політики інтеграція інтернету для співробітників компанії за допомогою глобальної бази даних класифікації інтернет-сайтів FortiGuard Web Filtering service (що включає в себе дані по більш 47 мільйонів сайтів). Фільтр здійснює контроль ActiveX, Cookie, Java Applet, фільтрацію URL і вмісту веб-сторінок;**
* **віртуальні домени (VDOM) дозволяють створювати кілька віртуальних пристроїв на базі одного фізичного пристрою з окремим управлінням, політиками безпеки і таблицями маршрутизації;**
* **інспектування SSL (Secure Sockets Layer) трафіку - дозволяє перевіряти інформацію всередині SSL тунелів для протоколів HTTPS, IMAPS, POP3S, SMTPS (підтримується в моделях FortiGate 80C, Voice-80C, 110C, 111C, 200B, 310B, 311B, 620B, серія 3000, серія 5000);**
* **контроль доступу до мережі (Network access control, NAC) - дозволяє забезпечувати контроль доступу до мережі пристроїв кінцевих користувачів, дозвіл або заборона доступу до мережі для комп'ютерів співробітників, в залежності від встановлених або невстановлених на них додатках і оновлень операційної системи;**
* **контроль додатків IM, P2P, VoIP, СУБД. FortiGate здійснює контроль за інтеграціям протоколів миттєвих повідомлень (ICQ, AIM, MSN, Yahoo), протоколів Peer2Peer мереж (eDonkey, BitTorrent, Kazaa, Gnutella і WinNY), протоколів передачі голосу поверх IP (H.323, SIP, SCCP, Skype). Також здійснюється захист різних додатків і протоколів (бази даних, системи архівування та ін.);**
* **контроль трафіку (traffic shaping). У FortiGate реалізовані функції управління потоком трафіку (гарантування / лімітування / пріоритизація смуги пропускання) для будь-якої програми / IP-адреси / користувача і квотування загального обсягу інформації, що завантажується;**
* **маршрутизація призначена для визначення маршруту проходження інформації в мережах зв'язку. Пристрій підтримує статичну, динамічну, гнучку маршрутизацію (RIP, OSPF, BGP, policy based routing), маршрутизацію групового (multicast) трафіку, балансування завантаження каналів зв'язку і протокол IPv6;**
* **міжмережевий екран (Firewall) призначений для здійснення контролю і фільтрації, що проходять через нього мережевих пакетів відповідно до політиками трафіку, які налаштовуються окремо для кожної категорії користувачів і кожного конкретного користувача;**
* **оптимізація і кешування WAN трафіку - спрямована на підвищення ефективності інтеграція смуги пропускання, оптимізація протоколів TCP, HTTP, FTP, MAPI, CIFS, кешування трафіку;**
* **запобігання витоку даних (Data Leak Prevention, DLP) - дозволяє запобігти поширення конфіденційної інформації через HTTP, FTP, NNTP, електронну пошту, системи миттєвих повідомлень;**
* **перетворення мережевих адрес (NAT) і балансування навантаження - підтримуються функції перетворення адрес (динамічний і статичний NAT, policy-based NAT, SIP / H.323 NAT traversal) і функції балансування навантаження між декількома серверами;**
* **режим відмовостійкості (паралельного резервування) (high availability) призначений для організації спільної роботи двох і більше пристроїв з метою підвищення відмовостійкості мережі. Підтримується синхронізація станів, Active / Active, Active / Standby режими;**
* **система виявлення і запобігання вторгнень в мережу (IDS / IPS) здійснює моніторинг мережі для виявлення несанкціонованого доступу в мережу і його блокування. Система проводить сигнатурний аналіз трафіку, аналіз аномалій трафіку, здійснює автоматичне оновлення сигнатур і дозволяє створювати власні сигнатури.**

### 2.5.3. Класифікація рішень CheckPoint

Ізраїльська компанія Check Point Software Technologies надає свої послуги з 1994 року. Продукцію CheckPoint розробляють понад дві тисячі фахівців з усього світу. Вони обслуговують всі компанії, що входять в список Fortune 100 і практично всі зі списку Fortune 500. Check Point Software Technologies надає своїм клієнтам лінійку продуктів, що захищає хмарні і віртуальні інфраструктури. Компанією розроблені технології, що запобігають крадіжку облікових записів, які забезпечують багаторівневий захист і блокування DoS-атак. Компанія надає своїм користувачам надійні шлюзи для захисту доступів до нових Інтернет-ресурсів та ін. Check Point захищає кінцеві точки мережі в компаніях малого бізнесу, забезпечує антивірусний захист підприємств через централізовану систему управління. Також продукти компанії борються з атаками вірусів-шифрувальників, які блокують роботу комп'ютерів користувачів і вимагають оплати за відновлення файлів. Фірма пропонує своїм клієнтам комплексний захист від усіх мережевих погроз - UTM-систему. Вона складається з систем запобігання витоку інформації, запобігання вторгнень, управління пропускною спроможністю та ін. Сервіс Check Point приваблює клієнтів доступною ціною, швидким підключенням і високою якістю обслуговування. Фахівці компанії оперативно реагують на будь-які запити клієнтів, використовують неформальний підхід до захисту їх продуктів. Партнерами Check Point є найвідоміші компанії в різних сферах виробництва.

Продукти Check Point можна умовно розділити на 2 великі групи:

* міжмережний захист (периметра мережі і трафіку філій, фільтрація трафіку);
* захист робочих станцій (Endpoint Security) і даних на них (Check Point GO).

В обох випадках необхідно вибрати «контейнер» і необхідний функціонал - Software Blade, що активується ліцензією. Контейнери відрізняються по продуктивності (для апаратних продуктів), кількістю підтримуваних ядер (для програмних продуктів), кількістю шлюзів безпеки, якими вони управляють (для системи управління). У випадку з Endpoint Security контейнери відрізняються лише ціною - в залежності від обсягу інсталяції.

Перевагами такого підходу є гнучкість вибору рішення, можливість підлаштувати вже куплену систему під нові вимоги інформаційної безпеки.

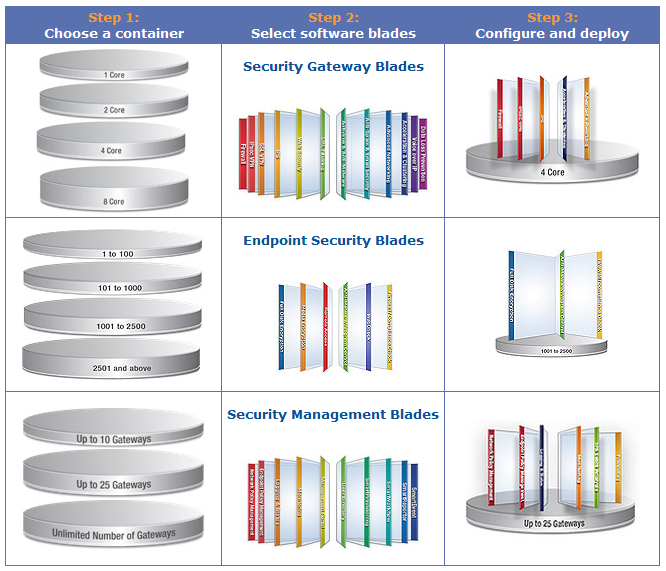


Рис. 2.2. Архітектура Checkpoint Blade

Список програмних лез для шлюзів безпеки (SecurityGateway):

* Брандмауер - забезпечує понад 200 додатків, протоколів та служб, що містять найбільш адаптивну та інтелектуальну технологію перевірки.
* IPsec VPN - безпечне підключення для офісів та кінцевих користувачів за допомогою складного, але простого управління VPN від сайту до сайту та гнучким віддаленим доступом.
* Мобільний доступ - безпечне та просте рішення для підключення корпоративних програм через Інтернет за допомогою смартфонів або ПК.
* IPS - найефективніше інтегроване рішення IPS з найкращим покриттям загроз в галузі.
* Контроль програм - забезпечує чіткий контроль додатків та ідентичності, дозволяючи організаціям створювати політики, які визначають, блокують або обмежують інтеграція тисяч програм на основі ідентичності користувача.
* Модуль інформованості - надає детальну політику безпеки для кожного користувача, групи та рівня машини. Він централізує управління, моніторинг та звітування про дії користувачів через внутрішню мережу, її периметр і далі.
* DLP - поєднує технологію та процеси для запобігання втрат даних важливої ​​бізнес-інформації.
* Веб-безпека - вдосконалений захист для всього веб-середовища, що забезпечує найсильніший захист від атак з переповненням буфера.
* Фільтрація URL-адрес - Найпопулярніша веб-фільтрація, що охоплює понад 20 мільйонів URL-адрес, захищає користувачів та підприємства, обмежуючи доступ до небезпечних веб-сайтів.
* Anti-Bot - Виявлення машин, заражених ботом, та запобігання пошкодженням бота, блокуючи зв’язок бота C&C.
* Антивірус та анти-зловмисне програмне забезпечення - провідний антивірусний захист, включаючи евристичний аналіз вірусів, зупиняє віруси, глисти та інші зловмисні програми на шлюзі
* Захист від спаму та електронної пошти - Багатовимірний захист інфраструктури обміну повідомленнями зупиняє спам, захищає сервери та усуває атаки через електронну пошту.
* Розширена мережа - додає динамічну маршрутизацію, підтримку бездротового зв'язку та якість обслуговування (QOS) до шлюзів безпеки.
* Прискорення та кластеризація - запатентовані технології SecureXL та ClusterXL забезпечують перевірку швидкості передачі пакетів, високу доступність та розподіл навантаження.
* Голосовий зв’язок через IP - розширені функції підключення та безпеки для розгортання VoIP, що мають вдосконалений захист з обмеженням швидкості, NAT в далекому кінці та інспекцію SIP TLS.

Класифікація міжмережевих екранів CheckPoint:

* CheckPoint 600 - молодший серійний пристрій, що включає в себе всі основні функції NGFW - класичний межсетевой екран, VPN, підтримує вхідний, антивірусний, контрольний додаток, веб-фільтрацію та захист електронної пошти. У серії представлені три пристрої, всі вони мають слот для SD-карти, два USB-порта, десять Ethernet-портів, підтримують ADSL, 3G / 4G-моделі, і в них також може бути доданий бездротовий адаптер Wi-Fi. У комплекті може бути включений один пристрій PCI Express.
* CheckPoint 1100 - середня серія пристроїв, що включає в себе три моделі, реалізує такі ж функції, як і пристрої 600 серій, но облачно більшу швидкість роботи. Як і 600-е, ці пристрої розміщують десять порталів Ethernet, підтримуючи різні моделі, Wi-Fi, USB, SD і PCI Express.
* CheckPoint 2200 - самостійне старше пристрій для малого бізнесу та удалених офісів. За швидкістю роботи близько до лінійки корпоративних пристроїв, більш швидкої в інших пристроях в лінійці до трех раз. У відмінні від продуктів 600 та 1100 серій, які облаковують випромінені набором захисні механізми, Check Point 2200 підтримує три віртуальні системи захисту, які можуть бути попередньо поставлені на обладнання або поставлені в процесі експлуатації. Така віртуальна система захисту компанії Check Point називає програмні блейдами, їх опис приводиться в наступному розділі. Устройство обладає шестью Ethernet-порталами, двома USB-порталами, відокремленим портом для управління і встроенним жестким диском великого об'єму.

У лінійних корпоративних продуктах та продуктів для дата-центрів пропонуються найрізноманітніші за ціною та характеристиками пристрої, а молодше обладнання в лінійці є одночасно старшим для магістрального пристрою Check Point 2200, про яке сказано вище. Характеристики інших пристроїв возрастают відповідно до індексами. У всіх продуктах корпоративні лінейки використовують технологічні програмні блейди, а продукти відрізняються кількістю одночасно працюючих комплексів захисту. Продукти корпоративної лінейки Брандмауери нового покоління включають в себе наступні серії пристроїв:

* CheckPoint 4000 - пристрої, що містять чотири моделі, можуть забезпечити різну кількість Ethernet-портів (4–8 у моделях 4200 та 8–16 в 4800-й), також можна буде запустити максимально максимум чотиримісних SFP-порталів, а також старше пристрій у кількох можливостях включити до двох порцій SFP +. Содержит 4 Гб оперативної пам’яті і жесткий диск на 250 Гб. У моделях 4200 підтримується 3 програмних блейда, в моделях 4400 і 4600 - 10, в старших моделях 4800 - до 25 блейдів. Форм-фактор усіх пристроїв 4000 серії - 1U.
* CheckPoint 12000 - у цій серії пропонується три різних пристрою. Младше обладнання з індексом 12200 підтримує від 8 до 16 Ethernet-портов, найсильніший диск в 500 Гб і можливість використовувати до 25 програмних блейдів за замовчуванням і до 50 при вдосконаленні апаратних начинок. Середнє пристрій 12400 - підтримує від 10 до 26 Ethernet-портов і дозволяє запустити 25 програмних блоків з можливістю збільшення цього числа до 75. Модель 12600 - від 14 до 26 Ethernet-портов і підтримує 75 програмних блейдів (максимум - 100). Усі пристрої серії можуть бути додатково оснащені порталами SFP / SFP + (до 4 в молодих моделях, до 12 в інших). Форм-фактор молодших моделей - 1U, інші моделі - 2U.
* CheckPoint 13000 - передбачувана серія пристроїв, що знаходиться в двох моделях - 13500 і 13800. Можливі встановити модулі з різним числом портів, що містяться в мережі Ethernet і до 12 порцій SPF / SPF +. У залежності від апаратного забезпечення підтримується запуск від 150 до 250 програмних блейдів. Форм-фактор - 2U.
* CheckPoint 21000 - сама виробнича серія, призначена для особливих великих інфраструктур та центрів даних. Оно включає в себе три моделі - 21400, 21700 і 21800. Вони оснащуються 13 Ethernet-порталами з можливістю розширення до 37, додатково можуть бути обладнані 36 SFP-порталів або 13 порталів SFP +. Младша модель підтримує 125 програмних блейдів, інших моделей - 150, для всіх моделей це число може бути розширено до 250. Усі моделі представлені у форматі-факторі 2U.

### 2.5.4. Функціональні можливості ядра мережі CheckPoint

Функціональність усіх продуктів Check Point, для дослідження двох найдрібніших продуктів у лінійці для малого бізнесу, працює на технологіях програмних блейдів. Програмні блейди - віртуальні комплексні програмні програми, налаштовані на апаратні рішення Check Point. Програмні блейди поділяються на дві категорії —обеспечають захисні механізми та надають функції за керуванням. Защитні блейди у своїй очевидності діляться на окремо ліцензовані підгруппи.

Повний список доступних для встановлення захисних блоків Брандмауер нового покоління включає брандмауер наступного покоління: Брандмауер наступної генерації Брандмауер наступного покоління включає в себе базові продукти: Система програмного забезпечення для запобігання вторгненням - підтримує багато інших, що використовуються з інтеграціям електронних і експериментальних перевірок, реалізованих потужних алгоритмів, які проаналізують захист, досить важливо намагаються різними сетевими атаками, які не були відомими ранішими і не містяться в сигнальних базах.

Програмне забезпечення для керування додатками Blade - реалізація політичної безпеки безпечного рівня для підвищення рівня доступу та окремих функцій у додатках. Область знань про більше ніж 6000 веб-представлених та 30000 соціальних сетевих віджетів. Зберігають вбудовані категорії, запропоновані, наприклад, сетеві мессенджери, файлообменники, відеоконференції та т. д., благодаря чему можна створити правила для різних типів, запропонованих без необхідності. Даний модуль може використовувати задані для настроювання політичної безпеки на рівень протоколів, запропонованих, а Gartner визначає як один з ключових відмінних NGFW від класичних середніх сетевих засобів захисту. Ім'я цього блоку можливо реалізувати правила з примери Gartner - захистити окремі функції, запропоновані, наприклад, передавати файли в Skype залишити можливість обміну повідомленнями. Групові блейдів Програми попередження загрози наступного покоління включають в себе продукти з груп Брандмауер нового покоління та наступні додаткові продукти: Блейд програмного забезпечення для фільтрування URL - керування доступом до веб-сайтів, автоматичне блокування фішингових посилань, можливість розширення доступу до інтернету для користувачів, а також скорочення швидких завантажень веб-сайтів шляхом кешування.

Антивірусне програмне забезпечення Blade - антивірусне рішення, перевіряючи весь сетевий трафік щодо наявності тимчасових файлів та об'єктів. Ми можемо значно підвищити рівень антивірусної захисту в мережах організації. Anti-Bot Software Blade - спеціалізоване рішення щодо збереження від класу тимчасових об'єктів, використовуючи комп'ютери в цілому, побудованих ботнетів та реалізацію нових зловмисних виробничих дій. У відмінність від антивірусних вирішених даних блейд реагує не на дію вредоносу на комп'ютерах, а на сетевій активності ботів, здатних обнаруживать віруси, не відомі навіть антивірусному ПО та антивірусному блейду. Блейд для захисту від спаму та електронної пошти - комплексний захист електронної пошти, який включає в себе антивірусну перевірку всіх поштових повідомлень, фільтрацію нежелатних поштових повідомлень (спаму) та захист поштових серверів від різних випадків, в тому, що вони відомі від «запису в обслуговуванні» при відправці чіткіше великого числа поштових повідомлень. Групи блейдів Безпечний веб-шлюз наступного покоління включає в себе URL-адресу Фільтр програмного забезпечення Blade, Blade Software Blade Blade та антивірусного програмного забезпечення. Несколько блейдів не входять у групи та ліцензуються окремо: IPSec VPN Software Blade - реалізація завантажених підключень між різними сегментами сетей та підключенням конкретних користувачів у мережі за захищеним протоколом IPSec. Блейд програмного забезпечення для мобільного доступу - рішення для підключення мобільних пристроїв до корпоративної мережі, що включає в себе Layer-3 VPN і SSL VPN, підтримує велику операційну систему на мобільних пристроях. У характеристичних пристроях, описаних у попередніх розроблених статтях, вказано кількість програмних блейдів, доступних для одночасних робіт на кожному з моделей. Забороняючи вільні віртуальні яйцеві програмні блейдами, можна реалізувати індивідуальну захисну систему, яка потрібна для конкретної інфраструктури. Встановлення та налаштування програмних блейдів працює з загальної для всіх продуктів Check Point програми управління SmartDashboard. При цьому в процесі роботи можливо змінити набір блейдів - в будь-якому моменті можна удалити один із захисних механізмів і замінити його іншими. Ліцензійна політика Check Point пропонує гнучкі можливості при виготовленні та прибутковості продуктів. Апаративні пристрої можуть бути доступні як окремі, так і в складі одного з вирішених, в цілому які входять одноіменні групи програмних блейдів. Програмні блейди для пристроїв, куплених відділів, можуть бути присутніми також у вигляді наборів або по відділу. Щонайменше програмні блейдови залежать від серійного обладнання, на сьогодні вони будуть вироблятись. Розрахунок вартості рішень доступний у каталозі продуктів на сайті Check Point після реєстрації.

### 2.5.5. Конкурентний аналіз виробників

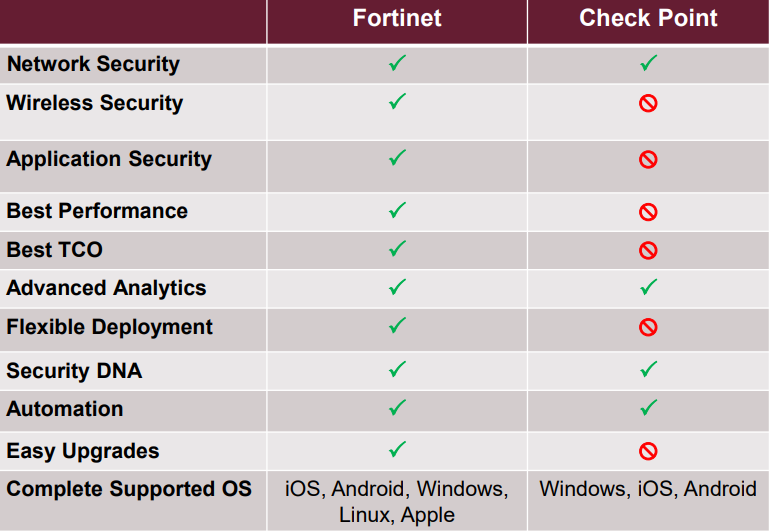


Рис. 2.3 Аналіз конкурентів ринку України

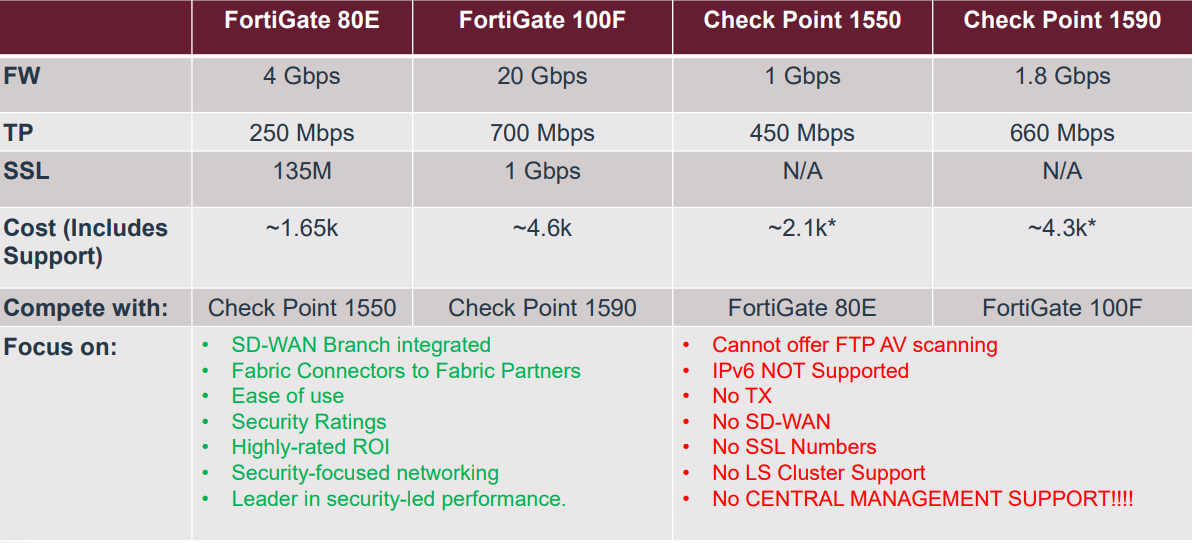


Рис. 2.4. Порівняння продуктів для малого бізнесу України

За результатами тестування ми можемо зробити однозначний висновок за найкращою ефективністю в порівнянні з конкурентними рішеннями.

У 2019 року пристрій FortiGate-600D зайняв лідируючу позицію у відвіданих лабораторіях NSS (рейтинг рекомендується) серед інших, вирішених у тестуванні NGIPS, показав найкращі знання про цінність захищеного обсягу інформації при максимальній ефективності захисту. Продукти CheckPoint показали більш високі показники вартості і уявлення про техніку обстеження.

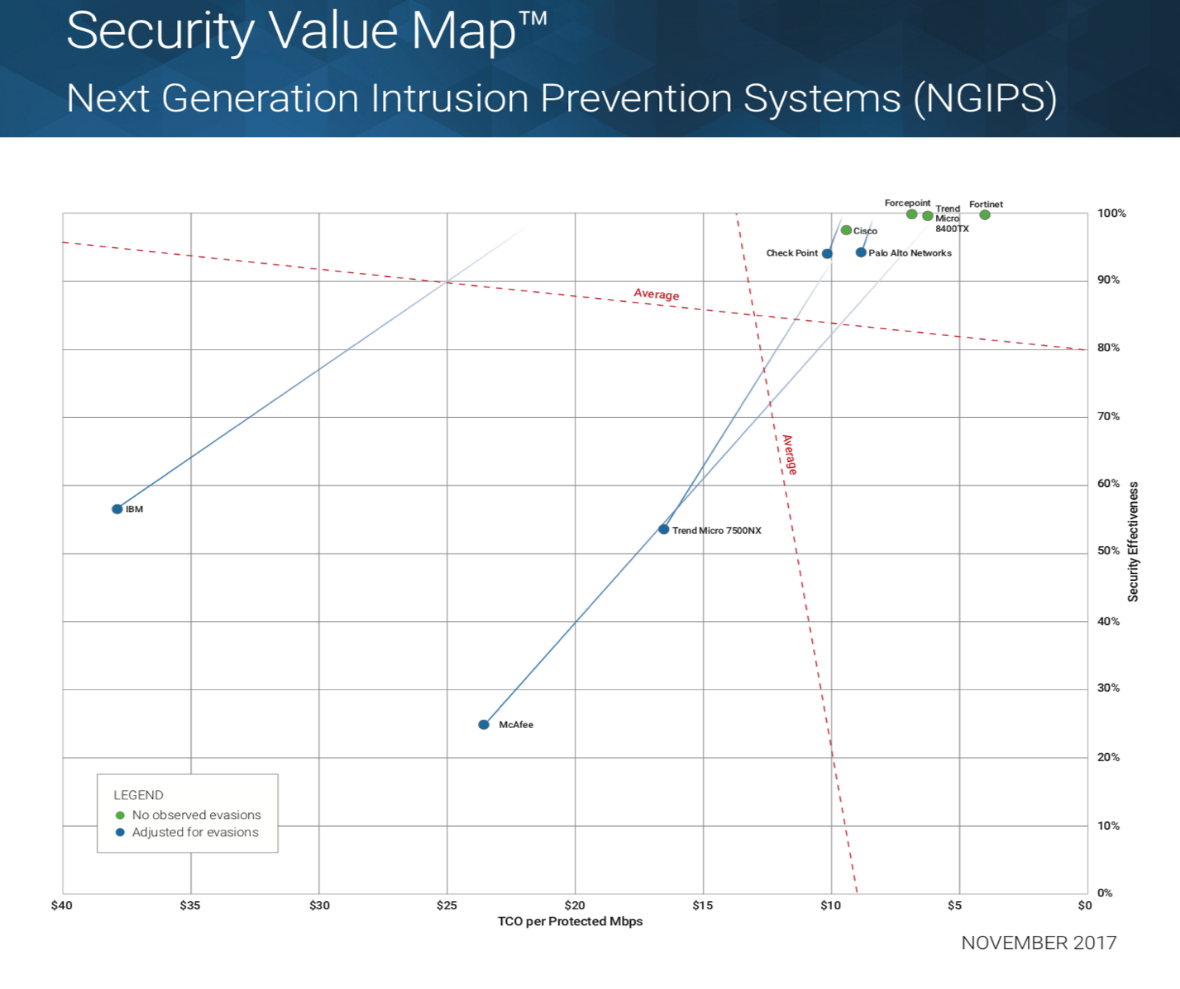


Рис. 2.5. Тестування NSS Labs МЕ наступного покоління

1. У липні 2018 року рішення FortiGate зайняло лідируючу позицію в звіті NSS Labs (рейтинг Recommended) серед інших рішень в тестуванні NGFW, показавши краще значення за вартістю об'єкта до захищеної інформації. Продукти Check Point показали низькі показники ефективності захисту при максимальній на ринку вартістю володіння, а також проблеми з доступністю і стабільністю рішення при пікових навантаженнях.

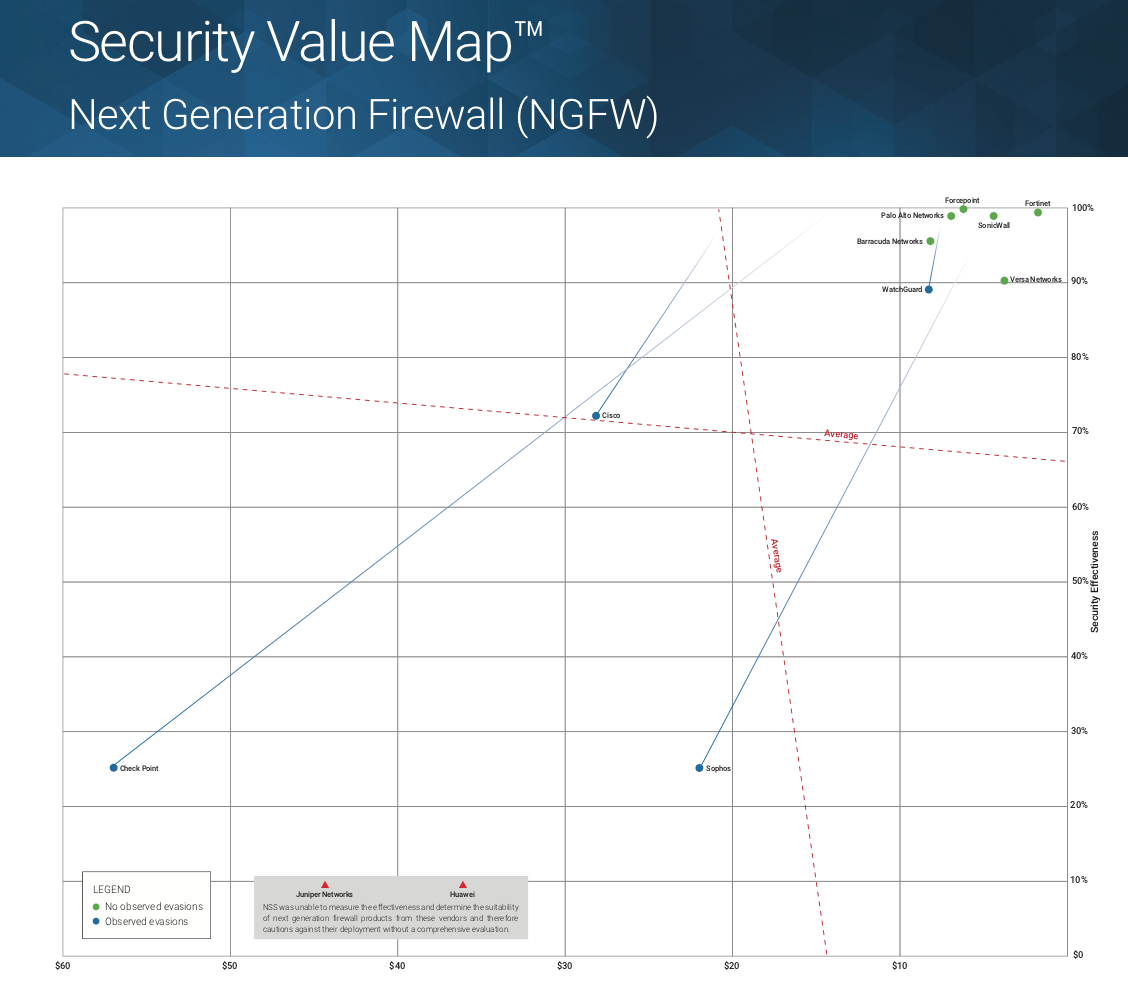
****

Рис. 2.6. Рейтинг NSS Labs

2. Ліцензування Check Point досить складне, передбачає облік і контроль кількості користувачів для деяких підписок (наприклад, для організації віддаленого захищеного доступу SSL VPN): чим більша кількість користувачів, тим вище кінцева вартість рішення. Сумарна вартість ліцензій Check Point може досягати більше половини вартості продуктів.

Багатофункціональні рішення FortiGate, на відміну від Check Point, не контролюють кількість користувачів рішення і не враховують їх у ліцензуванні, покладаючись тільки на продуктивність.

3.Закінчення дії підписок на рішеннях Check Point призводить до відмови працездатності багатьох сервісів, один з ключових елементів брандмауера - система виявлення вторгнень (IPS), повертається на сигнатурну базу 2009 року

Модулі рішень компанії Fortinet в разі закінчення дії підписки (наприклад, IPS) будуть працювати з сигнатурними базами на момент закінчення сервісу.

4.FortiGate - це програмно-апаратний комплекс, який використовує спеціалізовані ASIC. Рішення Check Point - це софтверний МЕ, який використовує Intel-архітектуру (тобто тільки центральний процесор CPU). Це призводить до помітного зниження продуктивності тестуванні (особливо при великій кількості політик безпеки).

5.Архітектура рішень Check Point призводить до великих втрат продуктивності на пакетах малих розмірів.

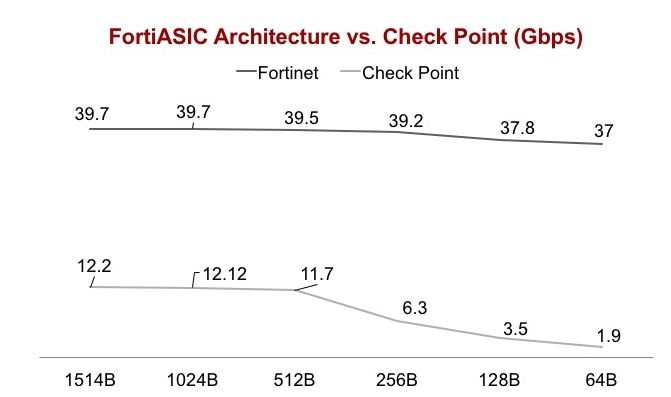
****

Рис. 2.7. Порівняння архітектури процесорів

6. Check Point демонструє високі показники по затриманню шкідливого ПЗ тільки в звіті компанії Miercom, яка готує платні звіти на замовлення.

7. Check Point підтримує обмежений набір архівів і глибини архівації, що призводить до низьких результатів в оцінках ефективності.

8. Check Point має низьку продуктивність при включенні SSL-інспекції трафіку, а також не підтримує інспекцію SSH-з'єднань, що потенційно може призвести до тунелюванні в SSH-сесіях нелегітимних додатків і трафіку.

9. Check Point не бере участі в дослідженнях лабораторії ICSA (network IPS, sandboxing, SSL, або AV / Malware).

*Таблиця 2.1*

Порівняння функціональних і технічних характеристик (на прикладі моделей FortiGate-1500D і Check Point 21700 Next Generation Firewall Appliance)

|  |  |  |
| --- | --- | --- |
| **Параметр** | **FortiGate-1500D UTM & 8x5 Bundle** | **Check Point 21700 Next Generation Firewall Appliance** |
| 1 | 2 | 3 |
| Пропускна здатність МЕ | 80 Гбіт/с | 78 Гбіт/с |
| Кількість одночасних з'єднань | 12 000 000 сесій | 6 000 000 |
| Максимальна кількість нових з'єднань в секунду | 300 000 сесій/с | 170 000 сесій/с |
| кількість пакетів | 82 500 000 пакетів/с | - |
| кількість політик | 100 000 | - |
| Пропускна здатність IPS / IDS (вхідного і вихідного трафіку) в режимі statefull packet inspection | 11 Гбіт/с | 8 Гбіт/с |
| Пропускна здатність IPSec VPN Throughput | 50 Гбіт/с | 11 Гбіт/с |
| Максимальна кількість IPSec-тунелів між VPN-шлюзами | 10 000 | - |
| Вноситься затримка системою Firewall в переданий потік даних | 3 мкс | - |
| Кількість розпізнаються додатків | Більше 5800 правил (3300 сигнатур додактів) | 5900 сигнатур |
| продуктивність антивірусу | 4.3 Гбіт/с | - |
| WAN-оптимізація | Так | Відсутній |
| функції DLP | Так | Отдельная лицензия |
| Контент-фільтрація | 78 категорій, власна база URL | 130 категорій |
| SSL VPN | Так | Окрема ліцензія |
| контролер WiFi | Так | Відсутній |
| Кількість керованих точок доступу (CAPWAP) | 1024 | - |

*Продовження табл 2.1*

|  |  |  |
| --- | --- | --- |
| 1 | 2 | 3 |
| Проізводетельность CAPWAP (HTTP) | 12.30 Гбіт/с | - |
|  |  |  |
| Віртуальні контексти | До 250 | До 150 |
| локальна пам'ять | 240 GB SSD | 2x500 HDD |
| Інтерфейси, розмір | 2U rack mount  8x10G SFP+,  16x1G SFP,  16x1G RJ-45,  2xGE RJ45 Management | 2U rack mount  до 13x10G SFP+,  12x1G SFP,  12x1G RJ-45,  2xGE RJ45 Management |
| порти USB | 1 | 1 |
| відмовостійкість | Так | Так |
| Резервне джерело живлення | Так | Так |

В результаті рішення Fortinet володіють наступними ключовими перевагами:

* Ефективність - найкраща за результатами тестів, всі захисні заходи (модулі, сигнатури) власної розробки;
* Висока продуктивність апаратних платформ за рахунок застосування ASIC, найширша підтримка віртуальних інфраструктур;
* Широкий спектр засобів захисту, можливість реалізації комплексного підходу до захисту мережі, в тому числі і від загроз нульового дня;
* Краща вартість володіння.

## 2.6 Висновок до розділу

**Поява великої кількості вразливостей, технік експлуатації привели до розуміння того, що потрібно міняти саму концепцію безпеки. Міжмережеві екрани не можуть забезпечити гарантований захист на кордоні мережі, оскільки постійно зростає число точок входу в мережу, а кордони мереж досить умовні. Виходячи з цього виникає концепція недовіри, що поклала початок автоматизації компонентів безпеки. Платформа Fortinet Security Fabric розроблена для забезпечення масштабованої і взаємозалежної безпеки в поєднанні з високою обізнаністю про загрози і відкритими стандартами API для захисту навіть найвимогливіших корпоративних середовищ. Технології безпеки Fortinet зарекомендували себе як ефективні та продуктивні в своїй галузі. Взаємопов'язані рішення Fortinet через Fortinet Security Fabric дозволяють закрити прогалини в захисті, залишені застарілими засобами захисту і платформами безпеки, забезпечуючи широке охоплення, потужний захист без шкоди для продуктивності мережі і автоматичне прийняття інтелектуальних дій.**

### Розділ 3.РЕАЛІЗАЦІЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

## 3.1. Характеристика та аналіз програмно-апаратних засобів для створення автоматизованої системи захищеної мережі.

Перш за все була обрана плафторма для безпечної емуляції мережі – VmWare Workstation Pro. Це [гіпервізор](https://uk.wikipedia.org/wiki/%D0%93%D1%96%D0%BF%D0%B5%D1%80%D0%B2%D1%96%D0%B7%D0%BE%D1%80) компанії [VMware](https://uk.wikipedia.org/wiki/VMware) для платформ [x86](https://uk.wikipedia.org/wiki/X86) і [x86-64](https://uk.wikipedia.org/wiki/AMD64), що дозволяє запустити на комп'ютері декілька [операційних систем](https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) одночасно. Кожна [віртуальна машина](https://uk.wikipedia.org/wiki/%D0%92%D1%96%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0) може виконувати свою власну операційну систему, включаючи [Microsoft Windows](https://uk.wikipedia.org/wiki/Microsoft_Windows), [Linux](https://uk.wikipedia.org/wiki/Linux), [BSD](https://uk.wikipedia.org/wiki/BSD) і [MS-DOS](https://uk.wikipedia.org/wiki/MS-DOS). VMware Workstation розроблений компанією VMware Inc., підрозділом корпорації [EMC](https://uk.wikipedia.org/wiki/EMC).

VMware Workstation підтримує з'єднання дійсних мережевих хостів та обміну фізичних дисків і USB пристрої з віртуальною машиною. Крім того, за допомогою VMware Workstation можна імітувати образи дисків. Можна змонтувати файл ISO у віртуальний привід оптичних дисків, так що віртуальна машина побачить його як реальний диск.

У VMware Workstation є можливість призначати кільком віртуальним машинам команди, які потім можуть бути запущені, закриті, перервані або відновлені як єдиний об'єкт, що робить її особливо корисною для тестування клієнт-серверних середовищ

Також на базі підприємства розгорнут корпоративний гіпервізор VmWare ESXI.

За рахунок консолідації кількох серверів на меншій кількості фізичних

пристроїв ESXi допомагає вивільнити простір, знизити енергоспоживання і оптимізувати ІТ-адміністрування, а також значно підвищити продуктивність. Гіпервизор ESXi володіє широкими можливостями, але при цьому займає всього 150 Мбайт на диску, що допомагає максимально захистити його від погроз безпеки. Гіпервизор підтримує програми будь-якого розміру завдяки можливості розгортати потужні віртуальні машини (до 128 віртуальних ЦП, 6 Тбайт ОЗУ і 120 пристроїв) для відповідності потребам різних додатків. Вивчіть рекомендовані параметри для окремих рішень, щоб не виходити за рамки підтримуваних конфігурацій для вашої середовища.

Потужні можливості шифрування для захисту конфіденційних даних на віртуальних машинах. Доступ на основі ролей для оптимізації адміністрування; розширені можливості аудиту і ведення журналів для більш прозорої звітності та полегшення ретроспективного аналізу. Велика екосистема забезпечує підтримку OEM-постачальників, партнерів по технологіям, додатків і гостьових операційних систем. Сучасний інтегрований інтерфейс на основі стандартів HTML5 для підтримки повсякденного адміністрування. Замовникам, яким потрібно автоматизувати процеси, VMware пропонує інтерфейс командного рядка vSphere і зручні для розробників API-інтерфейси на основі REST.

В цілому архітектура виглядає так:

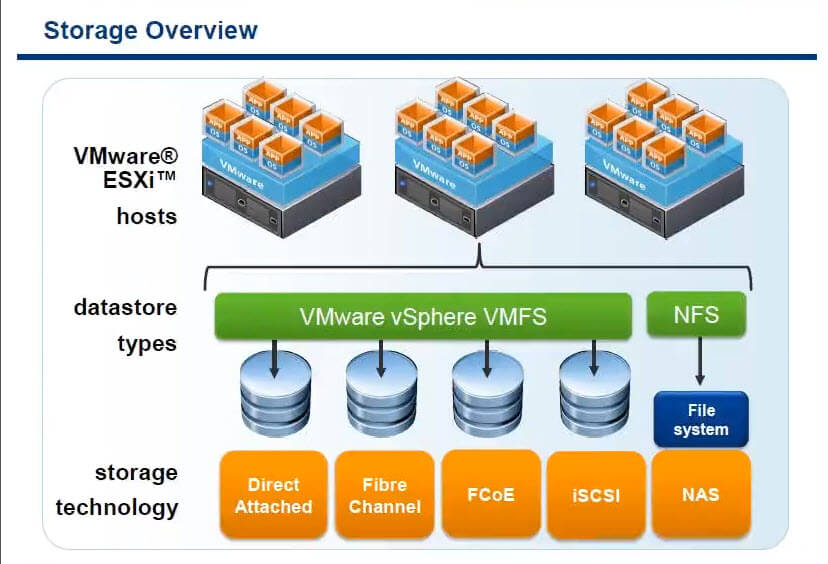


Рис. 3.1. Архітектура ESXI

Наступним кроком були обрані компоненти створення автоматизованої системи інформаційної безпеки. Серед них:

1. Міжмережевий екран Fortinet Fortigate VM02;
2. Програмний комплекс захисту від загроз нульового дня Fortinet FortiSandbox VM00;
3. Програмний комплекс інтегрованого захисту від складних загроз Fortinet FortiDeceptor;
4. Програмний комплекс звітування та логування інформаційних інцидентів Fortinet FortiAnalyzer VM02;

## 3.1.1 Характеристика міжмережевого екрана FGVM

FortiGate - пристрій комплексної мережевої безпеки. Містить в собі функціонал L2 / L3 маршрутизатора, брандмауера, VPN-концентратора, антивіруса, антиспам-фільтра, web / content фільтра, системи виявлення вторгнень (IPS), а також додатково функції авторизації користувачів, віртуалізації і забезпечення відмовостійкості рішень.

Маршрутизація - пристрій підтримує статичну, динамічну маршрутизацію (RIP, OSPF, BGP), маршрутизацію на вимогу (policy-based routing), а також маршрутизацію multicast-трафіку.

Брандмауер (Firewall) - на основі політик, які можуть гнучко настроюватися персонально під кожного користувача в мережі в залежності від напрямку руху трафіку.

Аутентифікація користувачів - пристрій підтримує функціонал аутентифікації користувачів перед наданням мережевих сервісів. Підтримується локальна база користувачів, взаємодія із зовнішніми системами аутентифікації по протоколах LDAP, RADIUS, TACACS +. При наявності в інфраструктурі серверів аутентифікації користувачів (таких, як контролер домену Windows Active Directory і Novell eDirectory), за допомогою технології Fortinet Single Sign-On, FortiGate має можливість виконувати одноразову аутентифікацію користувачів при їх доступі до корпоративних ресурсів мережі і / або мережі Інтернет ( наприклад, сервера додатків, розмежування доступу до ресурсів Інтернет).

VPN-концентратор - дозволяє встановлювати захищені з'єднання між мережевими локаціями з інтеграціям протоколів IPSec (Site-to-site, Hub-and-spoke, Dialup client), SSL (web-portal mode, tunnel mode), PPTP, L2TP. Підтримуються алгоритми шифрування DES, 3DES, AES.

Антивірус і протидія шкідливому ПО - дозволяє в режимі реального часу перевіряти на наявність вірусів і шкідливого коду: веб-трафік (HTTP, HTTPS), FTP, електронну пошту (SMTP, POP3, IMAP), протоколи обміну миттєвими повідомленнями (ICQ, AIM , MSN, Yahoo та ін.), P2P, протокол передачі новин (NNTP), і все це з підтримкою більшості популярних форматів стиснених файлів. Антивірусні сигнатури оновлюються автоматично з серверів Fortinet (існує PUSH механізм оповіщення про вихід нових сигнатур). Є механізм евристичного аналізу (пошук невідомих вірусів).

Антиспам - перевірка електронної пошти (SMTP, POP3, IMAP) на наявність спаму. Ефективне тестування різних параметрів електронної кореспонденції, білий / чорний листи IP-адрес і e-mail адрес відправників / одержувачів. Запобігання витоку інформації (список заборонених фраз). Перевірка репутації відправника в глобальній базі репутацій Fortinet. Сигнатурний аналіз кореспонденції.

Система запобігання вторгнень (IPS) - система виявлення і запобігання вторгнень на базі власної служби FortiGuard Intrusion Prevention Service. Сигнатурний аналіз трафіку, відстеження та аналіз аномалій трафіку, можливість створення власних сигнатур, визначення нових вторгнень, на які сигнатури ще не створені, автоматичне оновлення бази даних сигнатур.

WEB / контент фільтр - забезпечення корпоративної політики інтеграція інтернет користувачами компанії (аналітика сайтів за допомогою глобальної бази даних класифікації та репутації інтернет сайтів FortiGuard Web Filtering service), перевірка заголовків і вмісту WEB-трафіку, управління Java-апплетами, ActiveX-компонентами, Cookies .

Контроль додатків - FortiGate має функціонал контролю програм (веб-пошта, програми обміну миттєвими повідомленнями (IM), безкоштовні VoIP-дзвінки, P2P, панелі інструментів браузерів, обмін файлами, а також різні соціальні медіа-ресурси), протоколів передачі голосу крізь IP (H.323, SIP, SCCP). Бази даних ідентифікації додатків FortiGate в даний час містять більше 1500 сигнатур для додатків і протоколів по 18 категоріям.

Traffic shaping - пристрій має функції управління потоком трафіку (гарантування / лімітування / пріоритетність смуги пропускання).

NAT і балансування навантаження - підтримуються розвинені функції перетворення адрес (динамічний і статичний NAT, policy-based NAT, SIP / H.323 NAT-Traversal), також є функції балансування навантаження між декількома серверами.

Protection profile - дозволяє призначити (включити) набір сервісів безпеки персонально для кожного типу трафіку або користувача в мережі.

VDOM (Virtual Domain) - віртуалізація пристрою. Створення декількох віртуальних пристроїв з незалежним управлінням, політиками безпеки, таблицями маршрутизації для кожного. Активовано 10 VDOM-ліцензій в базовій поставці, можливе розширення кількості ліцензій.

HA (high availability) - режим спільної роботи двох пристроїв для підвищення відмовостійкості мережі. Підтримуються Active / Active, Active / Passive, VRRP режими.

IPv6 - продукт підтримує протокол IPv6.

VLAN - підтримуються VLAN 802.1q.

3G - пристрій працює із зовнішніми 3G або CDMA модемами в форм-факторі USB.

Управління та моніторинг може здійснюватися за допомогою ПЗ FortiAnalyzer.

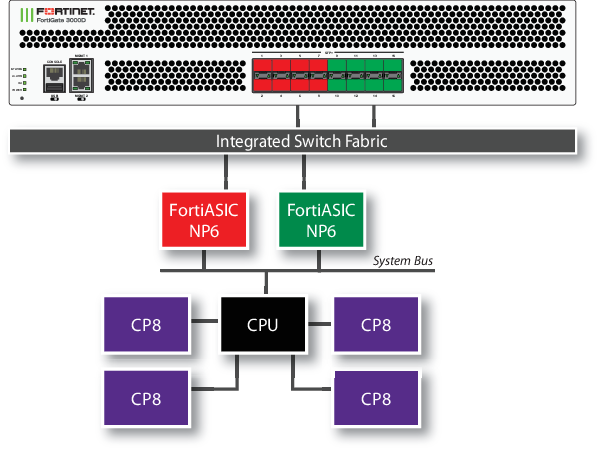


Рис. 3.2. Архітектура міжмережевого екрану Fortigate

## 3.1.2 Характеристика комплекса захисту від загроз нульового дня

FortiSandbox використовує систему емуляції коду для розкриття поведінки і виявлення невідомих складних загроз і цілеспрямованих атак. Для оцінки загрози виконуваних файлів, стислих файлів (ZIP-файлів) і широкого набору файлів додатків (таких як Adobe Flash, Adobe PDF, JavaScript і т. Д.) FortiSandbox використовує віртуальні машини, оснащені інструментами, емулює типову робоче середовище (операційні системи і програмне забезпечення). FortiSandbox підтримує можливість створення власних образів, що включають конкретне програмне забезпечення, що використовується замовником. Оскільки перевірка кожного файлу в ізольованому середовищі - ресурсномістка і довгострокове завдання, здатна обмежити загальне число оцінених підозрілих файлів і значно знизити продуктивність, то перед виконанням в FortiSandbox підозрілі файли піддаються попередній фільтрації: виконується антивірусне сканування (AV Engine) і робиться запит до хмарного сервісу FortiGuard (Cloud Query). Якщо в ході попередньої перевірки наявність або відсутність загрози з боку файлу не ідентифіковано, то зразок файлу передається для подальшого аналізу в віртуальну "пісочницю" (Full Virtual Sandbox), що включає емуляцію коду. Якщо зразок виявляється шкідливим, то FortiSandbox (при наявності відповідної настройки) завантажує дані про шкідливу програму в FortiGuard Labs, які будуть проаналізовані фахівцями і в кінцевому підсумку увійдуть в оновлення продуктів Fortinet для всіх користувачів.

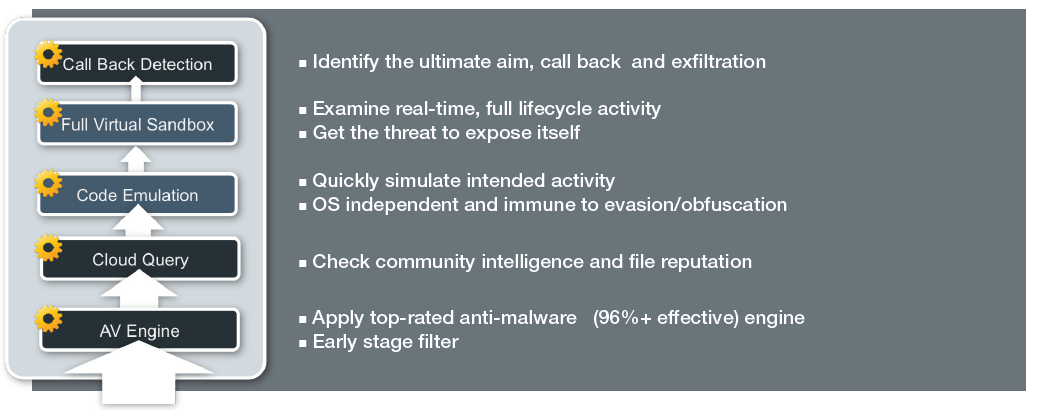


Рис. 3.3. Технології визначення загроз

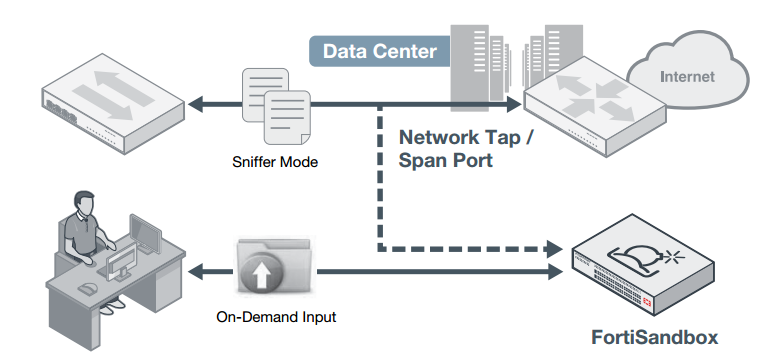


Рис.3.4. Ізольований режим роботи

При використанні FortiSandbox в розподілених мережах міжмережеві екрани FortiGate розгортаються в філіях організації і відправляють підозрілі файли центрального пристрою FortiSandbox. Така інтеграція дозволяє захистити від загроз віддалені сегменти мережі при низькій сукупній вартості.

## 3.1.3 Характеристика комплексу інтегрованого захисту від складних загроз

Рішення FortiDeceptor доповнює існуючу корпоративну систему захисту від порушень. В його основі лежить маскувальна технологія, завданням якої є запровадження зловмисників в оману, а також виявлення та усунення зовнішніх і внутрішніх атак до того, як вони стануть причиною реального збитку.

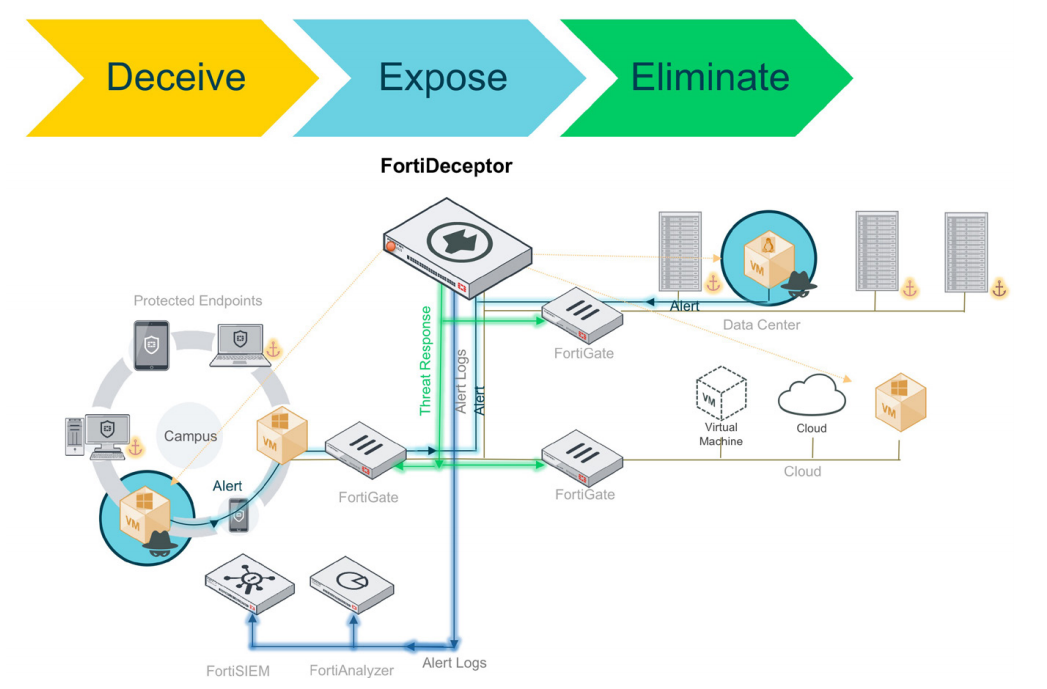


Рис. 3.5. Схема роботи системи протидії загроза 0 дня

За допомогою рішення FortiDeceptor організація може оперативно створити маскувальну мережу. Процедура полягає в автоматичному розгортанні віртуальних машин маскування і пасток, які вбудовуються в існуючу інфраструктуру і служать для виявлення зловмисників шляхом введення їх в оману. Завдяки ефективній технології виявлення загроз, яка зіставляє відомості про активність зловмисника і рухах в горизонтальній площині, рішення FortiDeceptor виконує функції завчасного оповіщення про більш масштабні атаки. Дані про загрози, отримані в ході відстеження дій зловмисника, автоматично передаються внутрішніх компонентів безпеки для блокування атак до того, як вони стануть причиною збитку.

## 3.1.4 Характеристика комплексу звітування та логування інформаційних інцидентів

FortiAnalyzer збирає, аналізує і реєструє дані про події з пристроїв мережевої безпеки Fortinet або syslog-сумісних пристроїв. Використовуючи набір легко змінюваних шаблонів звітів, можна відфільтрувати і оцінити події за різними параметрами, включаючи трафік, події, вірус, атаку, web-контент, і вміст поштових повідомлень - з метою визначення стану безпеки системи і її відповідність нормативним актам і стандартам.

Журнали подій - збір і зберігання журналів подій від пристроїв, агентів, груп пристроїв / агентів, таких як FortiGate, FortiMail, FortiClient, складання різноманітний звітів, які дозволяють стежити за станом мережевий середовища і оперативно реагувати на порушення правил роботи з мережевою інфраструктурою.

Інтелектуальний аналіз даних - інтерфейсу FortiAnalyzer, дозволяють адміністраторам проаналізувати заархівовані журнали подій, щоб відстежити дії користувачів на підставі імен користувачів, адрес електронної пошти, трафіку миттєвих повідомлень при розслідуванні інцидентів порушення інформаційної безпеки.

Централізований карантин - ізолювання заражених або підозрілих файлів, що входять в Вашу мережу в одному центральному сховищі. Має можливість перегляду файлів, поміщених в карантин. Особливо актуально для пристроїв FortiGate, не оснащених жорсткими дисками.

Мережевий аналізатор - інструмент для аналізу мережі, працює за принципом «перехоплення пакетів», перехоплені пакети зберігаються для подальшого аналізу.

Сканер вразливостей - інтегрований сканер вразливостей ідентифікує вразливість на РС або серверах, таких як поштовий сервер, файловий сервер, або інші сервера під керуванням UNIX або Windows, генерує звіти про вразливості вибраного пристрою.

Вбудований Syslog сервер - підтримується можливість інтеграції з third-party пристроям обмінюватися даними протокол Syslog.

Масштабованість - два режими роботи Analyzer і Collector, що забезпечують гнучкість і масштабованість мережі з великою кількістю пристроїв.

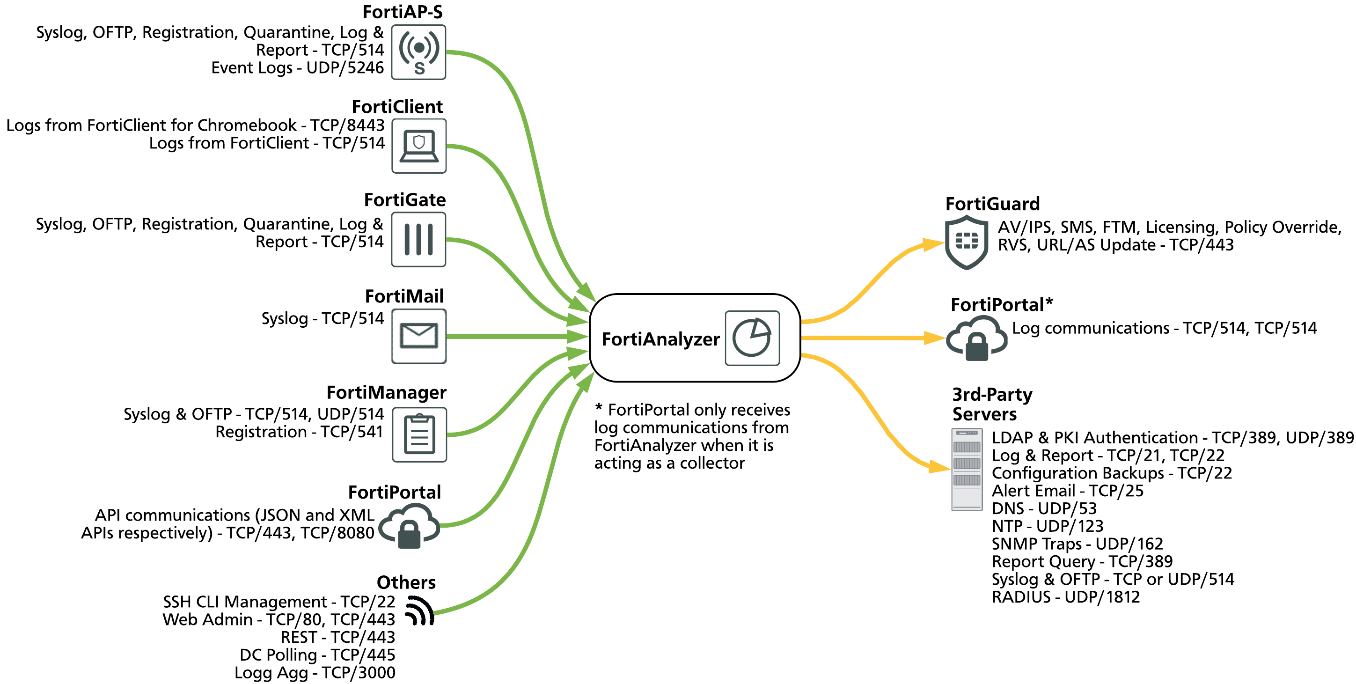


Рис. 3.6. Схема роботи комплексу протидії складним загрозам

## 3.2 Встановлення та нлаштування віртуальних пристрорїв

Під мережеву інфраструктуру підприємства було обрано спеціалізовані ВМ, які мають певні технічні рекомендації, щодо серверу віртуалізації.

Процес починається з реєстрації програмного забезпечення на веб-сторінці виробника:

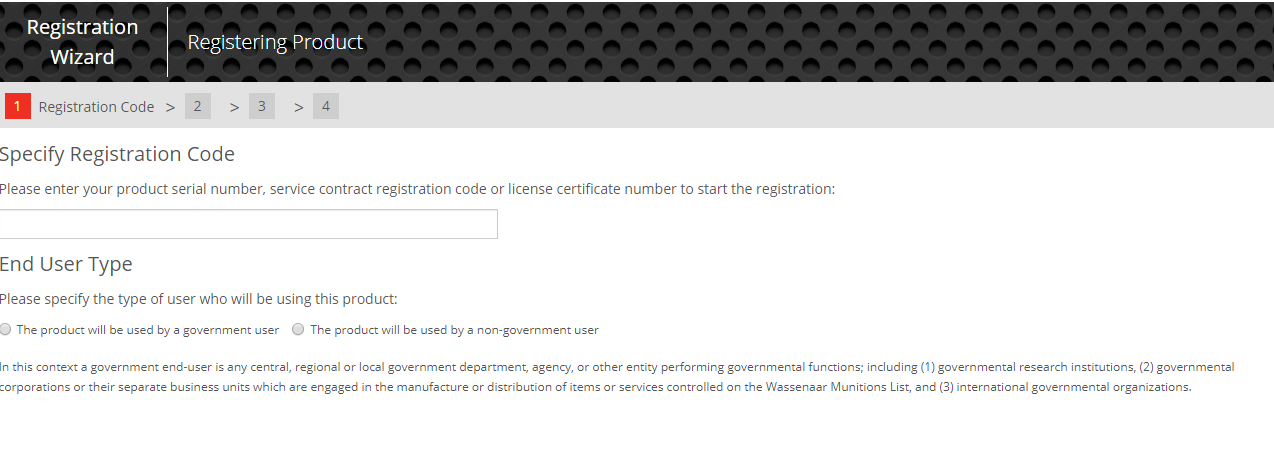


Рис. 3.7. Сторінка реєстрації ліцензій на ПЗ

Після реєстрації всіх віщезазначених продуктів, отримано актуальні ліцензії. Кожна ліцензія дозволяє користуватись спеціалізованим ресурсом Fortiguard.



Рис. 3.8. Сервіси Fortinet

Наступним кроком буде завантаження OVF шаблонів віртуальних машин. Кожен шаблон має рекомендовані параметри гіпервізора.

*Таблиця №3.1*

Кількісні характеристики ПЗ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Параметри | Fortigate | Analyzer | Sandbox | Deceptor |
| Пам'ять, Гб | 1 | 4 | 8 | 8 |
| Жорсткий диск, Гб | 32 | 82 | 201 | 201 |
| Кількість мережевих адаптерів | 10 | 4 | 6 | 6 |
| Кількість ядер процесора | 1 | 2 | 4 | 4 |

Після імпорту шаблонів, наступає процес ініціації ВМ (створення жорстких дисків, виділення пам’яті). Далі створюються віртуальні мережі, виглядає це настпуним чином:

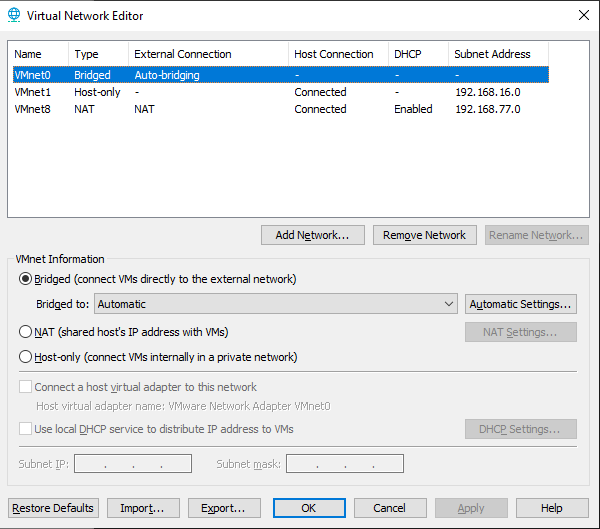


Рис. 3.9. Налаштування віртуальних мереж

Налаштовано декілька віртуальних мереж. Мережа VMnet1 використовується без трансляції NAT, тобто тільки локально. Мережа VMnet8 має вихід в інтернет для отримання оновлень та з’єднання з центром FortiGuard.

Наступний крок: первинне налаштування кожного програмного забезпечення.

При налаштуванні Fortigate, першим етапом є створення статичного маршруту, що дозволить МЕ доступ в інтернет:

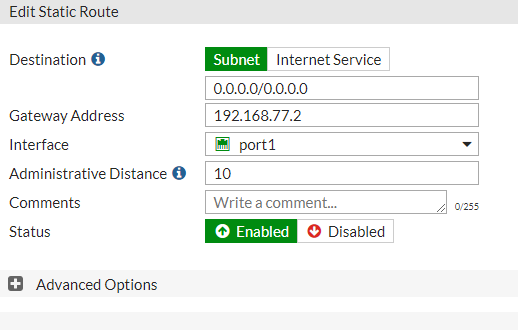


Рис. 3.10. Налаштування статичного маршруту доступу інтернет

Рис. 3.11. Перевірка доступності інтернету

Далі налаштовуємо для всіх інших ПАК статичний маршурт та робимо перевірку доступності інтернету:

|  |
| --- |
| Sydorov\_Yevhen\_FG # execute ping 1.1.1.1 |
| PING 1.1.1.1 (1.1.1.1): 56 data bytes |
| 64 bytes from 1.1.1.1: icmp\_seq=0 ttl=128 time=1.7 ms |
| 64 bytes from 1.1.1.1: icmp\_seq=1 ttl=128 time=2.5 ms |
| 64 bytes from 1.1.1.1: icmp\_seq=2 ttl=128 time=1.7 ms |
| 64 bytes from 1.1.1.1: icmp\_seq=3 ttl=128 time=1.5 ms |
| 64 bytes from 1.1.1.1: icmp\_seq=4 ttl=128 time=1.6 ms |
|  |
| --- 1.1.1.1 ping statistics --- |
|  |
| 5 packets transmitted, 5 packets received, 0% packet loss |
| round-trip min/avg/max = 1.5/1.8/2.5 ms |
|  |

Тепер стає можливим активування ліцензій для кожного ПАК, що дозволить інтеграція всіх модулів безпеки.

Ліцензії Fortinet Fortigate VM:

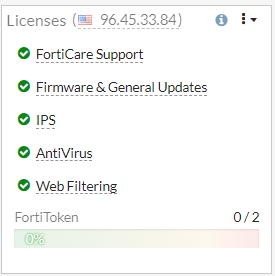


Рис.3.12. Перевірка статусу ліцензії Fortigate

Ліцензії Fortinet Sandbox VM:

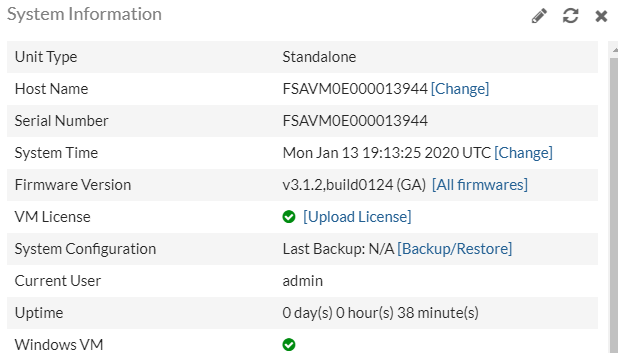


Рис. 3.13. Перевірка статусу ліцензії FortiSandbox

Ліцензії Fortinet Deceptor VM:

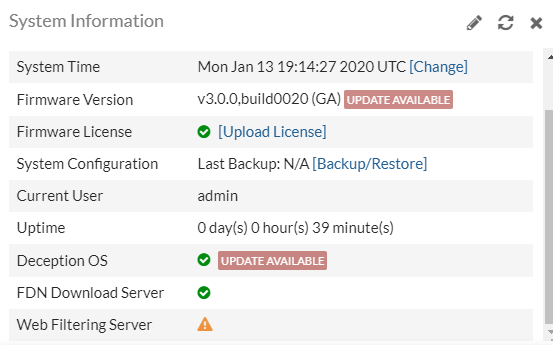


Рис. 3.14. Перевірка статусу ліцензії FortiDeceptor

Ліцензії Fortinet Analyzer VM:

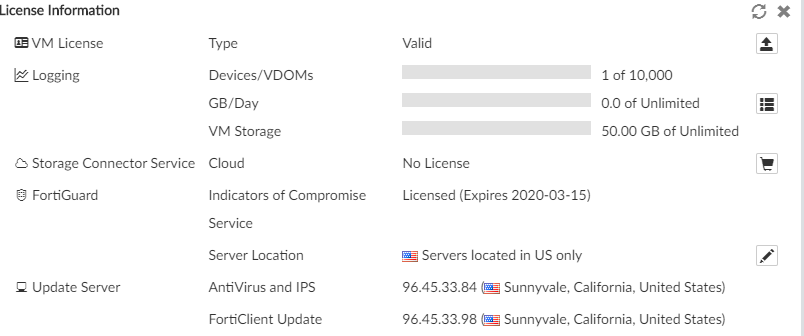


Рис. 3.15. Перевірка статусу ліцензії FortiAnalyzer

Наступним кроком буде конфігурація політик безпеки проходження трафіку крізь МЕ. Налаштовується наступним чином:

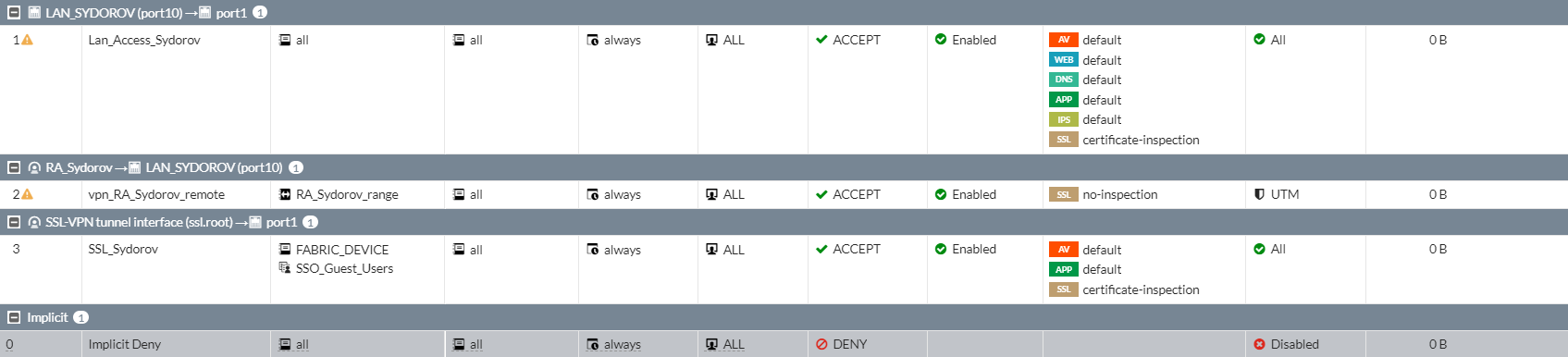


Рис.3.16. Налаштування політик

### 3.2. Налаштування інтеграції та автоматизації систем інформаційної безпеки

Після виконання первинних налаштувань міжмережевого екрану, системи протидії загрозам нульового дня, складним загрозам, звітування то логування – потрібно виконати інтеграцію. Єдина платформа має назву Fortinet Security Fabric.

Платформа побудована на основі 3 критеріїв:

* Всеосяжність. Fortinet Security Fabric покриває всю поверхню атак. При цьому адміністратори безпеки користуються видимістю всієї інфраструктури, включаючи кінцеві точки, пристрої IoT, точки доступу, мережеві елементи, центри обробки даних, хмари і навіть додатки і самі дані. Це дозволяє забезпечити захист всіх потенційних точок входу, а також сегментів всередині динамічної мережі. Таке широке розгортання і глибока видимість допомагає контролювати внутрішній трафік і пристрої, запобігає несанкціонованому доступу до обмежених даних і ресурсів та контролює поширення шкідливих програм і дій зловмисників.
* Потужність. Компоненти Fortinet Security Fabric розроблені на основі технології процесорів безпеки Fortinet (Security Processor Unit, SPU). Застосування спеціально розроблених процесорів безпеки значно підвищує продуктивність і масштабованість, запобігаючи вплив безпеки на пропускну здатність мережі і знижуючи навантаження на інфраструктуру.
* Автоматизація. Fortinet Security Fabric забезпечує швидке і скоординоване реагування на загрози. Платформа дозволяє автоматично визначити і динамічно ізолювати скомпрометовані пристрої, сегменти мережі, правила поновлення, відключити некоректні політики і видалити шкідливі програми. Fortinet Security Fabric також надає рішення для динамічної адаптації до змін конфігурації мережі, впровадження нових політик, оскільки зміни в бізнесі спричиняють зміни в ІТ-середовищі. Заходи безпеки і контрзаходи автоматично розгортаються в ході розгортання нових пристроїв, робочих навантажень і служб по всій інфраструктурі. Платформа також підтримує відкриті прикладні програмні інтерфейси (API), які дозволяють організаціям інтегрувати наявні засоби захисту і мережеві технології з Fortinet Security Fabric.

Налаштування інтеграції FortiGate з FortiAnalyzer. :

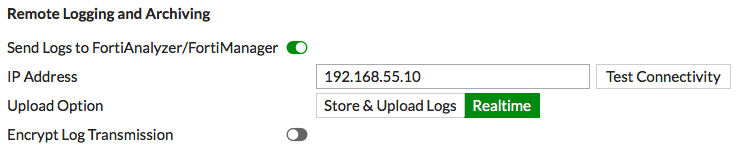


Рис.3.17. З’єднання міжмережевого екрану та логуючого пристрою

Далі підтверджуємо авторизацію з боку FortiAnalyzer та перевіряємо:

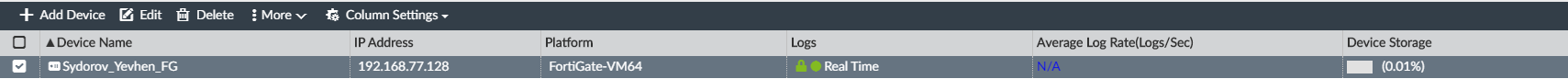


Рис. 3.18. Підтвердження авторизації міжмережевого екрану

Перевіряємо надходження логів та інформаційних інцидентів:

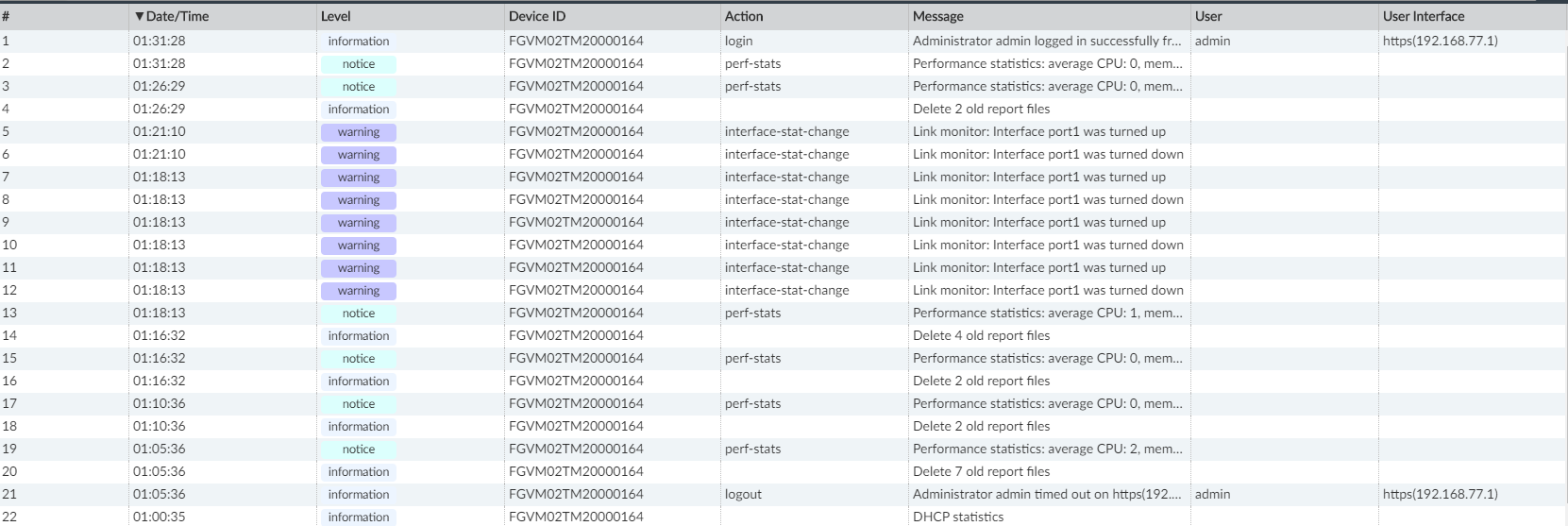


Рис. 3.19. Перевірка логування

Наступний крок, інтеграція міжмережевого екрану з системою протидії загрозам нульового дня. Для цього потрібно виконати авторизацію міжмережевого екрану на обладнанні FortiSandbox. Також потрібно налаштувати port1, port2, port3.

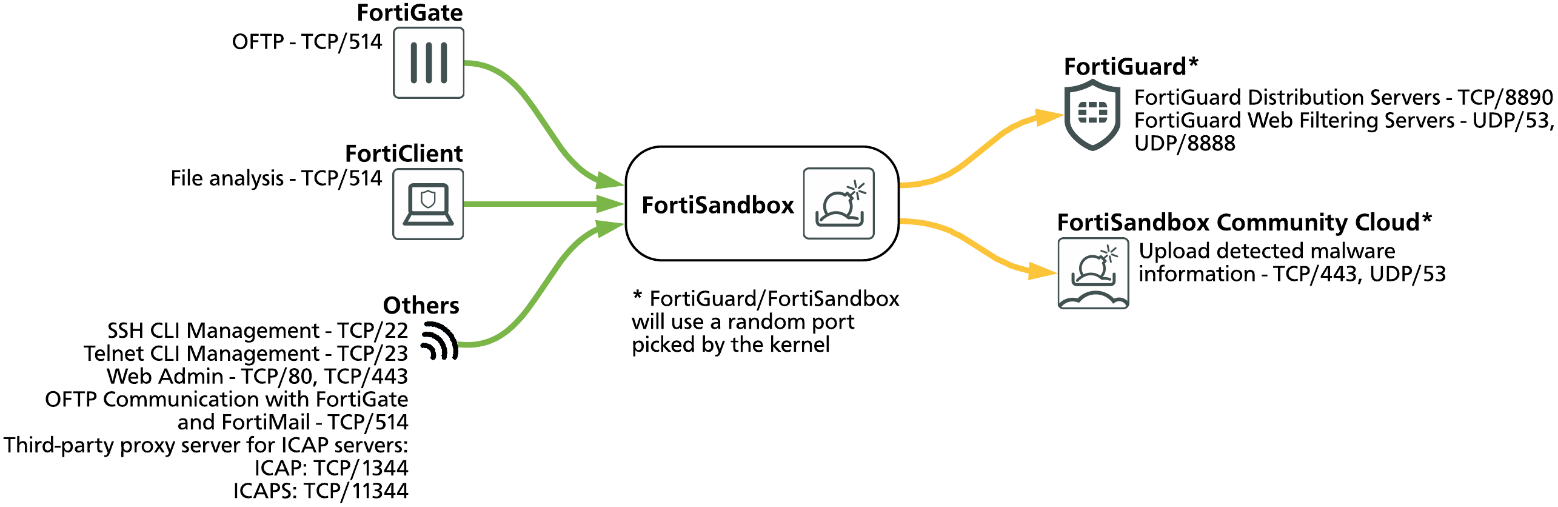


Рис. 3.20. Налаштування портів FortiSandbox

Далі налаштовуємо інтеграцію з системою протидії складним загрозам:

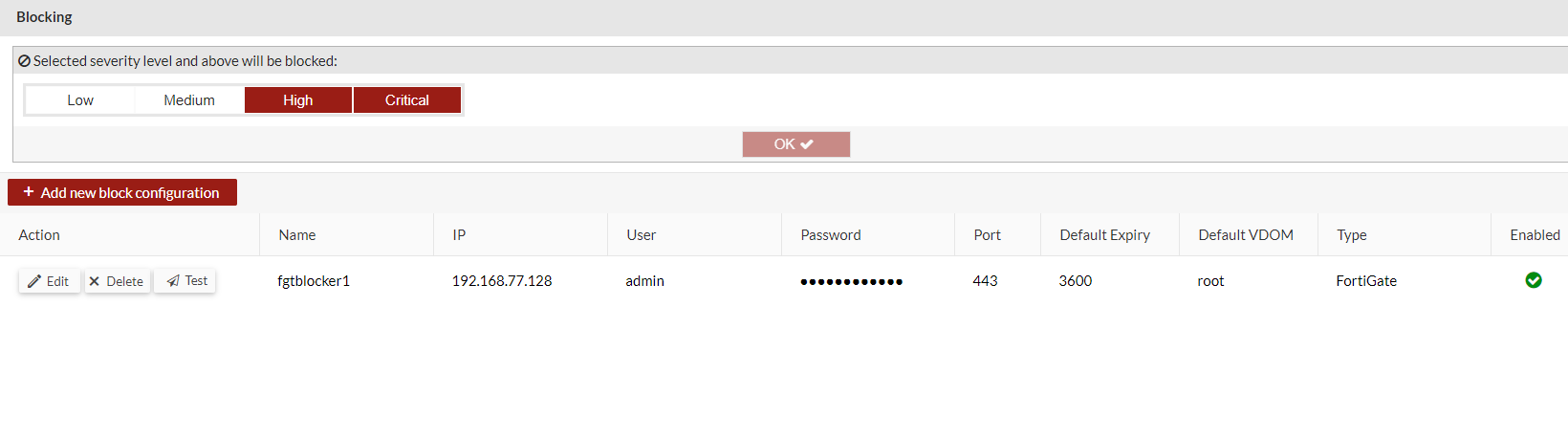


Рис. 3.21. Інтеграція с системою протидіїї складним загрозам

Наступним кроком буде створення пасток, як зображено нижче:

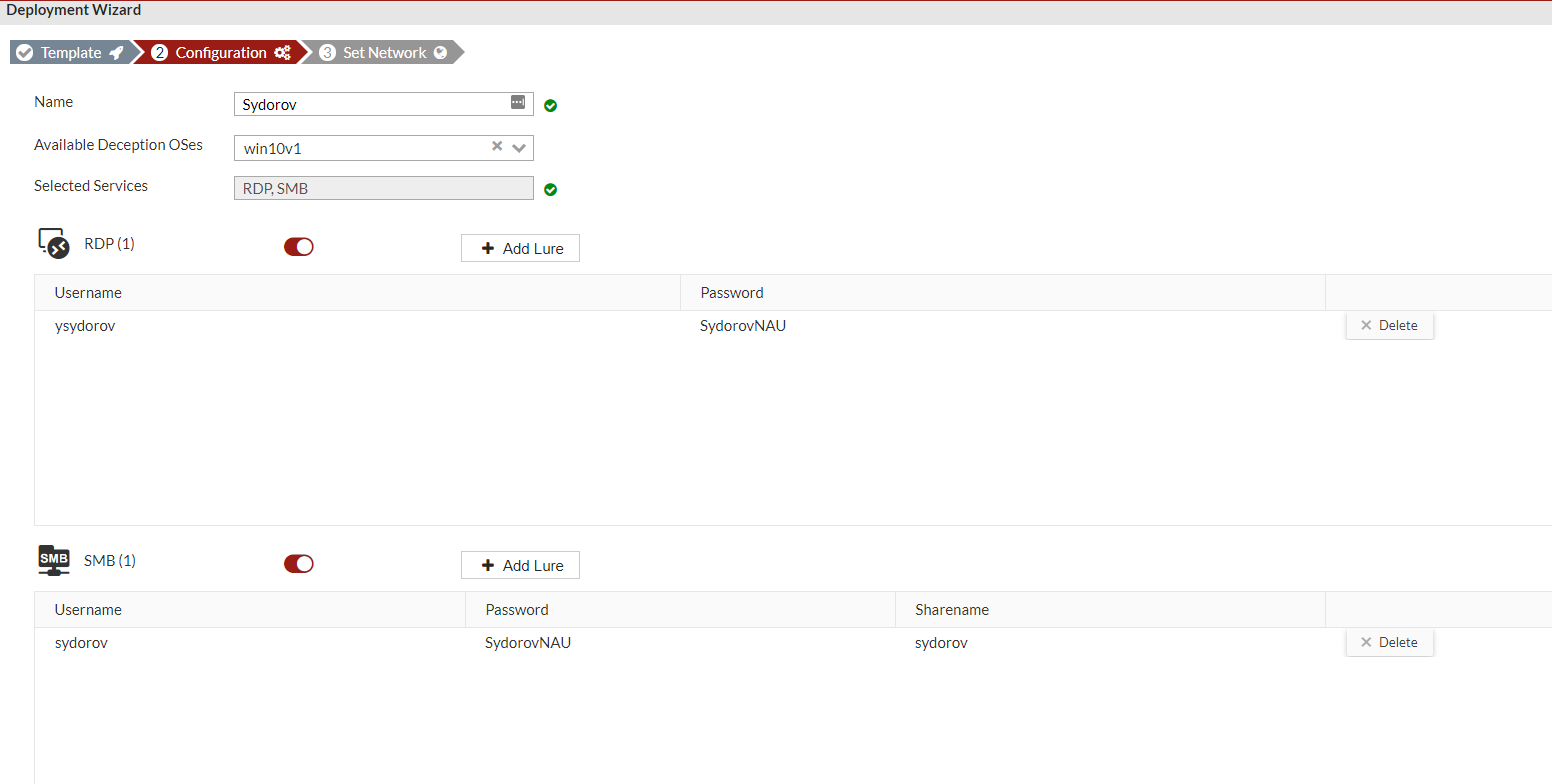


Рис. 3.22. Створення пасток

Після впровадження пасток, створюється мапа Deception:

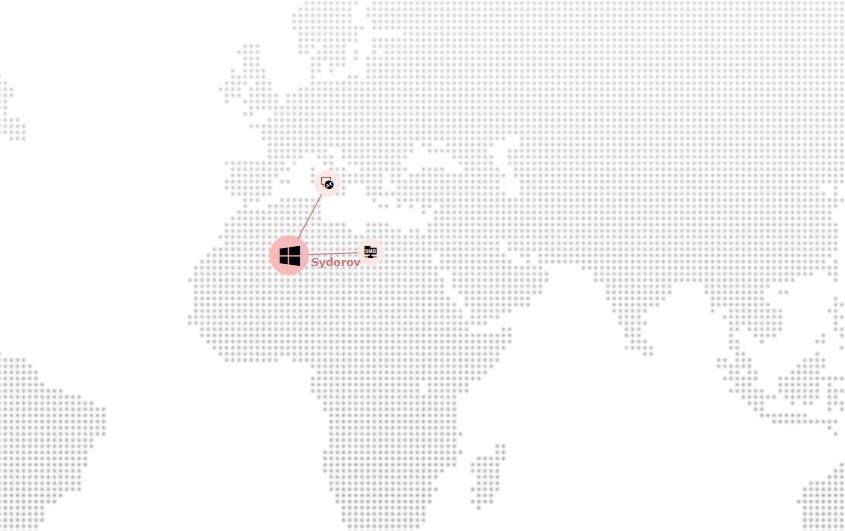


Рис. 3.23. Мапа пасток

Буде використовуватись наступна схема роботи:

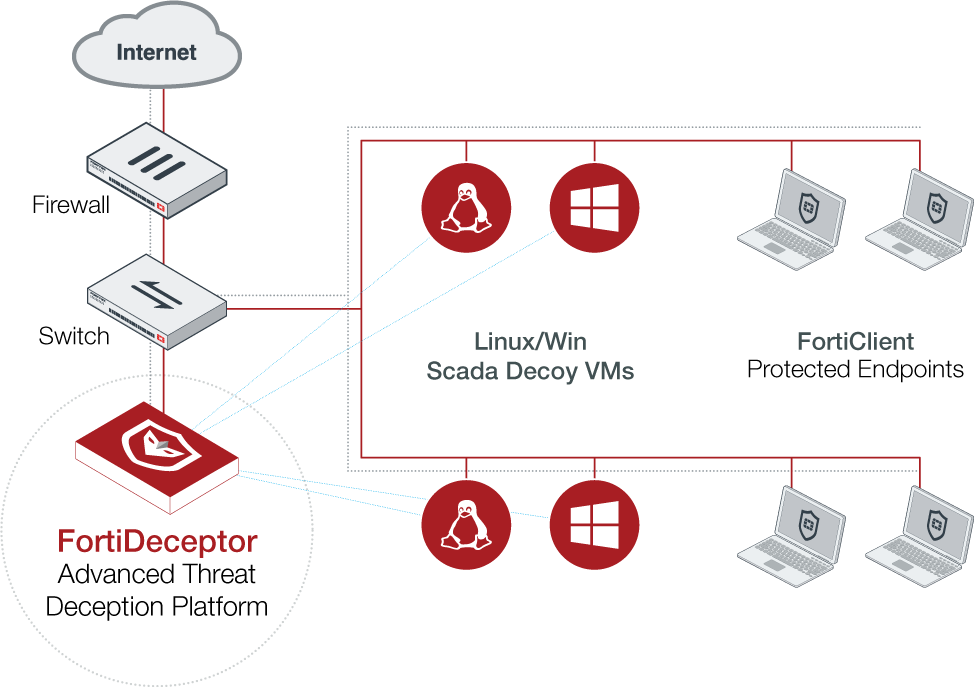


Рис. 3.24. Схема роботи системи пасток

Після інтеграцій пристроїв потрібно налаштувати автоматизацію фабрики безпеки. Для цього потрібно скористатись ядром мережі – FortiGate.

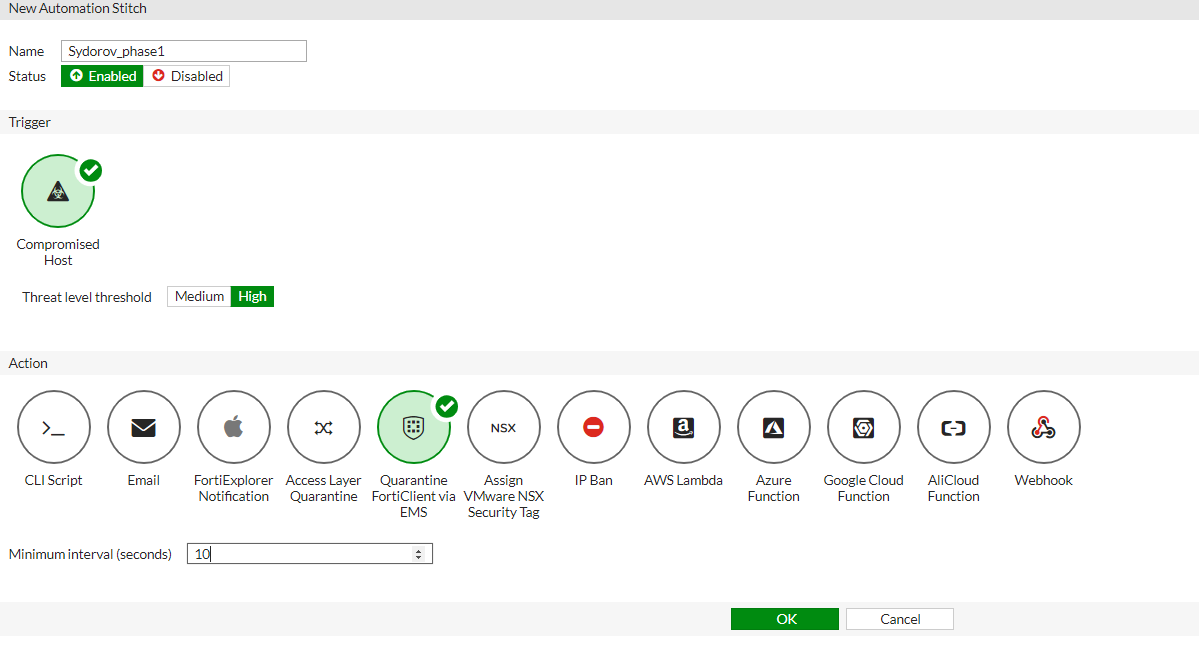
* Перший трігер: 

Рис. 3.25. Налаштування блокування хоста

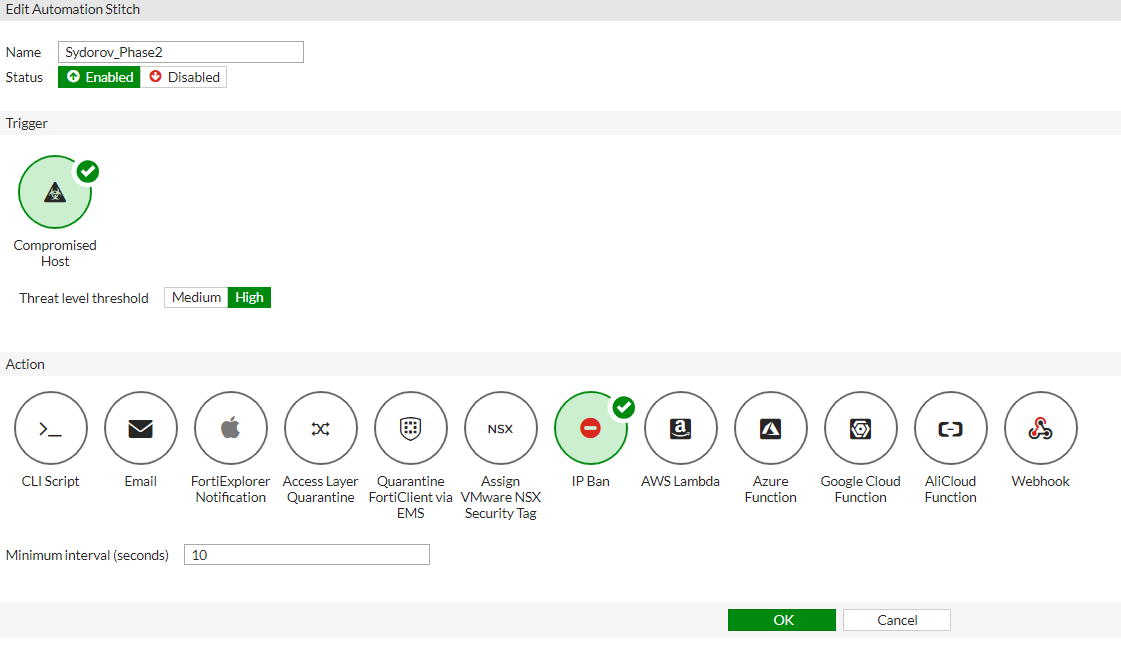
* Другий трігер: 

Рис. 3.26. Налаштування блокування IP-адреси

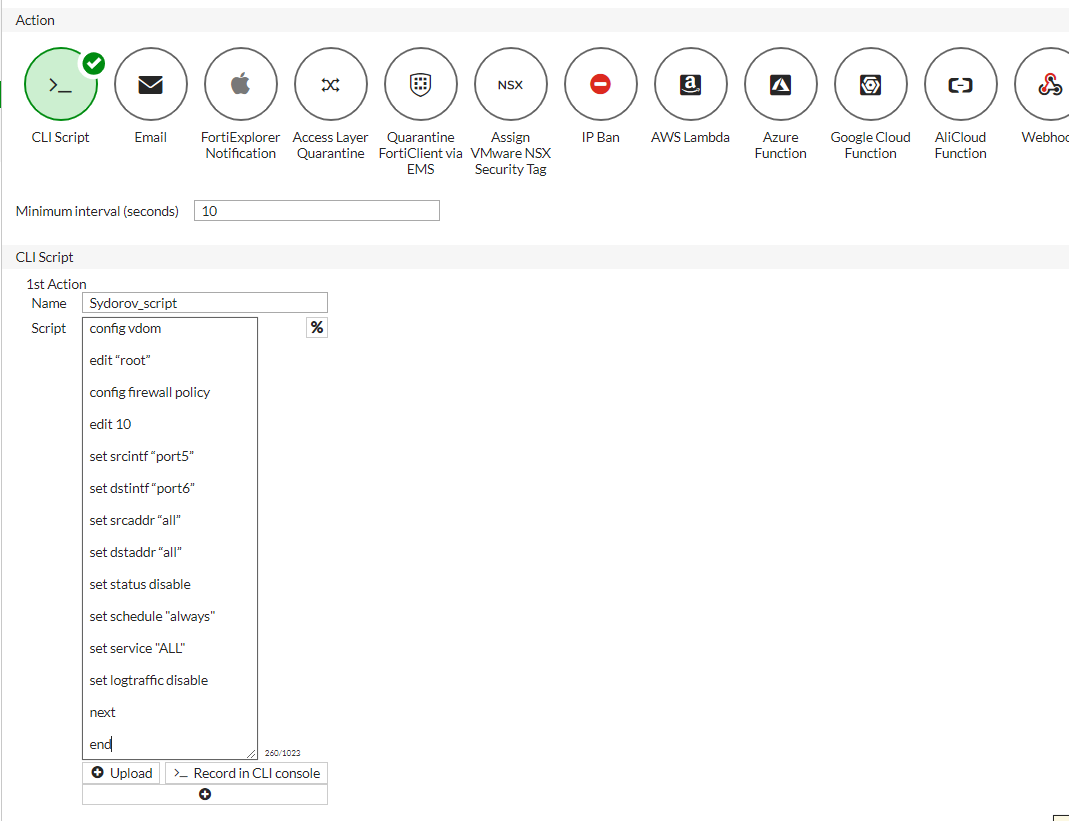
* Третій трігер: 

Рис. 3.27. Налаштування скрипту автоматизації

### 3.2. Створення програмного коду автоматизації безпеки

Так як Fortinet має відкритий API, то можна використати мову програмування Python для автоматизації дій. Був розроблений програмний код (див. Додаток А), що дозволяє створювати політики безпеки для всіх систем, які приймають участь у захисті. До впровадження спеціалізованих ПАК автоматизації процесів інформаційної безпеки кожен адміністратор витрачав багато часу на підключення до консолі адміністрування, з’ясування причин на наслідків інциденту, або навіть не з’ясовував. Задля того, щоб коректно встановити інцидент, потрібно було встановлювати взаємозв’язок та кореляцію інцидентів.

Після впровадження, потрібно лише увійти до однієї консолі, в якій буде зображено вектор атаки, логування та потрібні дії, щодо відновлення.

Розроблений програмний код дозволяє всім пристроям, що приймають участь ініціювати створення політик за допомогою компанда інтерфейсу API, крім того можливо власноруч розробити спеціалізовані плагіни для підключення сторонніх виробників, якщо потрібно.

Все це обробляється ядром інфраструктури Fortinet FortiGate:

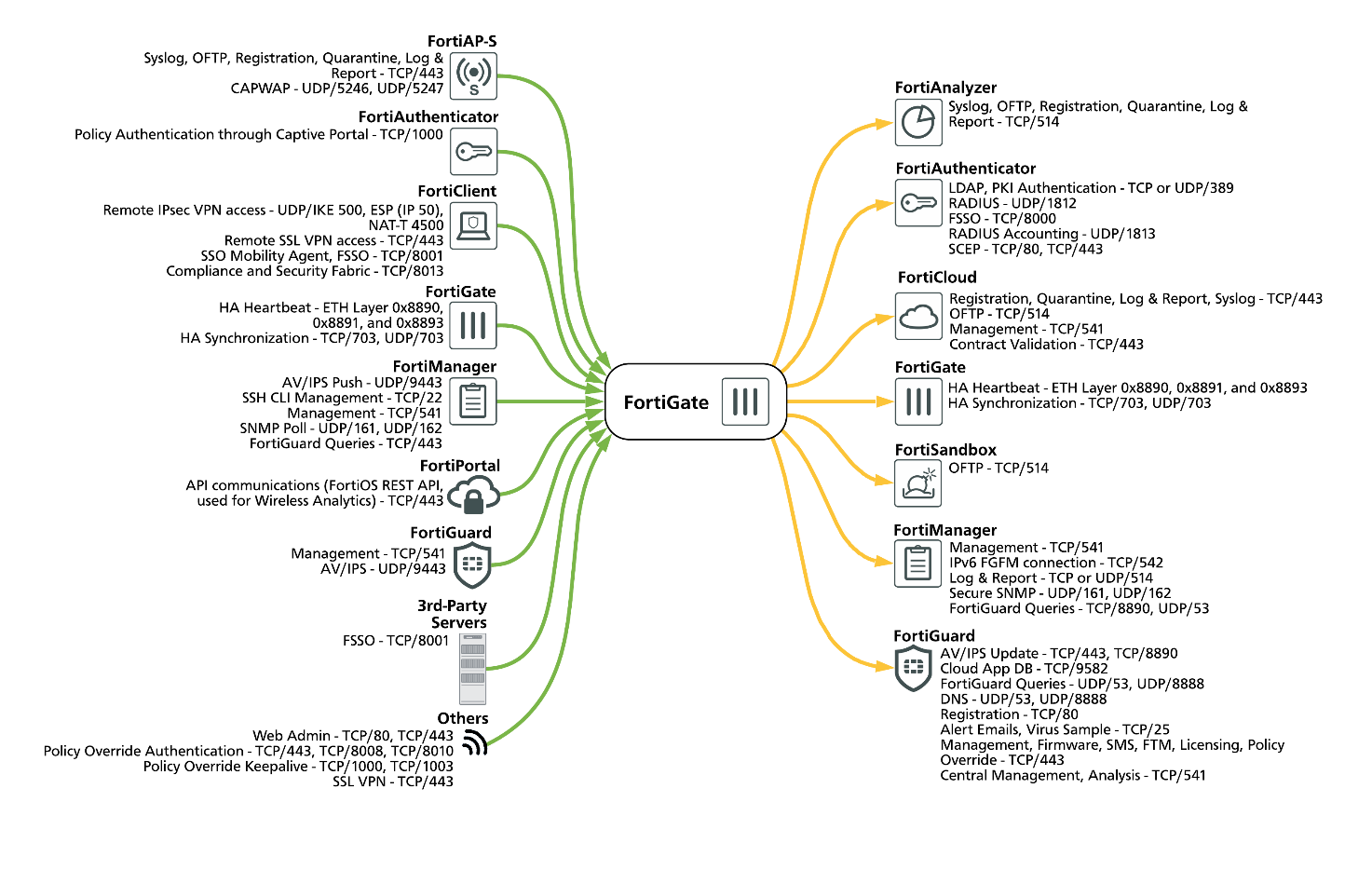


Рис. 3.28. Зв’язки фабрики безпеки

*Таблиця 3.2*

Кількісний аналіз метрик до і після впровадження

|  |  |  |
| --- | --- | --- |
| Метрика 30 діб | До впровадження | Після впровадження |
| Кількість знайдених в мережі вірусів | 0 | 23.574 |
|
| Кількість відбитих загроз | 4474 | 24574 |
| Кількість інспектованих додатків | 375000 | 1355645 |
|
| Кількість часу персоналу | 49 г. | 2 г. |

Таке покращення показників обумовлено тим, що була вропаджена система проактивного аналізу мережі. FortiDeceptor дозволяє знаходити загрози, що вже були колись інфільтровані в інфраструктуру. Крім того, після аналізу було виявлено близько 1.4 млн. додатків, що використовують шифрування, що унеможливлює повний ефективний аналіз лише одного пристрою. Варто зазначити, що інтегрований програмний код на мові програмування Python, удосконалює процес створення політик безпеки і не потребує часу персоналу, як показано в таблиці 3.2.

Інтегрований комплекс протидії загрозам 0 дня прискорив аналіз додатків без сигнатур та зменшив навантаження на ядро захисту.

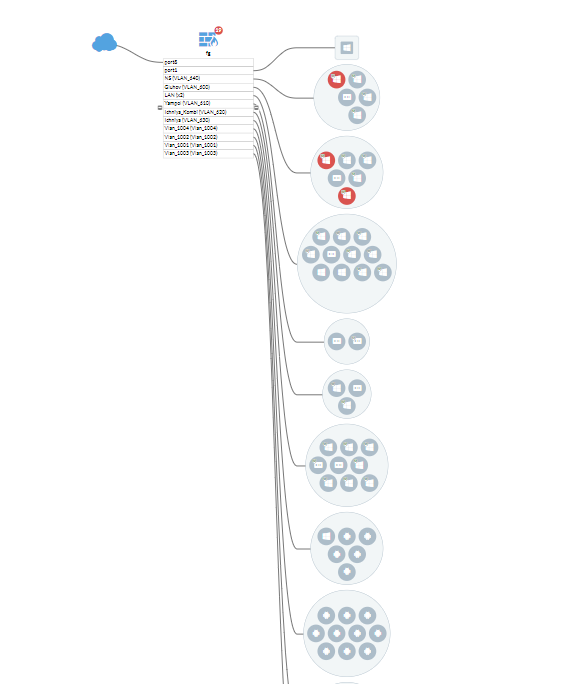


Рис. 3.28. Логічна топологія автоматизованого захисту

### 3.3. Оцінка ефективності та перспективи інтеграція

Для оцінки ефективності варто скористатись двома методами. Першим методом буде кількісний. Розрахунок відбувається на основі витрат, щодо придбання рішень ІБ та можливих втрат від НСД та вилучення конфіденційої інформації, втрати репутації і т.д.

Проект автоматизації системи інформаційної безпеки включає в себе закупку 3 основних продуктів, тоді витрати:

*Таблиця 3.3*

Кількісний аналіз впровадження

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Продукти | Витрати, грн | Заощадження | | |  |
| Визначення | min | mid | max |
| FortiGate | 500 000 | P1 | 150 000 | 250 000 | 500 000 |
| FortiSandbox | 700 000 | P2 | 300 000 | 450 000 | 900 000 |
| FortiAnalyzer | 250 000 | P3 | 50 000 | 90 000 | 195 000 |
| Сума | 1 450 000 | Сум | 500 000 | 790 000 | 1 595 000 |
|  |  |  |  |  |  |

В таблиці наведені дані витрат на закупку пристроїв та збитки у випадку викрадення інформації та зупинення бізнесу. Тому, придбання продуктів є цілком рентабельним. Також підприємство мінімізує витрати на новий персонал обслуговування систем захисту, завдяки автоматизованності процесів реагування на інциденти.

В результаті впровадження автоматизованої системи безпеки було зупинено звичайних загроз без відповідної реакції в перший день:



Рис. 3.29. Статистика зупинених атак

Стосовно складних загроз, за допомогою FortiSandbox та FortiDeceptor:

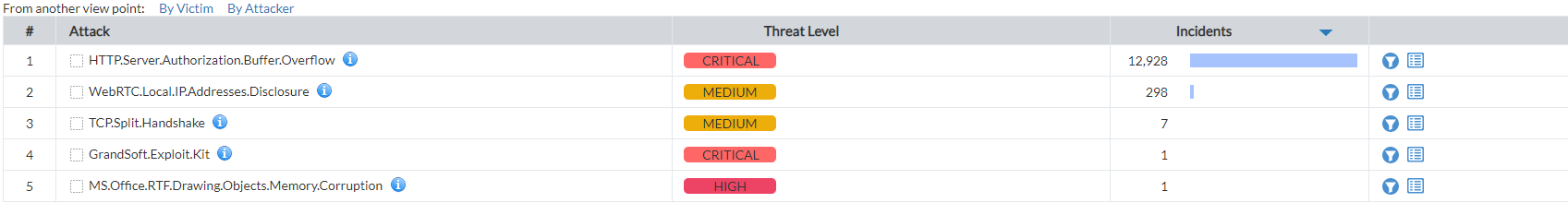


Рис. 3.30. Статистика заблокованих загроз FortiDeceptor

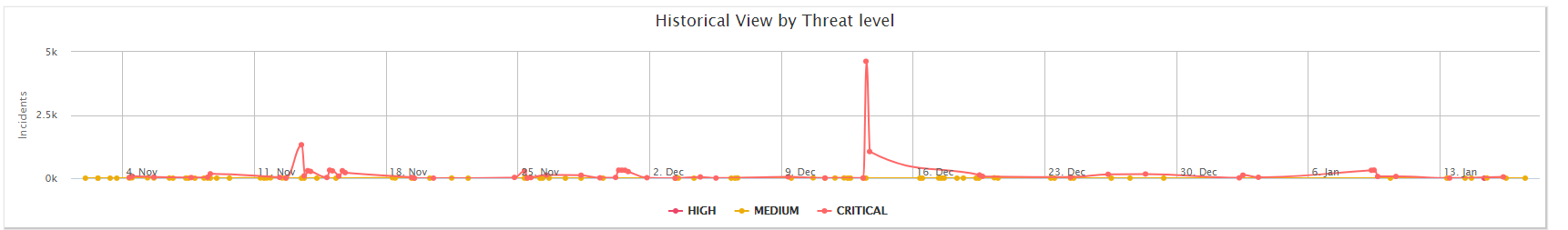


Рис. 3.32 Історичний аналіз атак

За весь час було інспектовано на рівні L7:

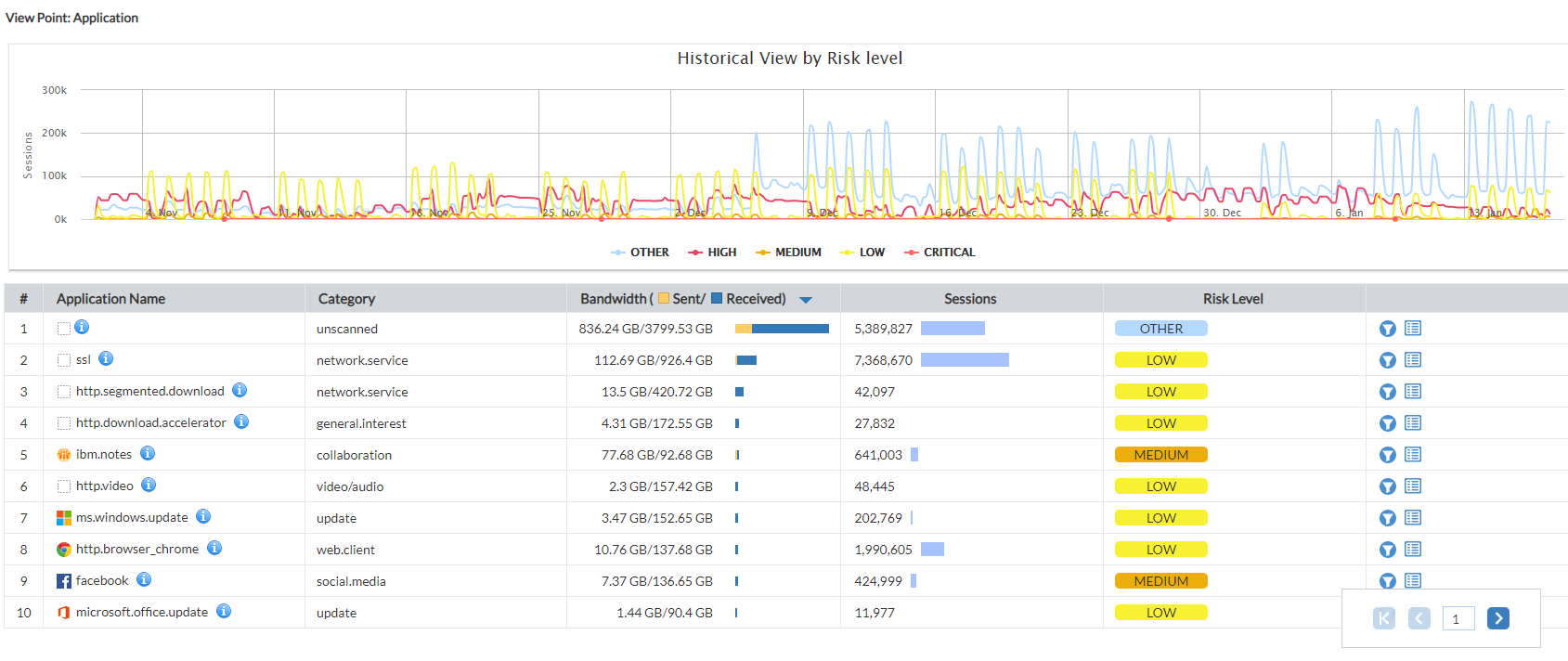


Рис. 3.33. SSL-інспекція додатків та з’єднань

Таким чином, за допомогою автоматизованої системи інформаційної безпеки від початку роботи:

* 47 вірусів (Malware Generic.P0, Android/DRDream.FV!tr, Riskware/CoinHive);
* Інспектовано >10 000 000 сесій;
* Заблоковано 24000 складних загроз (HTTP.Server.Authorization.Buffer.OverFlow, WebRTC.Local.Ip.Address, Disclosure, TCP.Split.Handshake, GrandSoft.Exploit.Kit, MS.IE.Stack.Exhaustion.Handler.Remote.Code.Execution, MS.Office.RTF.Drawing.Objects.Memmory.Corruption, PHP.URI.Code.Injection).

Можна зробити висновок, що система є ефективною з точки зору автоматизованої реакції на інциденти та мінімалізує втручання адміністраторів і офіцерів безпеки.

Перспективою покращення автоматизованої системи безпеки є інтеграція наступних рішень: ядро збору та кореляції інцидентів FortiSIEM, система контролю мережевих пристроїв FortiNAC, мультифакторна автентифікація FortiMFA, комплекс захисту веб-серверів з модулем штучного інтелекту FortiWEB, система балансування навантаження FortiADC.

FortiNAC - це контроль доступу до мережі Fortinet рішення, що покращує захисну видимість, контроль та автоматизоване реагування на все, що підключається до мережі. FortiNAC забезпечує захист від загроз IoT, розширює контроль на стороні пристроїв та оркеструє автоматичні відповіді на широке коло мережевих подій.

FortiSIEM - це засіб управління безпекою, продуктивністю і забезпеченням відповідності вимогам всіх компонентів інфраструктури, здатний працювати як з хмарами, так і з інтернетом речей (IoT). Рішення FortiSIEM направлено на зниження складності виявлення загроз при підвищенні ефективності системи безпеки. SIEM-система такого рівня спрямована на захист не тільки інформації, а й репутації клієнтів, знижуючи негативні наслідки від загроз і протидіючи виникненню нових атак.

Контролери доставки додатків FortiADC оптимізовують доступність, досвід роботи користувачів, продуктивність та безпеку додатків. Пристрій забезпечує швидке, безпечне та інтелектуальне прискорення та розподіл вимогливих додатків на підприємстві.

FortiWeb є міжмережевим екраном рівня веб-додатків (WAF), який реалізує захист від атак, спрямованих на експлуатацію відомих і невідомих вразливостей. Завдяки інтеграція багаторівневої системи виявлення загроз на базі штучного інтелекту, а також методів кореляції подій FortiWeb забезпечує захист додатків від відомих вразливостей і загроз нульового дня.

Головною перспективою є створення наступної захищеної, автоматизованої інфраструктури:

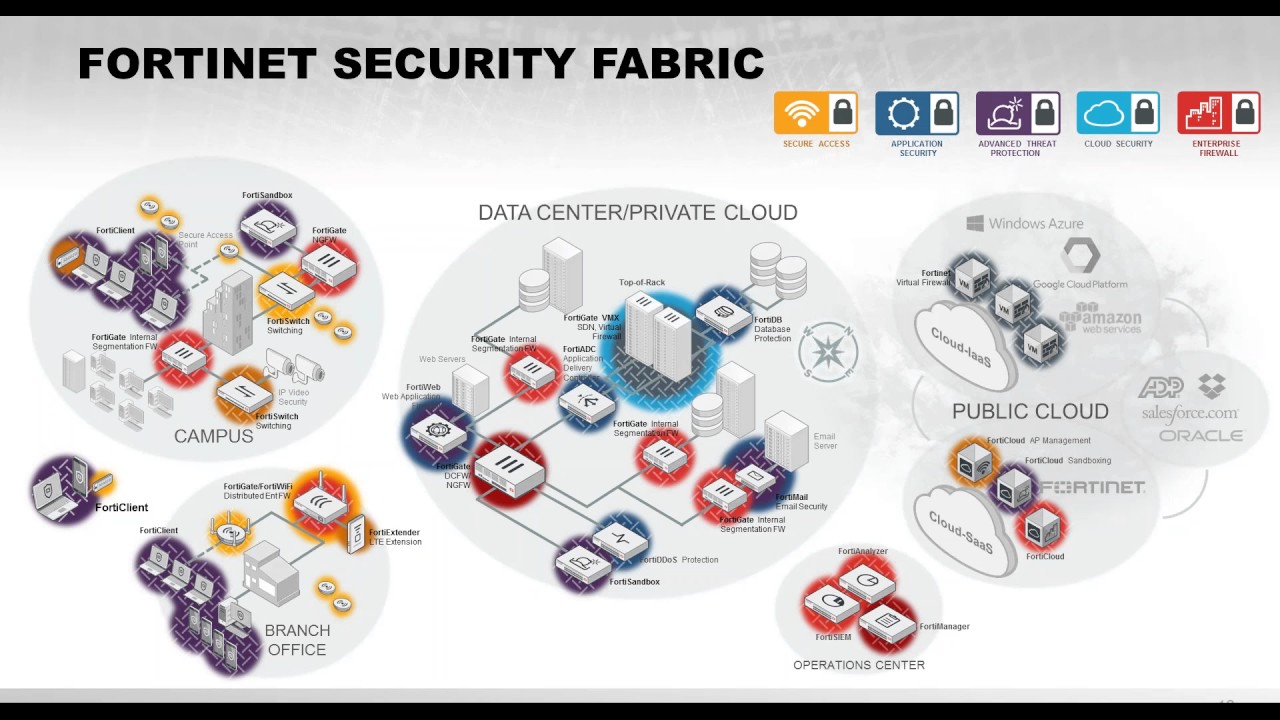


Рис. 3.33. Фабрика безпеки Fortinet

## 3.4 Висновок до розділу

**В цьому розділі було проаналізовано та розроблено ефективний метод автоматизації інформаційнох безпеки мережі на базі обладнання Fortinet. Ключовими елементами захисту є FortiGate, FortiClients, FortiDeceptor, FortiSandbox, FortiAnalyzer. Всі елементи були повністю інтегровані, що дало високий результат при порівнянні з минулим станом захисту. Також був розроблений програмний код мовою програмування Python. Скрипт удосконалив автоматизацію за рахунок автоматичного створення політик безпеки усіма учасниками комплексу. Таким чином ручна робота працівників відділу безпеки була знижена за 49 годин до 2 годин на місяць.**

# ВИСНОВКИ

Результатом виконаної роботи є вирішення задачі побудови системи автоматизованого захисту інформації.

У процесі виконання роботи отримані наступні результати:

1. Досліджено та прокласифіковано сучасні методи та напрями автоматизації захисту мережноїінфраструктури, що дало змогу визначити базові компоненти мережної інфраструктури які підлягають захисту та сучасні проблеми автоматизації інформаційної безпеки;
2. досліджено та проведено порівняльний аналіз спеціалізованого програмного забезпечення для реалізації автоматизованої системи інформаційної безпеки підприємства, що дало змогу визначити Fortinet, як найбіль гнучкий для реалізації захищеної мережної інфраструктури;
3. розроблено програмний код, що автоматизує впровадження налаштування політик захисту для всіх елемнтів системи на мові програмування Python;
4. проведено оцінку ефективності та обґрунтовано перспективи впровадження даного підходу щодо автоматизації системи інформаційної безпеки підприємства, що дозволило мінімізувати зовнішні та внутрішні загрози, а також збільшити кількість виявлених зовнішніх втручань в інформаційну систему.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Остроухов В.В. Інформаційна безпека (соціально-правові аспекти): Підручник / [Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. ; за заг. ред. Є.Д.Скулиша]. – К. : КНТ, 2010. – 776 с.
2. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
4. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
5. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI
6. ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.
7. ДСТУ 3396.1-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт
8. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту в комп’ютерних системах від несанкціонованого доступу
9. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення
10. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
11. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
12. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
13. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
14. ДСТУ ISO/IEC 25012:2016 Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Модель якості даних (ISO/IEC 25012:2008, IDT) [Электронный ресурс] – Режим доступа: <http://online.budstandart.com/ua/catalog/docpage.html?id_doc=69135>.
15. ДСТУ ISO 9000:2007 Системи управління якістю. Основні положення та словник термінів [Електронний ресурс]. – Режим доступу до ресурсу: http://document.ua/docs/tdoc14237.php
16. Міжнародний стандарт ISO/IEC 27001 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org 6. Міжнародний стандарт ISO/IEC 27002 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
17. Міжнародний стандарт ISO/IEC 27003-27004 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
18. Міжнародний стандарт ISO/IEC 27005 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
19. Міжнародний стандарт ISO/IEC 27006 / – [Електронний ресурс]. – Режим доступу: http://www.iso.org
20. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
21. Fortinet Security Fabric ― Режим доступа <https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security.html>.
22. Fortinet Fortigate ― Режим доступа  [<https://www.fortinet.com/products/next-generation-firewall.html>](https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security.html).
23. Fortinet FortiDeceptor ― Режим доступа <https://www.fortinet.com/products/fortideceptor.html>.
24. Fortinet FortiSandbox ― Режим доступа <https://www.fortinet.com/products/fortideceptor.html>
25. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: [навчальний посібник] / В. А. Ліпкан, Ю. Є. Максименко, В.М.Желіховський. — К.: КНТ, 2006. — 280 с.
26. Богуш В.М., Юдін О.К. Інформаційна безпека держави – К.: «МК-Прес», 2005 – 432с., іл.
27. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М. ДМК Пресс, 2010. - 544 с.
28. Диффи У. Первые десять лет криптографии с открытым ключом // ТИИЭР. - 1988. - Т. 76. - № 5. - С. 54-74.
29. Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. / М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с.
30. Группы и поля (повторение из теории чисел) [Електронний ресурс]. - Режим доступу: http://docplayer.ru/26528862-18-gruppy-i-polya-povtorenie-iz-teorii-chisel.html
31. Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информации: Учебное пособие. - Красноярск: СибГАУ, 2007. - 217 с.
32. Астахов А.М. Искусство управления информационными рисками / Астахов А.М. – М : ДМК Пресс, 2010. – 314 с.
33. Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности : BS ISO/IEC 27005:2008. – К.: 2011. – 70 с.
34. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: ГОСТ Р ИСО/МЭК 13335-1 – 2006. – Введ. 2007.05.31. – М. : ИПК «Издательство стандартов», 2007. – 23 с.
35. Информационная технология. Уровни целостности систем и программных средств : ГОСТ Р ИСО/МЭК 15026 – 2002. Введ. 2003.06.30. – М.: ИПК «Издательство стандартов», 2003. – 15 с.
36. Информационные технологии. Свод правил по управлению защитой информации : ISO/IEC 27002:2005(E) – М. : Компания «Технорматив», 2007. – 117 с.
37. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу [Текст] : НД ТЗІ 1.1-003 – 1999. – Чин. 1999. 04.28. – К. : ДСТСЗІ СБ України, 1999. – 12 с.
38. CMS Information Security Risk Assessment (RA) Methodology / [CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)] – Baltimore : Centers for Medicare & Medicaid Services, 2002. – 21 p.
39. International standard Risk management. Principles and guidelines : ISO/FDIS 31000:2009(E) / International Organization for Standardization // JISC – 2009. – 24 р.
40. Гуцу С. Ф. Правові основи інформаційної діяльності : навч. посіб. / С. Ф. Гуцу. ― Х. : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. ― 48 с.
41. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Б. А. Кормич ; Нац. ун-т внутр. справ. ― Х., 2004. ― 42 c. 3.
42. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А. І. Марущак // Державна безпека України. ― 2011. ― № 21. ― С. 92―95.
43. Сороківська О. А. Інформаційна безпека підприємства : нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. ― 2010. ― № 2, т. 2. ― С. 32―35.
44. Кулініч О. А. Структурні чинники економічної безпеки України / О. А. Кулініч // Шлях України до економічної безпеки : матеріали наук.-практ. конф. ― Х. : ХНУВС, 2007. ― С. 59―63.
45. Живко З. Б. Соціально-економічна безпека : навч. посіб. для самост. вивч. дисц. / З. Б. Живко, М. І. Керницька. ― Львів : Ліга-Прес, 2008. ― 345 с.
46. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия / С. В. Кавун // Управління розвитком. ― Х. : ХНЕУ, 2008. ― Вип. 6. ― С. 17―21.
47. Smieliauskas W. Auditing: An International Approach / W. Smieliauskas, K. Bewley. ― McGraw-Hill Ryerson Higher Education, 2006. ― 800 p.
48. Иванов О. В. Информационная составляющая современных войн / О. В. Иванов // Вестн. Моск. ун-та: сер. 18 : Социология и политология. ― 2004. ― № 4. ― С. 64―70.
49. Гришина Н. В. Организация комплексной системы защиты информации / Н. В. Гришина. ― М. : Гелиос АРВ. ― 2007. ― 256 с.
50. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері інтеграція комп’ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк ; за заг. ред. Р. А. Калюжного. ― Запоріжжя : Просвіта, 2001. ― 252 с.
51. Porter B. Principles of External Auditing / B. Porter, D. Hatherly, Jon Simon. ― [3rd edition]. ― Wiley, 2008. ― 816 p.
52. Марунич А. В. Захист інформації як основна складова економічної безпеки підприємства / А. В. Марунич // Управління розвитком. ― 2014. ― № 14. ― С. 130―132.
53. Гордієнко С. Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії / С. Б. Гордієнко, О. С. Микитенко, В. Г. Данильчук // Вісник ДУІКТ. ― 2013. ― № 1. ― С. 104―107.
54. Ясенев В. Н. Информационная безопасность в экономических системах : учеб. пособ. [Электронный ресурс] / В. Н. Ясенев. ― Н. Новгород : Изд-во ННГУ, 2006. ― Режим доступа : <http://ebib.pp.ua/informatsionnaya-bezopasnost-ekonomicheskih88.html>.
55. Захаркін О. О. Інформаційні системи та технології у фінансових установах : конспект лекцій [Електронний ресурс] / О. О. Захаркін, М. Ю. Абрамчук, М. А. Деркач. ― Суми : Вид-во СумДУ, 2007. ― 80 с. ― Режим доступу : http://elkniga.info/book\_188.html.

### Додаток А

**ПРОГРАМНИЙ КОД АВТОМАТИЗАЦІЇ ДОДАВАННЯ ПОЛІТИК БЕЗПЕКИ**

|  |
| --- |
| import requests, json, sys |
|  |
| # Функції |
| def api\_request(method, params=None): |
| 'requests methods to api\_url and prints the result in json decoded format' |
| r = s.get(api\_url + method, verify=False) |
| return r |
|  |
| def api\_post(method, params=None, data=None): |
| 'post to api\_url in json encoded format' |
| r = s.post(api\_url + method, params=params, data=repr(data), verify=False) |
| return r |
|  |
| def add\_to\_group(Address,grp\_name): |
| #check for group membership |
| member = 0 |
| r = api\_request('cmdb/firewall/addrgrp/'+grp\_name) |
| if r.status\_code == requests.codes.ok: |
| members = r.json() |
| for results in members['results']: |
| for m in results['member']: |
| if m['name'] == Address: |
| print 'Member of group' |
| member = 1 |
| break |
| if member == 0: |
| print 'Not member of group' |
| print 'Adding to group' |
| payload = [ |
| { |
| 'name':Address, |
| 'q\_origin\_key':Address, |
| 'uuid':uuid, |
| 'subnet':subnet |
| **Продовження додатку А**  } |
| ] |
| print payload |
| r = api\_post('cmdb/firewall/addrgrp', params={'vdom':vdom, 'name':grp\_name, 'mkey':grp\_name, 'addrgrp-member':payload}) |
| print r.status\_code |
| else: |
| print 'Error getting group' |
|  |
| def get\_group(Address,grp\_name,vdom): |
| member = [] |
| r = api\_request('cmdb/firewall/addrgrp/'+grp\_name) |
| if r.status\_code == requests.codes.ok: |
| results = r.json() |
| for result in results['results']: |
| for r in result['member']: |
| member.append({'name':r['name']}) |
|  |
| member.append( |
| { |
| 'name':Address, |
| } |
| ) |
| payload = json.dumps(member) |
| # payload = {'json': |
| # { |
| # 'name':'all' |
| # }, |
| # { |
| # 'name':Address |
| # } |
| # } |
| print payload |
| payload = str(payload) |
| payload = '{\'vdom\':'+vdom+', { json : ' + payload.replace('\"','\'') + '}' |
| **Продовження додатку А**    print payload |
|  |
| r = api\_post('cmdb/firewall/addrgrp'+grp\_name, params={'vdom':vdom}, data=payload) |
| print r.status\_code |
| #if member == 0: |
| # print 'Not member of group' |
| # print 'Adding to group' |
| # payload = members |
| # print payload |
| # r = api\_post('cmdb/firewall/addrgrp', params={'vdom':vdom, 'name':grp\_name}, data=payload) |
| # print r.status\_code |
| else: |
| print 'Error getting group' |
|  |
|  |
| def add\_to\_Policy(Address,Direction,PolicyID): |
| added = 0 |
| if Direction == 'Source': |
| Direction = 'srcaddr' |
| elif Direction == 'Destination': |
| Direction = 'dstaddr' |
| else: |
| print 'Invalid parameter' |
| return |
| r = api\_request('cmdb/firewall/policy/'+PolicyID) |
| if r.status\_code == requests.codes.ok: |
| members = r.json() |
| for results in members['results']: |
| for d in results[Direction]: |
| if d['name'] == Address: |
| print 'Added to Policy' |
| added = 1 |
| break |
| **Продовження додатку А**  if added == 0: |
| print 'Not added to policy' |
| print 'Adding to policy' |
| payload = {'dstaddr': |
| { |
| 'name':Address, |
| 'q\_origin\_key':Address |
| } |
| } |
| print payload |
| r = api\_post('cmdb/firewall/policy'+PolicyID, params={'vdom':vdom}, data=payload) |
| print r.status\_code |
|  |
|  |
| def add\_Address\_Object(Address): |
| global uuid |
| global subnet |
| #Check address exists |
| print 'Check if Address exists\n' |
| r = api\_request('cmdb/firewall/address/' + IPAddr) |
| if r.status\_code == requests.codes.ok: |
| print 'Object Already exists' |
| print |
|  |
| else: |
| print 'Object creation' |
| payload = {'json': |
| { |
| 'name':IPAddr, |
| 'subnet':IPAddr +'/32' |
| } |
| } |
| r = api\_post('cmdb/firewall/address', params={'vdom':vdom}, data=payload) |
| print r.status\_code |
|  |
| r = api\_request('cmdb/firewall/address/' + IPAddr) |
| results = r.json() |
| for result in results['results']: |
| uuid = result['uuid'] |
| subnet = result['subnet'] |
| **Продовження додатку А** |
|  |
|  |
| #Головна функція |
|  |
| cli\_usage = '\nUsage: Please specify FortiGate IP Address, VDOM (default to root if not specified), User, Pass and IP to add\n' |
|  |
| if \_\_name\_\_ == '\_\_main\_\_': |
| if len(sys.argv) == 6: |
| FGHost = 'http://' + sys.argv[1] |
| vdom = sys.argv[2] |
| api\_user = sys.argv[3] |
| api\_pass = sys.argv[4] |
| IPAddr = sys.argv[5] |
| else: |
| if len(sys.argv) == 5: |
| FGHost = 'http://' + sys.argv[1] |
| vdom = 'root' |
| api\_user = sys.argv[2] |
| api\_pass = sys.argv[3] |
| IPAddr = sys.argv[4] |
| else: |
| print cli\_usage |
| exit() |
|  |
|  |
| # Визначення urL |
| login\_url = FGHost + '/logincheck' |
| logout\_url = FGHost + '/logout' |
| api\_url = FGHost + '/api/v2/' |
| uuid='' |
| subnet='' |
|  |
|  |
| **Продовження додатку А** |
| # Початок сесії |
| s = requests.Session() |
|  |
| # Login admin && Password Sydorov |
|  |
| payload = {'username':api\_user, 'secretkey':api\_pass} |
| r = s.post(login\_url, data=payload, verify=False) |
|  |
| print 'login status:', r.status\_code |
| print r.text |
| print s.cookies['ccsrftoken'] |
|  |
|  |
| for cookie in s.cookies: |
| if cookie.name == 'ccsrftoken': |
| csrftoken = cookie.value[1:-1] |
| s.headers.update({'X-CSRFTOKEN': csrftoken}) |
|  |
| #csrftoken = s.cookies['ccsrftoken'] |
| #s.headers.update({'X-CSRFTOKEN': csrftoken}) |
|  |
| # Виклики |
| #api\_request('monitor/system/interface?interface\_name=port1') |
| #api\_request('monitor/system/interface/') |
| #api\_request('monitor/system/firmware') |
|  |
| **Продовження додатку А**  add\_Address\_Object(IPAddr) |
| #print uuid |
| #Мережі |
| #add\_to\_group(IPAddr,'Block') |
| get\_group(IPAddr,'test',vdom) |
| #add\_to\_Policy(IPAddr,'Destination','1') |
|  |
| # Вихід |
| r = s.get(logout\_url) |
| if r.status\_code == requests.codes.ok: |
| print 'Successfuly logged out' |
| s.close() |

**Додаток Б**