**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

**КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ**

# Пояснювальна записка

до магістерської роботи
на тему:

# «ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ PANDA ADAPTIVE DEFENSE 360»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Данильченко Ю.С.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BYOD – Bring your own device

EDR – Endpoint Detection and Response

EOL – End-Of-Life (product)

EPP – Endpoint Protection Platform

IoT – Інтернет речей

MTD – Moving Target Defense

RDP – Remote Desktop Protocol

SIEM – Security information and event management

VDI – Virtual Desktop Infrastructure

ІС – Інформаційна система

ОС – Операційна система

ПЗ – Програмне забезпечення

СУБД – Система управління базами даних

ПНП – Потенційно небажані програми

# ВСТУП

*Актуальність дослідження.* Кількість використовуваних кінцевих точок в організаціях стрімко росте. Вони щодня передають важливу та конфіденційну інформацію між собою, яка може стати ціллю зловмисників. Будь-яка інформація, навіть маленької організації може виявитись потрібною для шахраїв. Іноді їм легше атакувати велику кількість маленьких підприємств, тому організаціям усіх видів та розмірів потрібно пам’ятати про захист кінцевих точок.

З ростом кількості кінцевих точок, росте і кількість видів атак на кінцеві пристрої, і технології захисту повинні вміти захищати кінцеві точки від шкідливого програмного забезпечення та від атак нульового дня, відстежувати складні загрози та слідкувати за поведінкою користувачів на усіх кінцевих точках. Простого антивірусу, яким у більшості випадків користуються компанії недостатньо. Тому важливо виростання рішення класу Endpoint Detection and Response, аби виявляти та вивчати усю шкідливу активність на кінцевих точках в організації. Для цього і потрібно розглянути існуючі технології та розробити варіант технології захисту кінцевих точок організації та рекомендації щодо застосування.

*Мета роботи* – розробити варіант технології захисту кінцевих точок інформаційної системи організації та рекомендації щодо застосування технології їх захисту.

Наукові завдання:

проаналізувати науково-літературну базу, щодо використання кінцевих точок в організації;

вивчити проблему захисту кінцевих точок в організації;

провести аналіз атак та загроз кінцевих точок інформаційної системи організації;

проаналізувати існуючі технології захисту кінцевих точок інформаційної системи організації;

провести огляд програмних продуктів для захисту кінцевих точок організації;

розробити варіант технології забезпечення для захисту кінцевих точок організації та рекомендації по застосуванню.

*Об'єкт дослідження* – процес забезпечення захисту кінцевих точок організації.

*Предмет дослідження* – технологія забезпечення захисту кінцевих точок організації.

*Практичне значення одержаних результатів* полягає в розробці варіанту технології захисту кінцевих точок організації та розробка рекомендацій щодо захисту кінцевих точок організації.

# 1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

## 1.1. Призначення та функції кінцевих точок інформаційної системи організації

На початку слід визначити що є кінцевою точкою. Кінцева точка (Endpoint) – це будь-який пристрій, який фізично являється кінцевою точкою у мережі. До кінцевих точок можуть відноситись ноутбуки, настільні персональні комп'ютери, мобільні телефони, планшети, сервери та віртуальні середовища можуть вважатися кінцевими точками [1].

Кінцеві пристрої (End Device) – це ще одна назва кінцевих точок, вони створені для обміну інформацією між собою. Необхідну інформацію з кінцевого пристрою може вимагати користувач (співробітник) організації, а може й інший кінцевий пристрій, трапляються випадки обміну даними без участі користувача.

Інакше можна сказати, що кінцеві пристрої (точки) - це пристрої, що ініціалізують процес обміну даними, вони або починають процес передачі даних, або вимагають отримання даних в інших кінцевих пристроїв.

Всі пристрої, які були перераховані вище, є прикладом передачі даних між кінцевими точками в інформаційній системі організації. За допомогою комп'ютера користувача ініціалізується передача даних із сервера або на нього, завантаження необхідних файлів із сайту, а отже з сервера, на якому вони зберігаються. Щоб надіслати електронну пошту, листи завантажуються з комп'ютерів на поштові сервери. Під час ініціалізації дзвінка на мобільному телефоні починається передача даних на сервер оператора мобільного зв'язку. Всі дані в месенджери, сервіси перегляду відео та соціальні мережі завантажуються з серверів на наші телефони, комп'ютери або планшети. Для завантаження програми або гри так само надсилається запит з нашого пристрою на сервер, щоб почалася передача файлів [2].

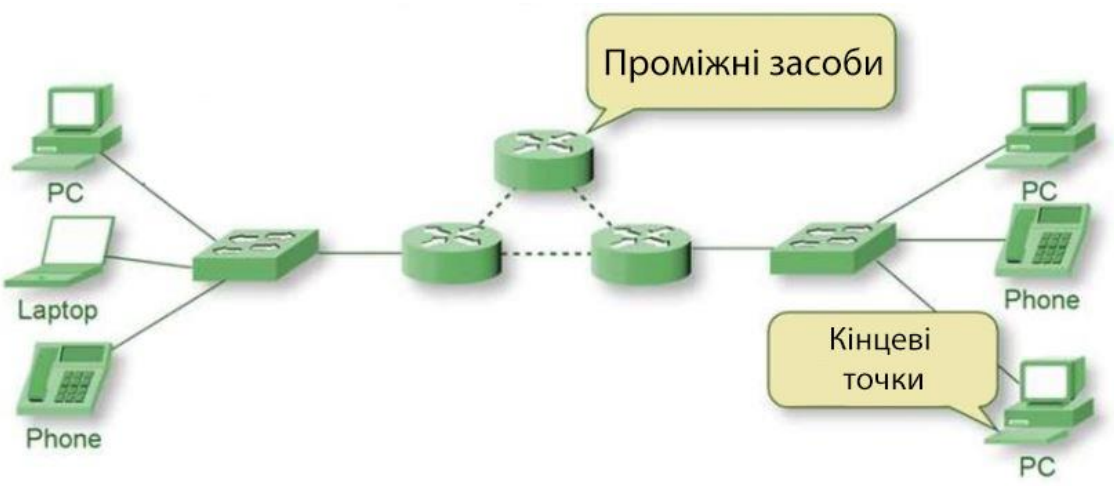


Рис. 1.1. Зв’язок кінцевих точок в мережі

Інформаційною системою організації є поєднання техніки, програм та людей, що забезпечує отримання своєчасної та достовірної інформації, необхідної для прийняття управлінських рішень.

Інформаційна система є на будь-якому підприємстві, її життєвий цикл дорівнює життю самого підприємства. Суть управління - це отримання, обробка та передача інформації. Поштовх розвитку інформаційних систем в останні роки дала комп'ютеризація.

Призначення інформаційної системи підприємства полягає у технічному, програмному забезпеченні організації необхідними даними. Причому, від того, наскільки повно і швидко здійснюються ці функції, залежить успішність компанії в цілому.

*Основними функціями інформаційних систем є:*

- Систематизація процесу керування компанією.
- Збір, обробка та передача даних, а також своєчасне забезпечення працівників необхідною інформацією.
- Автоматизація робочих процесів.
- Комунікація різних підрозділів.
- Технічне забезпечення процесу документообігу.

Ринок динамічно розвивається, а це означає, що мають відбуватися технологічні покращення. Виходячи з цього інформаційна система організації

повинна так само розвиватися в питаннях актуальності використовуваного програмного забезпечення, апаратних засобів та їх захисту від атак.

Загалом можна сказати, що сучасна інформаційна система підприємства є живим організмом, який складається з трьох основних складових (рис.1.2.):

- Комп'ютерна мережа;
- Програмне забезпечення;
- Персонал.


Рис. 1.2. Компоненти інформаційної системи організації

Дана робота буде присвячена важливим компонентам комп'ютерних мереж, а саме кінцевим точкам та їхньому захисту від атак зловмисників з метою отримання інформації, що знаходиться в інформаційній системі організації.

## 1.2. Аналіз проблеми забезпечення захисту кінцевих точок інформаційної системи організації

У попередньому розділі, було визначено, що кінцева точка у інформаційній системі організації – це «прохід» для співробітників для доступу до корпоративних даних. Наразі організації складаються не лише з офісних співробітників, які працюють на пристроях, що належать самій організації. В організаціях спостерігаються співробітники, які працюють віддалено на своїх персональних пристроях, або використання особистих комп'ютерів на робочому місці, концепція Bring your own device (BYOD) . Хоча така робоча модель зручна для співробітників, вона має свої мінуси. Головним є загроза безпеці завдяки неналежному захисту особистих кінцевих пристроїв.

Дослідження Ponemon Institute, проведене в 2020 році, показало, що за 12 місяців 68% організацій зіткнулися з однією або декількома атаками на кінцеві точки в своїй інформаційній системі. Дані атаки змогли успішно скомпрометувати дані цих організацій або їхню IT-інфраструктуру. У цьому ж звіті зазначається, що 68% фахівців інформаційної безпеки помітили, що кількість та частота атак на кінцеві точки збільшилася, якщо порівнювати з 2019 роком (рис.1.3.).

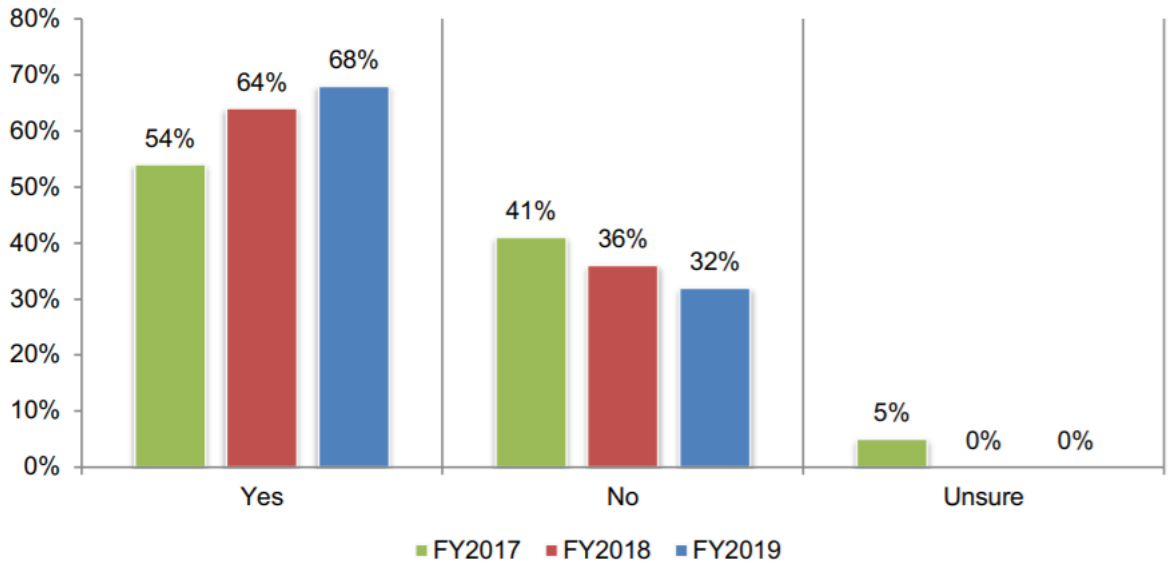


Рис. 1.3. Кількість організацій, що зіткнулись з однією або декількома атаками на кінцеві точки (Дослідження Ponemon Institute)

Дане дослідження показує, що атаки на кінцеві точки організацій виявилися одними з найпоширеніших, з якими мали справу опитані представники компаній. 81% організацій відчули на собі атаки з використанням різноманітного шкідливого програмного забезпечення, а 28% зазнали атак за участю вкрадених або зламаних пристроїв[3].

Звіт про загрози Webroot за 2020 рік свідчить, що вищезгадані організації з віддаленими співробітниками, або з використанням концепції BYOD частіше схильні до найвищого ризику атак на кінцеві точки. Адже особисті пристрої частіше заражаються шкідливим програмним забезпеченням, ніж їх аналоги, які використовуються виключно в організаціях.

Хоча, незважаючи на те, що збільшуються ризики безпеки, пов'язані з віддаленою роботою співробітників, всього 47% організацій контролюють свої мережі цілодобово і без вихідних, такі дані показало спільне дослідження Ponemon Institute та Keeper Security. Також лише 50% організацій приділяють увагу шифруванню своїх конфедіційних даних, що зберігаються на пристроях. Лише менше половини підприємств забезпечують захист кінцевих пристроїв інформаційної системи організації за допомогою сучасного антивірусного програмного забезпечення (ПЗ), шифрування пристроїв та брандмауерів (рис.1.4.).

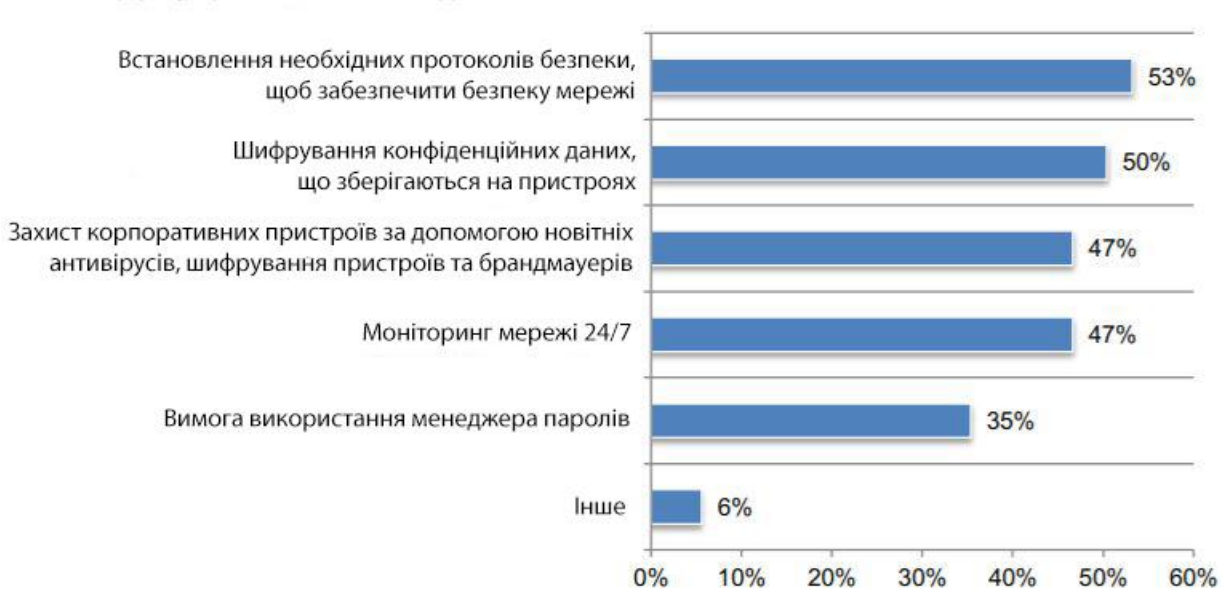


Рис. 1.4. Кроки забезпечення кібербезпеки компаній для створення умов безпечної роботи (Дослідження Ponemon Institute та Keeper Security 2020)

Важливо, що найчастіше при атаках на підприємства використовуються програми-вимагачі і найчастіше піддаються відносно невеликі організації. Кіберзлочинці розглядають їх як легкі цілі через відсутність належного захисту.

Державні організації у свою чергу менш схильні до атак програм-вимагачів, ніж приватні організації, про це згадується в дослідженні Sophos.

Ціна злому кінцевої точки з кожним роком стає дедалі вищою і середній дохід програм-вимагачів зростає порівняно з попередніми роками.

Окрім фінансових витрат, які вимагають кіберзлочинці, компанії ще стикаються з ризиком втрати чи розкриття конфіденційних даних.

При проблемі з програмами-вимагачами найкраще звернутися до відновлення даних через резервні копії, про які потрібно заздалегідь потурбуватися, ніж платити викуп зловмисникам. Тим більше, що оплата викупу не означає, що дані точно будуть повернені [4].

## 1.3. Види атак та загроз кінцевих точок інформаційної системи організації

Ознайомившись з проблемою забезпечення захисту кінцевих точок в інформаційних системах організацій, слід детальніше розглянути які саме існують атаки та загрози кінцевих точок.

Атакою на кінцеву точку інформаційної системи організації називають тип кібератаки, яка спрямована на кінцеві пристрої, що знаходяться у мережі даної інформаційної системи. Після атаки та отримання доступу до кінцевої точки зловмисник може заразити систему шкідливим ПЗ. Тому безпека кінцевих точок означає заходи, які вживаються для запобігання даних атак на всі пристрої (кінцеві точки), які підключені до певної мережі в будь-якій точці світу.

Кінцеві точки є основними цілями, які можуть бути використані як точки входу, через які кіберзлочинці можуть отримати доступ до мережі [5].

Загрози та вектори атак на кінцеві точки інформаційної системи підприємства діляться на типи, наведені нижче.

*Безфайлові шкідливі програми та атаки нульового дня*

Існуюче шкідливе ПЗ розвивається паралельно з посиленням захисту від відомих кіберзагроз, а також кількість видів шкідливого ПЗ постійно збільшується. Дані Інституту Ponemon повідомляють, що 41% атак здійснюється за допомогою «безфайлового шкідливого ПЗ», яке не завантажує файли, а використовує процеси операційних систем. У таких випадках звичайні антивіруси не реагують та не запускають сканування пристрою, а вбудований шкідливий код запускається та зникає, залишаючись непоміченим.

Не менш важливими є атаки нульового дня, і на них організації повинні звертати особливу увагу. Дані атаки характеризуються відсутністю сигнатури або можливістю використання вразливості, яка виявлена ще до виходу патчу. За фактом атаки нульового дня обходять антивірусні рішення за допомогою машинного навчання, вони отримують атрибути, які відсутні в наборі зразків.

Сучасне рішення, що використовується для захисту кінцевих точок, повинно мати можливість їх захисту від шкідливого ПЗ і від атак нульового дня.

*Загрози з хмарного сховища*

Зараз багато робочих процесів підприємств відбуваються у хмарі і залежать від неї. У зв'язку з цим хакери намагаються отримати максимальний собі прибуток. Багато підприємств сподіваються, що їхні хмарні провайдери мають надійну безпеку і стежать за нею, але це не завжди так.

Через це хмарне сховище є одним із вразливих векторів атак на кінцеві точки в інформаційній системі підприємства, із захистом якого не впораються застарілі рішення для захисту кінцевих точок та прості антивіруси.

Ідеальне рішення для захисту закінчених точок інформаційно системи підприємства включає в себе моніторинг поведінки та машинне навчання.

*Інтернет речей (IoT)*

Інтернет речей найчастіше поставляється без елементів захисту від кіберзагроз; також вони можуть мати жорстко запрограмовані основні паролі адміністратора. Популярні методи безпеки рідко мають можливості, які необхідні для моніторингу пристроїв IoT. У тому числі рішення виявлення та реагування (EDR) для кінцевих точок можуть не побачити пристрої IoT, через що вони можуть проникнути в мережу і вийти з неї, залишившись непоміченими. З цих причин Інтернет речей дають можливість кіберзлочинцям створювати погрози або перебувати в мережі непоміченими [6].

*Шкідливі атаки криптомайнінгу*

Інструменти Cryptomining перетворюють обчислювальні потужності у прибуток. Ринок криптовалют продовжує зростати, але обладнання для цього є дорогим. Тому кіберзлочинці знаходять способи, щоб оволодіти обчислювальними ресурсами жертв.

Способи включають атаки з використанням веб-браузера, які працюють, коли гравець знаходиться на законному, але скомпрометованому веб-сайті. Також існує шкідливе програмне забезпечення, яке доставляється через фішингові кампанії і навантажує процесор на кінцевих точках в інформаційній системі організації.

Будь-який вид криптомайнінгу може зазнавати величезних збитків для бізнесу. Прикладом такого може бути перетворення скомпрометованих кінцевих точок та хмарного сховища на видобувачів криптовалют. Таку атаку буде складно виявити, не маючи розширених інструментів виявлення загроз, спрямованих на кінцеві точки. Єдиною ознакою може бути зниження продуктивності мережі.

*Атаки на протокол віддаленого робочого столу*

Протокол віддаленого робочого стола (RDP - Remote Desktop Protocol) дозволяє підключитися до системи Windows віддалено і зазвичай запитує пароль користувача, щоб отримати доступ до сеансу. Зазвичай, вимагаючи надати пароль користувача, перш ніж ви зможете отримати доступ до сеансу. Однак існує спосіб обійти цей пункт – запустити tscon.exe (процес клієнта RDP) від імені користувача SYSTEM, який не запитує пароль. На цей спосіб не спрацьовують жодні антивіруси. Тому варто переконатися, що політика шлюзу блокує ці з'єднання за умовчанням (або дозволяє підключення лише з авторизованих IP-адрес).

*APT / Rootkits*

Удосконалені постійні погрози (APT) – це атака, під час якої користувач, який не авторизований, отримує доступ до системи або мережі та довгий час може перебувати всередині без виявлення. Такі кіберзагрози починаються з фішингового листа для отримання облікових даних, далі впроваджуються шкідливі програми Rootkits, які маскують роботу шкідливих програм. Вони можуть глибоко впроваджуватися в операційну систему кінцевої точки.

*Ухиляння кіберзлочинців від виявлення традиційними антивірусами*

Дані атаки не є однаковими, вони мають характерні відмінності, але так само вони мають специфічні особливості, які допомагають їм уникати виявлення традиційними антивірусними інструментами. Нижче розглянуто 4 основні кроки як це відбувається:

1. Антивіруси відловлюють і поміщають до карантину шкідливі файли на основі сигнатур, у міру їх завантаження або виконання на кінцевих точках. Але існує нюанс у тому, що сучасні атаки не потребують завантаження або виконання шкідливих файлів на об'єкті, що атакується. Вони використовують соціальну

інженерію (фішинг), використовують уразливості операційних систем (ОС) та ховають шкідливий код у файли, які не виглядають підозріло, щоб не бути виявленими під час доставки.

Після закріплення зловмисника на кінцевій точці, він може скористатися PowerShell, щоб завантажити та поширити потрібні дані. Традиційні антивірусні програми націлені на пошук незвичайних файлів, тому не сприймуть PowerShell або інші звичні процеси як щось шкідливе.

2. На другому етапі злочинець використовує нативні компоненти системи проти жертви. Використовуючи те, що вже на кінцевій точці. Так атака відбувається швидко і уникає виявлення антивірусної програми.

3. Скомпроментовані кінцеві точки дають хакерам вільний вхід до мережі жертви. Далі злочинець починає пересування по інших об'єктах, що знаходяться в тій самій мережі, у пошуках необхідних даних чи наступної мети. Ними можуть стати дані адміністратора домену або файлові сервери.

При захопленні даних адміністратора, кіберзлочинець може переміщатися практично в будь-яку точку даної мережі, отримувати доступ до будь-яких даних та залишатися непоміченим антивірусом.

4. Останнім кроком кіберзлочинця є приховування своїх слідів перебування у мережі. Маючи дані адміністратора він легко може видалити файли журналів на кожній кінцевій точці, яка була використана, щоб не виникло жодних зачіпок при подальшому дослідженні кіберінциденту [7].

## 1.4. Вибір технології захисту кінцевих точок інформаційної системи організації

Переходячи до питання захисту кінцевих точок, варто відзначити, що класичного антивіруса буде недостатньо. Для якісного захисту кінцевих точок необхідно використовувати інструменти класу Endpoint Detection and Response (EDR) — клас рішень для виявлення та вивчення шкідливої активності на кінцевих точках: підключених до мережі робочих станцій, серверів, пристроїв Інтернет речей. На відміну від антивірусів вони борються з типовими та масовими загрозами, EDR-рішення орієнтовані на виявлення цільових атак та складних загроз, таких як експлойти, скрипти чи вразливість «нульового дня».

На окремих робочих станціях також важливими є наявність DLP-системи, контроль USB-носіїв та шифрування жорсткого диска. Однак при встановленні цього на середньостатистичну робочу станцію, її продуктивність істотно впаде.

Тут важливо відштовхуватися саме від потреб клієнта та брати до уваги, які завдання вирішує кінцева точка. Хорошим рішенням буде використання агента безпеки для відстеження дій користувача на кожній кінцевій точці.

Ще одним варіантом захисту кінцевих точок є використання рухливих цілей - Moving Target Defense (MTD). Цей спосіб захисту заснований на регулярній зміні цільової системи, щоб вона стала непередбачуваною для зловмисників, що ускладнить процес атаки. Один із способів використання MTD - випадкова зміна місця розташування процесу в пам'яті пристрою. Але дана технологія поки є досить вузькою, хоча має розвиток.

Рішення MTD не є широко поширеним продуктом, не всі організації потребують цієї системи. Головна цільова аудиторія – великі організації, які зберігають велику кількість конфіденційної інформації, яка може стати метою атаки [8].

Повертаючись до антивірусів і розглянувши їх детальніше, варто відзначити їх основну технологію, яка є і їх недоліком. Нею є сигнатурний аналіз – технологія, яка дозволяє обчислити контрольну суму зараженого файлу та записати її до

центральної сигнатурної бази. Для наступних перевірок кожного файлу його контрольна сума проходить порівняння з усіма записами, які знаходяться в сигнатурній базі і під час збігу файл виділяється як заражений. Власне головним недоліком є те, що виявити таким методом можна лише ті загрози, які вже знаходяться в базі, нові вразливості та методи їх використання не потрапляють до огляду сигнатурного аналізу.

Наступним кроком у розвитку антивірусів було використання статичного аналізу. Суть даного способу полягає в тому, що на основі певного набору патернів і статичних ознак евристичний механізм намагається передбачити можливу поведінку файлів, перш ніж вони зможуть завдати шкоди системі. Використання статистичного аналізу збільшило відсоток виявлення шкідливих файлів, навіть тих, що відсутні в сигнатурній базі. Однак і цей метод має свої недоліки. Головним є органічний метод при ідентифікації атак, у яких були використані не відомі раніше вразливості в ПЗ. У таких випадках статичні властивості та інструкції, які використовуються шкідливим файлом, з точки зору евристичного аналізу можуть не відрізнятися від інструкцій у безпечних файлах.

Головною метою атаки не завжди є заражені файли, що виконуються. Часто зустрічаються атаки на кінцеві точки, які експлуатують існуючі вразливості у ПЗ. Це можуть бути і атаки на вразливості браузера, у такому разі користувач завантажує веб-сторінку, яка заражена, і атака з доставкою шкідливого навантаження на кінцеву точку, використовуючи вразливість мережевих протоколів та ОС. У цих випадках недостатньо просто перехопити та проаналізувати файл, який був заражений. Необхідно забезпечення захисту мережевих з'єднань після аналізу мережного трафіку, який надходить і виходить із кінцевої точки. Для таких потреб до функціоналу класичних антивірусів додаються технології мережного захисту: міжмережеві екрани, системи запобігання вторгненням та системи контролю пристроїв, які підключаються до кінцевих точок.

Для поєднання всіх необхідних функцій для захисту кінцевих точок була створена платформа захисту кінцевих точок, або Endpoint Protection Platform (EPP). Endpoint Protection Platform є системою комплексного захисту кінцевих точок, яка

включає як класичні функції захисту антивірусів, так і розширені технології безпеки. Дана платформа відрізняється наявністю персональних міжмережевих екранів, системи запобігання вторгненням, системи контролю портів та пристроїв, що підключаються, системи шифрування дисків тощо.

Через зростання спрямованих атак більшість EPP-рішень перестали відповідати сучасним вимогам до безпеки кінцевих точок. Дані атаки переважно використовують уразливості нульового дня і є масовими через використання ботнетів. Ще є криптолокери (або шифрувальники), які не використовують відомі вразливості, а експлуатують ще невідомі вразливості. Через зростання кількості атак та їх еволюцію EPP-рішення теж еволюціонували, щоб не відставати від необхідних методів захисту кінцевих точок.

За підсумками еволюціонування з'явилися системи під назвою — NGEPP. NGEPP (Next Generation Endpoint Protection Platform) — це системи, призначені для захисту кінцевих станцій, які, крім базового функціоналу класичних антивірусів, захисту мережі та контролю портів, додатково мають розширені функції для боротьби з сучасними загрозами. Додаткові системи, які розширюють можливості класичних EPP-систем, перераховані далі:

- Системи, що емулюють файли, що проходять в пісочниці (sandboxing), аби боротися з загрозами нульового дня.
- Anti-Bot системи, які призначені для боротьби з ботнетами, вони ґрунтуються на аналізі патернів трафіку та визначення в них бот-активності.
- EDR-системи (Endpoint Detect and Response) - системи, які забезпечують реактивний захист кінцевих точок, відповідають за розслідування інцидентів шкідливої активності та подальше відновлення системи.
- Системи контролюючі додатки та відповідальні за блокування підозрілих додатків, ґрунтуючись у тому числі на поведінкових факторах, але не допускаючи їх впливу на основні процеси та критичні дані.
- Системи захисту пам'яті, які активно блокують всю підозрілу активність, якщо програма звертається до оперативної пам'яті.

• Системи захисту даних, які включають резервне копіювання, шифрування даних, системи, які запобігають витоку даних та борються з фішингом [9].

На ринку технологій для забезпечення кібербезпеки існує багато видів Endpoint Protection Platform, далі я розгляну Gartner Magic Quadrant for Endpoint Protection Platforms (EPP) 2021, та на його основі продемонструю приклади популярних платформ, які використовуються для захисту кінцевих точок інформаційних систем організацій (рис.1.5.).


Рис. 1.5. Gartner Magic Quadrant for Endpoint Protection Platforms 2021 [10]

Gartner вибирає для звіту 30 критеріїв залежно від можливостей рішення, 15 з яких обов'язкові. До них відносяться здатність виявляти відомі та невідомі шкідливі програми, не покладаючись на оновлення, автоматичне видалення загроз при виявленні та можливість збору даних про підозрілі події на пристроях, що працюють за межами корпоративної мережі.

Можна помітити, що квадрант поділяється на 4 секції: Претенденти, Лідери, Нішеві гравці та Провидці.

В якості прикладів я розгляну Лідерів, які не завжди задовольняють купівельні потреби кожного клієнта, але надають «широкі можливості розширеного захисту від шкідливих програм і перевірені можливості управління великих корпоративних акаунтів».

*1. McAfee Endpoint Protection.*

Програмне забезпечення McAfee Endpoint Protection – це інтегрована система захисту від шкідливого ПЗ та несанкціонованих пристроїв комп'ютерів на ОС Windows. McAfee Endpoint Protection призначений для контролю пристроїв, електронної пошти та web-безпеки на кінцевих точках інформаційних систем. Керується захист із централізованої консолі, а розгортання McAfee Endpoint Protection виконується за допомогою агента завдяки інтеграції з платформою McAfee ePolicy Orchestrator. McAfee Endpoint Protection має можливість об'єднання з іншими продуктами компанії McAfee.

*Можливості McAfee Endpoint Protection*

- Захист у режимі реального часу. Можливість блокування вірусів, черв'яків, троянів, рекламних та шпигунських програм, інших шкідливих компонентів, які створені для викрадення конфіденційних даних та порушення роботи комп'ютерів.
- Проактивний захист. Система перехоплює шкідливе програмне забезпечення та небажані листи до того, як вони потрапляють у поштову скриньку користувачів. Вбудований компонент McAfee SiteAdvisor Enterprise Plus має можливість миттєвого попередження про небезпеку при спробі користувача відкрити ненадійний ресурс. Також ця можливість допомагає адміністраторам безпеки регулювати доступ до сайтів для відповідності нормативно-правовим вимогам.
- Міжмережевий екран. Ця можливість дозволяє контролювати програми на кінцевих точках, які мають доступ до Інтернету. Вона блокує мережеві

атаки та запобігає простоям. Розгортання та менеджмент політик міжмережевого екрану здійснюються на основі розташування.

- Керування пристроями. Відбувається відстеження та обмеження копіювання даних на портативні пристрої зберігання та носії інформації.
- Централізоване керування. McAfee ePolicy Orchestrator (ePO) дає уявлення про стан безпеки системи та конкретних подій, пропонуючи можливість єдиного контролю усіх засобів безпеки та відповідності нормативно-правовим вимогам [11].

*2. Microsoft Defender для кінцевих точок.*

Microsoft Defender для кінцевих точок є провідною технологією для захисту кінцевих точок на ОС Windows, macOS, Linux, Android, iOS та мережевих пристроїв. Цей рішення є ефективним у зупиненні атак, масштабуванні ресурсів безпеки та розвиванні захисту. Дане рішення використовується у масштабі хмари, володіє вбудованим штучним інтелектом та забезпечує широкий аналіз загроз. Рішення є комплексним, воно допомагає виявити усі кінцеві точки у інформаційній системі. Є можливість керувати вразливостями, захищати кінцеві точки та протидіяти загрозам на кінцевих точках (EDR), має у складі функцію захисту від мобільних.

*Можливості рішення*

- Виявлення вразливостей та помилок у конфігураціях у реальному часі. Поєднання засобів захисту, IT та управління загрозами та вразливістю дозволяє виявити слабкі місця, ранжувати їх за серйозністю та усунути, а також при необхідності виправляти неправильні конфігурації.
- Моніторинг та аналіз загроз на професійному рівні. Користувач може залучити експертів Microsoft з протидії загрозам до центру безпеки. Існують засоби для глибокого аналізу, збільшені можливості для моніторингу загроз, аналітики та підтримки, для визначення критичних загроз.
- Автоматизація аналізу сповіщень. Аналіз усіх повідомлень відбувається автоматично, тому можна заблокувати серйозні атаки максимально

швидко. Застосування кращих методик та інтелектуальних алгоритмів прийняття рішень дозволяє визначати активні загрози та заходи, які слід вжити.

- Блокування складних загроз та програм. Засоби наступного покоління допоможуть захистити компанію від файлових та безфайлових загроз. Також можна встановити захист від поліморфних та метаморфних шкідливих програм.
- Виявлення та реагування на складні атаки. Виявлення атак та загроз нульового дня буде легшим за допомогою машинного навчання та аналізу поведінки [12].

*3. Sophos Central Endpoint Intercept X* .

Sophos Central Endpoint Intercept X являється рішенням для несигнатурного захисту від здирників, експлойтів, також має функції аналізу головних загроз, аби захистити кінцкві точки від поширених зароз. Не дає зловмисникам самовільно шифрувати дані з використанням програм вимагачів, навідь якщо це довірені файли ибо процеси, які все було запущено. Рішення сфокусовано на невеликому наборі методів, що використовуються для пошерря шкідливого ПЗ, таким чином захощаючі концеві точки від атак нульового дня.

*Особлвості Sophos Central:*

- Показники загроз, що є додатковими, наприклад, підозрілий трафік у мережі, одразу ж діляться між Next-Gen Firewall і Next-Gen Endpoint, аби виявити та запобігти атакам.
- Можливість активно ідентифікувати системні імена комп'ютерів, користувачів і шляхів між кінцевими точками та брандмауером, що було скомпроментовано, для швидкого вжавання заходів захисту.
- Кінцеві точки, що було зламано, брандмауер автоматично ізолює, а в цей час кінцева точка зупинає та видаляє шкідливе ПЗ. Дана можливість допомагає економити час IT-фахівців і гроші завдяки автоматичному реагуванню на події.

*Особливості Sophos Endpoint:*

- Має у своєму складі іноваційну безпеку, що включає захист від шкідливого ПЗ, Host-based Intrusion Prevention System (HIPS) та мовливість віявляти шкідливий трафік.
- Користувачі, що виходять за межі корпоративної мережі проходять фільтрацію.
- Зупинка програм крипто-вимагачів [13].

*4. CrowdStrike Falcon Endpoint Protection.*

Falcon Endpoint Protection є гнучкою, що масштабуємою хмарною платформою, яка захищає кінцеві точки (EPP).

Дане рішення має у своєму складі розширені функції, які виявляють, запобігають і реагують на вірусні атаки і мають відповіді на інциденти. Falcon Endpoint Protection заснований на штучному інтелекті, який поєднує сучасні технології, інтелект та досвід в одне рішення.

*Ключові можливості Falcon Endpoint Protection:*

- Посилена технологія запобігання з повною видимістю атак AI NGAV. Забезпечується захист від різних атак без необхідності оновлення. Використовуються найкращі методики запобігання загрозам, до яких належить машинне навчання, індикатори атаки. Це дозволяє зупиняти безфайлові атаки. Продукт усуває загрози після традиційних антивірусів та захищає кінцеві точки в онлайн та в офлайн режимах.
- Розширена видимість атаки. Спрощений процес розподілу атаки з вмістом контекстних даних інструментами Threat Intelligence. Інформативність та оповіщення удосконалені, а всі дані про виявлені загрози зберігаються 90 днів.
- Контроль пристроїв. Докладно можна побачити як використовувався USB-пристрій. Є можливість повного контролю використання USB-пристроїв.
- Технологія Threat Intelligence. Під час визначення погроз відбувається виявлення пріоритетів за допомогою оцінки ступеня серйозності небезпеки. Складність та вплив загроз у мережі визначається автоматично.

- Міжмережевий екран. Ця можливість допомагає забезпечити захист від мережевих загроз. Міжмережевий екран допомагає бачити погрози, щоб підвищувати захист і інформувати про небезпеку.
- Контроль та реакція. Швидкий віддалений доступ до кінцевої точки допомагає моментально нейтралізувати загрози [14].

Розглянувши рішення, що є лідерами у сфері захисту кінцевих точок інформаційних систем організацій, я хочу звернути увагу на «Нішевих гравців» з квадранта Gartner.

«Нішеві гравці», за визначенням Gartner, надають користувачам необхідні можливості, але вони часто обмежуються послугами для певних географічних регіонів або клієнтів певних розмірів; це означає, що вони можуть бути надійним вибором для підприємств, які потрапляють до їх спеціалізованих сценаріїв використання.

Далі у роботі я розгляну рішення Panda Adaptive Defense 360, що входить до комплексної платформи Panda Security, яка увійшла до квадранту Gartner як «Нішевий гравець».

# 2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ PANDA ADAPTIVE DEFENSE 360

## 2.1. Призначення, можливості та функції Panda Adaptive Defense 360

У попередньому розділі було з’ясовано, що захист кінцевих точок інформаційної системи організації є важливим питанням для забезпечення інформаційної безпеки компанії. Рішення Panda Adaptive Defense 360 добре підходить для цієї задачі. Даний продукт є комплексним рішенням безпеки, що надає функції запобігання, виявлення та реагування на будь-які види загроз безпеки на кінцевих точках: робочих станціях, серверах та ноутбуках усередині та за межами корпоративної мережі. Автоматизує всі ці процеси на будь-які існуючі та майбутні складні загрози, невідоме шкідливе ПЗ, шифрувальників, фішинг, експлойти, а також атаки без використання шкідливих програм усередині та за межами корпоративної мережі.

Рішення інтегрує всі доступні технології превентивного захисту кінцевих пристроїв (EPP) та передові функції автоматичного виявлення атак та реагування на них (EDR) в єдиному легкому агенті. Плюс, рішення надає два унікальні на ринку керовані сервіси безпеки, включені в рішення:

- 100% Attestation Service для класифікації всіх програм та процесів, запущених на кінцевих пристроях.
- Threat Hunting Service проти зовнішніх хакерських та внутрішніх інсайдерських атак.

*Можливості Panda Adaptive Defense 360*

Panda Adaptive Defense 360 надає компаніям гарантований захист від складних загроз та цільових атак. В його основі лежать чотири принципи:

- Видимість: існує можливість відстежувати кожну дію, яка виконується запущеними програмами.

- Виявлення: відбувається постійний моніторинг запущених процесів та блокування в реальному часі атак нульового дня та цільових атак, а також інших складних загроз, які призначені для обходу традиційних антивірусних рішень.
- Виправлення та відповідь: збирається інформація для поглибленого аналізу кожної спроби атаки, а також засоби її виправлення.
- Запобігання: запобігання майбутнім атакам редагування налаштувань різних модулів захисту та виправлення вразливостей, виявлених у встановлених операційних системах та програмах (рис.2.1.).


Рис. 2.1. Підхід до захисту в рішенні Panda Adaptive Defense 360

Panda Adaptive Defense 360 поєднує традиційні технології захисту кінцевих пристроїв (EPP) з інноваційними технологіями адаптивного захисту, виявлення та реагування (EDR), що дозволяє IT-спеціалістам справлятися з передовими кібер-загрозами.

Традиційні превентивні технології захисту:

- Персональний або керований фаєрвол (IDS)
- Контроль пристроїв

- Колективний розум
- Білі списки/чорні списки
- Постійний захист від шкідливого ПЗ та перевірки на запит
- Евристика до виконання процесів
- URL-фільтрація – веб-захист
- Антифішинг
- Анти-тамперінг
- Відновлення та відкат

Розширені технології захисту:

- Безперервний моніторинг пристроїв за допомогою EDR;
- Хмарний штучний інтелект, який навчається класифікувати 100% процесів (APT, шифрувальники, руткіти тощо);
- Пісочниці у реальних оточеннях;
- Захист від експлойтів;
- Функції Threat Hunting, включаючи поведінковий аналіз та виявлення індикаторів атак IoA для виявлення атак типу living off the land (LotL);
- Індикатори атак відповідно до матриці MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge);
- Виявлення та запобігання атакам RDP (атак brute force);
- Стримування та відновлення: ізоляція комп'ютера, блокування програм хешу або назви тощо.

Цінність даного рішення з опціями розширеного захисту ґрунтується на чотирьох принципах:

- Запобігання, виявлення та реагування на атаки, що використовують шкідливе ПЗ чи ні;
- Видимість у реальному часі та ретроспективі всієї докладної інформації про всі процеси на кінцевих пристроях;
- Класифікація 100% процесів: 99,98% - машинне навчання, 0,02% - експерти та аналітики Panda;

- Threat Hunting та Експертний аналіз атак виконуються аналітиками Panda Security та MSSP (постачальниками послуг керованої безпеки).

Поєднання цих рішень та сервісів забезпечує докладний огляд всіх процесів на кожному кінцевому пристрої, повний контроль усіх запущених процесів та скорочення схильності до атаки [15].

***Переваги рішення Panda Adaptive Defense 360***

- Дане рішення легко у використанні та управлінні, що буде розглянуто далі, а його захист високий. Усі послуги автоматизовані та знижують витрати на висококваліфікований персонал. Немає необхідності керувати неправдивими спрацьовуваннями, всі процеси автоматизовані.
- Для встановлення та налаштування не потрібна локальна інфраструктура. Рішення не впливає на продуктивність кінцевих точок, адже воно засноване на легкому агенті та хмарній архітектурі.
- Всі потреби захисту кінцевих пристроїв покриваються простим керуванням через єдину вебконсоль.
- Легко впровадити та налаштувати на кінцевих пристроях з різними операційними системами.
- Інтуїтивно зрозумілий інтерфейс керування.

Рішення Panda Adaptive Defense 360 має автоматизовані функції EDR:

- Виявляє та блокує хакерські техніки, тактики та процедури, та експлойти до виникнення проблем.
- Є можливість розслідування та реагування: експертна аналітика для глибокого розслідування кожної атаки та інструменти пом'якшення наслідків.
- Відстеження кожної дії: зрозуміла видимість хакера та його дій, що спрощує розслідування інциденту [16].

Panda Adaptive Defense 360 ґрунтується на декількох технологіях захисту, воно дозволяє організаціям замінити традиційне антивірусне рішення, встановлене в їхній мережі, повноцінною керованою службою безпеки:

*1. Рішення дозволяє запускати лише легітимне ПЗ*

Panda Adaptive Defense 360 відстежує та класифікує всі процеси, що виконуються на кінцевих пристроях у мережі організації, залежно від їхньої поведінки та характеру. Служба захищає робочі станції та сервери, дозволяючи запускати лише ті програми, які класифікуються як довірені. Рішення адаптується до середовища організації.

*2. Оцінка та усунення проблем безпеки*

Пропозиція безпеки рішення доповнюється інструментами моніторингу, криміналістичного аналізу та виправлення, що дозволяють адміністраторам визначати обсяг інцидентів безпеки та вирішувати їх.

Безперервний моніторинг надає цінну інформацію про контекст, у якому були виявлені проблеми. Ця інформація дозволяє адміністраторам оцінювати вплив інцидентів та вживати необхідних заходів для запобігання їх повторенню.

*3. Кросплатформовий сервіс*

Panda Adaptive Defense 360 є хмарним кросплатформним сервісом, який сумісний з Windows, macOS, Linux та Android, а також із постійними та непостійними середовищами VDI (Virtual Desktop Infrastructure). Таким чином, рішення є єдиним інструментом, який відповідає вимогам безпеки всіх комп'ютерів у корпоративній мережі. Він надає адміністраторам єдиний інструмент для безпеки всіх кінцевих точок в організації без необхідності встановлювати нову інфраструктуру управління і тим самим знижувати загальну вартість володіння.

***Ключові функції Panda Adaptive Defense 360***

- Технології запобігання, виявлення, реагування та керовані сервіси безпеки проти: 1) відомих та невідомих загроз (шифрувальники, трояни, хробаки, APT); 2) експлойтів (атак через пам'ять) та атак з використанням адміністративних утиліт; 3) зовнішніх хакерських та внутрішніх інсайдерських атак.
- Машинне навчання у хмарному середовищі Великих даних (Big Data).
- Керовані сервіси безпеки без прихованих або додаткових витрат.
- Видимість активності процесів та додатків у реальному часі.
- Швидке та прозоре впровадження та встановлення.
- Хмарна веб-консоль централізованого керування.

- Оповіщення у реальному часі. Детальний звіт для керівників.

*Додаткові функції Panda Adaptive Defense 360:*

- Інструменти віддаленого відновлення та реагування на атаки.
- Файєрвол, IDS/IPS.
- Контроль пристроїв та URL-фільтрація [17].

## 2.2. Можливості, переваги та архітектура платформи Aether

Рішення Panda Adaptive Defense 360 управляється за допомогою платформи та хмарної веб-консолі Aether, яка була створена для віддаленого та централізованого управління корпоративними рішеннями безпеки Panda.

Aether є платформою управління, зв'язку та обробки даних, розроблена Panda Security та призначена для централізації послуг, спільних для всіх продуктів компанії.

Платформа Aether управляє зв'язком з агентами, розгорнутими у мережі. Консоль управління представляє дані, зібрані Panda Adaptive Defense 360, у найпростішій та зрозумілій формі для подальшого аналізу адміністратором мережі.

***Можливості платформи Aether***

Модульна конструкція рішення позбавляє організації необхідності встановлювати на кінцеві точки нові агенти або продукти для будь-якого нового придбаного модуля. Всі продукти Panda Security, що працюють на платформі Aether, використовують один і той же агент на кінцевих точках клієнтів, а також ту саму веб-консоль управління, що полегшує управління продуктами та мінімізує споживання ресурсів.

***Ключові переваги Aether***

Нижче будуть розглянуті основні послуги, які надає Aether для всіх сумісних продуктів:

*1. Платформа управління хмарою*

Aether є хмарною платформою з низкою значних переваг з точки зору використання, функціональності та доступності.

- Не потрібно, щоб сервери керування розміщували консоль управління на території клієнта: оскільки вона працює з хмари, до неї можуть безпосередньо звертатися всі пристрої, підписані на послугу, з будь-якого місця та в будь-який час, незалежно від того, чи вони знаходяться в офісі або в дорозі.
- Мережеві адміністратори можуть отримати доступ до консолі керування в будь-який момент та з будь-якого місця, використовуючи будь-який

сумісний інтернет-браузер з портативного комп'ютера, настільного комп'ютера або навіть мобільних пристроїв, таких як планшети або смартфони.

- Це платформа високої доступності, що працює на 99,99% часу. Мережним адміністраторам не потрібно розробляти та розгортати дорогі системи з надмірністю для розміщення інструментів управління.

*2. Зв'язок із платформою в реальному часі*

Надсилання налаштувань та запланованих завдань на мережеві пристрої виконується в режимі реального часу, коли адміністратори використовують нові налаштування до вибраних пристроїв. Адміністратори можуть відразу налаштувати параметри безпеки, усунути порушення безпеки або адаптувати службу безпеки до динамічної корпоративної IT-інфраструктури.

*3. Мультипродукція та кросплатформеність*

Через інтеграцію продуктів Panda Security в єдину платформу у адміністраторів з'являється багато переваг:

- Мінімізація кривої навчання: всі продукти використовують ту саму платформу, що скорочує час, необхідний адміністраторам для навчання використанню нового інструменту, що, у свою чергу, знижує сукупну вартість володіння.

- Єдине розгортання для кількох продуктів: на кожному пристрої потрібна лише одна програма для забезпечення функціональності всіх продуктів, сумісних із платформою Aether. Це мінімізує споживання ресурсів на пристроях користувачів, порівняно з окремими продуктами.

- Велика сумісність між продуктами: всі продукти надають звіти через одну консоль: адміністратори мають єдину панель управління, на якій вони можуть бачити всі згенеровані дані, що скорочує час та зусилля, які витрачаються на підтримку кількох незалежних репозиторіїв інформації та об'єднання інформації, отриманої з різних джерел .

- Сумісність з кількома платформами: більше немає необхідності інвестувати в ряд продуктів, щоб охопити весь спектр пристроїв, що використовуються компанією: платформа Aether підтримує Windows, Linux,

macOS та Android, а також постійні та непостійні віртуальні пристрої та середовища VDI.

*4. Гнучкі та детальні налаштування*

Нова модель конфігурації прискорює керування пристроями за рахунок повторного використання профілів налаштування та використання певних механізмів, таких як спадкування та призначення налаштувань окремим кінцевим точкам. Мережеві адміністратори можуть призначати більш детальні та конкретні налаштування з меншими зусиллями.

*5. Повна індивідуальна інформація*

Платформа Aether реалізує механізми, які дозволяють налаштовувати обсяг даних, що відображаються у широкому діапазоні звітів, залежно від потреб адміністратора або кінцевого користувача інформації.

Ця інформація доповнюється даними про мережеві пристрої, встановлене обладнання та програмне забезпечення, а також журнал змін, який допомагає адміністраторам точно визначати стан безпеки мережі.

***Архітектура платформи Aether***

Архітектура Aether призначена для масштабування, щоб пропонувати гнучкі та ефективні послуги. Інформація надсилається і виходить у реальному часі з багатьох джерел та пунктів призначення одночасно. Це можуть бути кінцеві точки, пов'язані зі службою, зовнішні споживачі, такі як Security information and event management (SIEM) або поштові сервери, або веб-екземпляри для запитів на зміну конфігурації та подання інформації адміністраторам мережі.

Більш того, Aether реалізує рівень серверної частини та сховища, що реалізує широкий спектр технологій, що дозволяють ефективно обробляти численні типи даних.

На малюнку показано високорівневу діаграму платформи Aether (рис.2.2.).

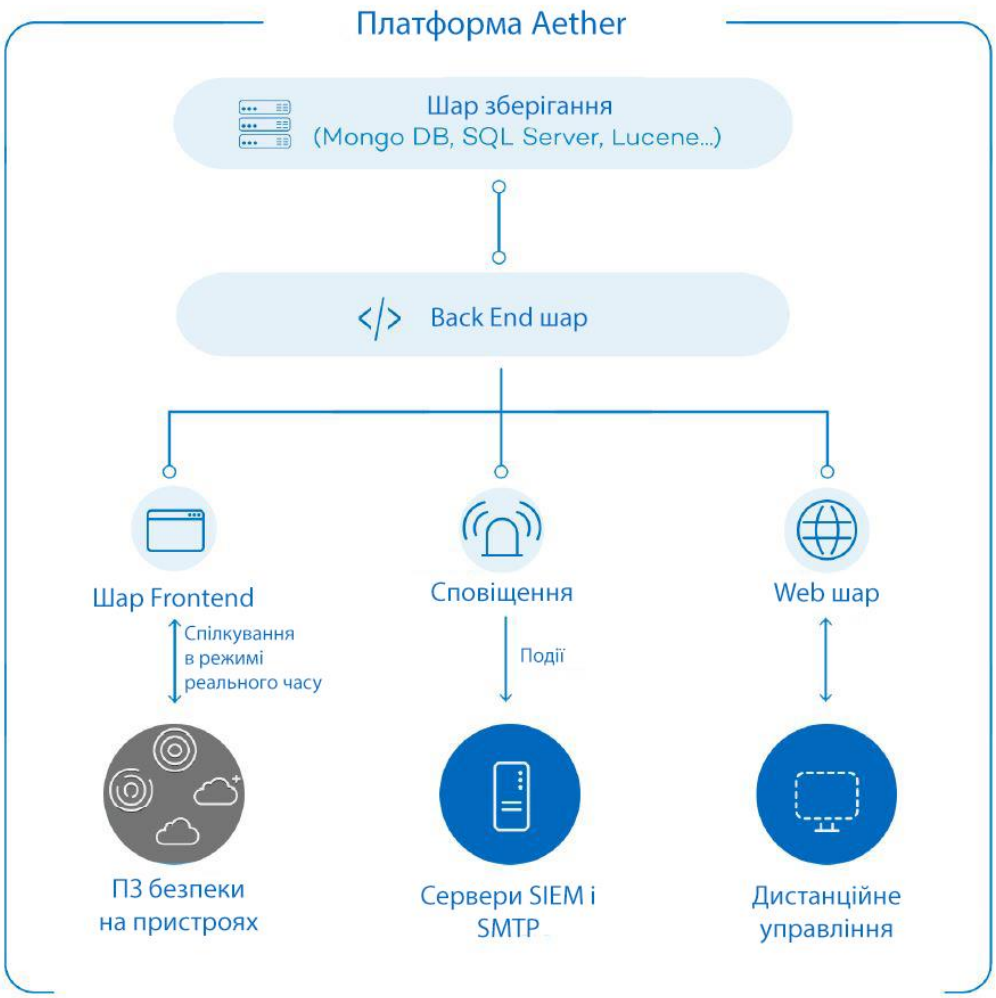


Рис. 2.2. Логическая структура платформы Aether

*Aether на комп'ютерах користувачів*

На мережевих комп'ютерах, які знаходяться під захистом Panda Adaptive Defense 360, встановлено програмне забезпечення, що складається з двох незалежних, але пов'язаних модулів, які забезпечують всі функції захисту та управління.

- Модуль агента зв'язку Panda (агент Panda): він діє як міст між модулем захисту та хмарою, керуючи зв'язком, подіями та налаштуваннями безпеки, які реалізує адміністратор з консолі управління.
- Модуль захисту Panda Adaptive Defense 360: відповідає за забезпечення ефективного захисту комп'ютера користувача. Для цього він використовує

комунікаційний агент для отримання профілів налаштувань і відправки статистики та інформації про виявлення, а також відомостей про елементи, що скануються.

***Агент зв'язку у реальному часі Panda***

Агент Panda забезпечує обмін даними між керованими комп'ютерами та сервером Panda Adaptive Defense 360. Він також встановлює діалог між кінцевими пристроями, що належать до однієї мережі в інфраструктурі клієнта.

Цей модуль керує процесами вирішення безпеки та збирає зміни конфігурації, зроблені адміністратором через веб-консоль, та застосовує їх до модуля захисту.

Зв'язок між пристроями та Command Hub здійснюється через постійні з'єднання WebSocket у реальному часі (рис.2.3.). Для кожного комп'ютера встановлюється з'єднання для надсилання та отримання даних. Щоб проміжні пристрої не закривали з'єднання, створюється постійний поток пакетів підтримки активності.

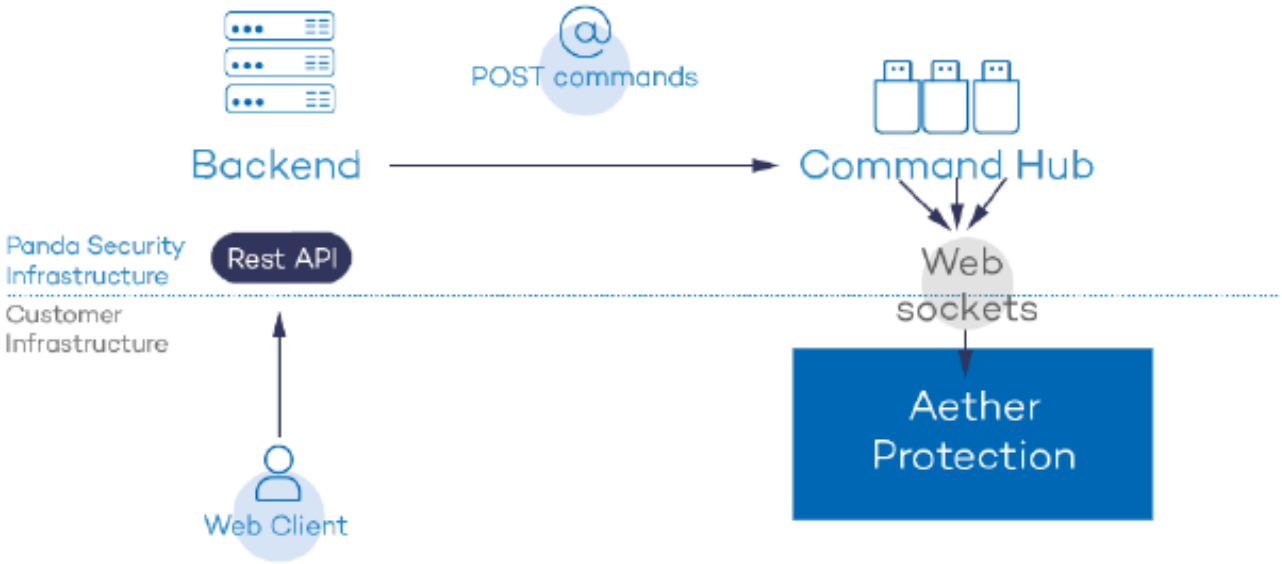


Рис. 2.3. Блок-схема команд, що вводяться через консоль управління

Налаштування, що вносить мережний адміністратор через консоль керування Panda Adaptive Defense 360, надсилаються на серверну частину через REST API. Бекенд, у свою чергу, пересилає їх у Command Hub, генеруючи команду POST, яка надсилає інформацію на всі керовані пристрої. Ця інформація

передається миттєво, якщо лінії зв'язку не перевантажені та кожен проміжний елемент працює належним чином.

## 2.3. Компоненти та сервіси рішення Panda Adaptive Defense 360

Panda Adaptive Defense 360 є сервісом, який відповідає за інформаційну безпеку та заснований на аналізі поведінки процесів, що виконуються на комп'ютерах в IT-інфраструктурі кожного клієнта. Цей аналіз виконується з допомогою методів машинного навчання серед великих даних, розміщених у хмарі.

Далі на малюнку показано загальну структуру рішення Panda Adaptive Defense 360 та його компонентів (рис.2.4.):

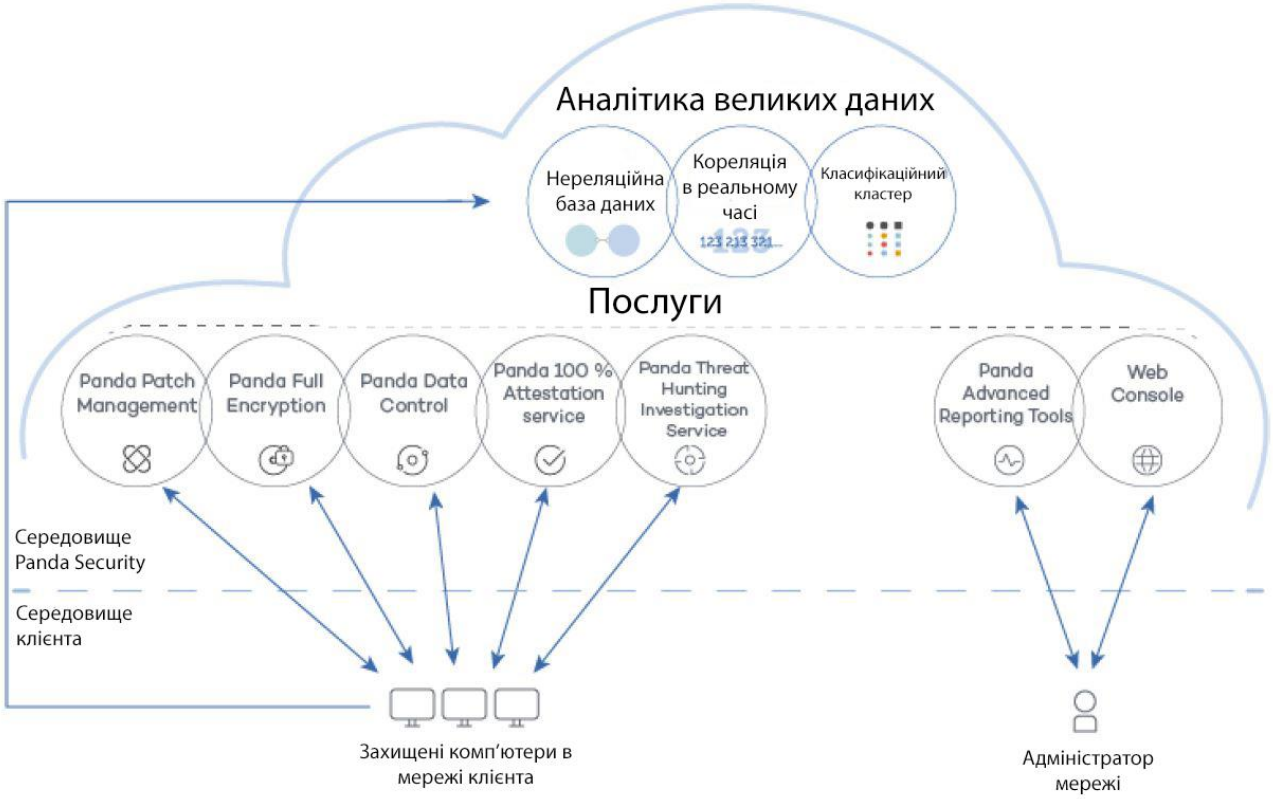


Рис. 2.4. Загальна структура Panda Adaptive Defense 360

- Інфраструктура аналітики великих даних: складається з нереляційних баз даних, сервісів, які корелюють події, що відстежуються в режимі реального часу, і класифікаційного кластера для відстежуваних процесів.
- Служба програм з нульовою довірою: класифікує всі процеси, що виконуються на комп'ютерах Windows, без двозначності або помилкових спрацьовувань/заперечень.

- Служба розслідування погроз: служба перехресного розслідування, включена до базової ліцензії на продукт. Він виявляє невідомі загрози та атаки LotL. Ці цільові атаки призначені для обходу захисту, встановлених на комп'ютерах.
- Panda SIEMFeeder (не є обов’язковою): інтегрує Panda Adaptive Defense 360 зі сторонніми інструментами SIEM.
- Служба Panda Data Control (не є обов'язковою): служба пошуку, інвентаризації та моніторингу особистої інформації, що зберігається у файлах PII.
- Служба Panda Advanced Reporting Tool (не є обов'язковою): служба звітів для створення розширених аналітичних даних безпеки.
- Служба Panda Patch Management (не є обов'язковою): служба для виправлення операційних систем Windows та сторонніх програм.
- Служба Panda Full Encryption (не є обов'язковою): шифрує внутрішні запам'ятовуючі пристрої комп'ютерів Windows, щоб мінімізувати розкриття даних у разі втрати або крадіжки, а також при видаленні запам'ятовуючих пристроїв без видалення вмісту.
- Веб-консоль: сервер консолі керування.
- Комп'ютери, захищені встановленим програмним забезпеченням (Panda Adaptive Defense 360).
- Комп'ютер адміністратора мережі, який має доступ до веб-консолі.

***Інфраструктура аналітики великих даних***

Є хмарним кластером серверів, який отримує телеметрію, згенеровану на комп'ютерах в мережі клієнта. Ця телеметрія складається з дій, що виконуються програмами користувача, що відстежуються модулем захисту, їх статичних атрибутів та інформації про контекст виконання. Все це забезпечує постійний потік інформації, яка сканується у хмарі з використанням методів штучного інтелекту для оцінки поведінки програм та видачі класифікації кожного запущеного процесу. Ця класифікація повертається модулю захисту, встановленому на кожному комп'ютері, і використовується як основа для виконання дій, необхідних для забезпечення захисту комп'ютера.

Ця хмарна модель дає безліч переваг у порівнянні з методологією, яка використовується традиційними антивірусами, які відправляють зразки антивірусу для ручного аналізу:

- Кожен процес, що виконується на захищених комп'ютерах, відстежується та аналізується: це усуває невизначеність, властиву традиційним антивірусним рішенням, які можуть розпізнавати шкідливі об'єкти, але не можуть ідентифікувати інші програми.
- Затримка в класифікації процесів, що спостерігаються вперше (вікно можливостей для шкідливих програм), мінімальна, оскільки Panda Adaptive Defense 360 відправляє дії, що запускаються кожним процесом, у режимі реального часу на сервери. Хмарні сервери Panda постійно працюють над діями, що збираються датчиками, що значно скорочує затримку у видачі класифікації та час, протягом якого комп'ютери зазнають загроз.
- Безперервний моніторинг кожного процесу дозволяє Panda Adaptive Defense 360 класифікувати як шкідливі об'єкти, які спочатку поводилися як хороше ПЗ. Це типово для цільових атак та інших складних загроз, які діють непомітно.
- Хмарне сканування звільняє користувачів від необхідності встановлювати та обслуговувати виділену апаратну та програмну інфраструктуру.

*Адміністрування через веб-консоль*

Веб-консоль сумісна з більшістю популярних інтернет-браузерів і доступна у будь-який час та в будь-якому місці з будь-якого пристрою з підтримуваним браузером.

Веб-консоль адаптивна, тобто її можна без проблем використовувати на смартфонах та планшетах.

*Комп'ютери захищені Panda Adaptive Defense 360*

Panda Adaptive Defense 360 потребує встановлення невеликого програмного компонента на всіх кінцевих точках в мережі, схильних до проблем з безпекою. Цей компонент складається з двох модулів: агента зв'язку Panda та модуля захисту Panda Adaptive Defense 360.

Модуль захисту Panda Adaptive Defense 360 містить технології, що призначені для захисту комп'ютерів клієнтів. Panda Adaptive Defense 360 надає в одному продукті все необхідне для виявлення цільових шкідливих програм та шкідливих програм нового покоління (APT), а також інструменти управління продуктивністю та виправлення для лікування компрометованих комп'ютерів та оцінки впливу спроб вторгнення.

***Сервіси Panda Adaptive Defense 360***

Panda Security надає інші послуги, деякі з яких є необов'язковими, які дозволяють користувачам інтегрувати рішення у свою поточну IT-інфраструктуру та безпосередньо отримувати вигоду з аналітики безпеки.

*Служба додатків із нульовою довірою*

Ця служба, включена в стандартний продукт для комп'ютерів Windows, призначена для виконання тільки тих програм, які сертифіковані Panda Security. Для цього вона використовує комбінацію локальних технологій на комп'ютері користувача та хмарних технологій в інфраструктурі великих даних. Ці технології дозволяють автоматично класифікувати 99,98% всіх запущених процесів. Відсоток, що залишається, вручну класифікується експертами з шкідливих програм. Такий підхід дозволяє класифікувати 100 відсотків усіх двійкових файлів, які виконуються на комп'ютерах користувачів, без створення помилкових спрацьовувань або помилкових заперечень.

Всі файли, що виконуються, виявлені на комп'ютерах користувачів, які невідомі Panda Adaptive Defense 360, відправляються в інфраструктуру аналітики великих даних Panda Security для аналізу.

*Служба розслідування загроз*

Служба, яка виявляє атаки та загрози LotL, призначені для обходу засобів захисту, встановлених на комп'ютерах. Ця послуга використовує продукт Orion, передову платформу Threat Hunting, розроблену Panda Security.

Завдяки телеметрії, що надсилається з комп'ютерів, Orion виконує крос-аналітику процесів, що виконуються в IT-інфраструктурах клієнтів, для виявлення нових загроз та створення розширених правил полювання. Коли індикатор атаки

виявляється, він підтверджується командою експертів з кібербезпеки Panda Security. Після перевірки Panda Adaptive Defense 360 показує пов'язаний індикатор атаки (IOA) у консолі разом з описом його характеристик та рекомендаціями для адміністратора щодо вирішення ситуації.

*Послуга Panda Advanced Reporting Tool (не є обов'язковою)*

Panda Adaptive Defense 360 автоматично та прозоро надсилає всю інформацію, зібрану з комп'ютерів користувачів, до Panda Advanced Reporting Tool, системи зберігання та використання знань.

Усі дії, ініційовані процесами, що виконуються в IT-мережі, надсилаються до Panda Advanced Reporting Tool, де вони співвідносяться та аналізуються для отримання інформації про безпеку. Це надає адміністраторам додаткову інформацію про загрози та те, як користувачі використовують корпоративні комп'ютери. Ця інформація подається найбільш гнучким і наочним способом, щоб полегшити її розуміння.

Служба Panda Advanced Reporting Tool доступна безпосередньо з інформаційної панелі веб-консолі Panda Adaptive Defense 360.

*Послуга Panda SIEMFeeder (не є обов'язковою)*

Panda Adaptive Defense 360 легко інтегрується із сторонніми рішеннями SIEM, встановленими клієнтами на їхній IT-інфраструктурі. Діяльність, яку виконують програми, що запускаються в мережі, доставляють на сервер SIEM, готовий до використання та збагачений знаннями, наданими Panda Adaptive Defense 360.

Системи SIEM, сумісні з Panda Adaptive Defense 360:

- QRadar;
- AlienVault;
- ArcSight;
- LookWise;
- Bitacora.

*Послуга Panda Data Control (не є обов'язковою)*

Це модуль безпеки, інтегрований у платформу Panda Adaptive Defense 360, призначений для того, щоб допомогти організаціям дотримуватися застосовних правил захисту даних, які регулюють зберігання та обробку персональної інформації (PII).

Panda Data Control виявляє, перевіряє та відстежує в режимі реального часу повний життєвий цикл файлів PII, що зберігаються на комп'ютерах Windows: від даних у стані спокою до даних, що використовуються (операції, що здійснюються над особистими даними) і даних у русі (вилучення даних). На основі цієї інформації Panda Data Control створює інвентар, який показує зміну кількості файлів з персональними даними, знайдених на кожній кінцевій точці в мережі.

*Послуга Panda Patch Management (необов'язково)*

Ця служба зменшує поверхню атак на робочі станції та сервери Windows в організації, оновлюючи знайдене вразливе програмне забезпечення (операційні системи та сторонні програми) за допомогою патчів, випущених відповідними постачальниками.

Крім того, вона знаходить усі програми в мережі, які досягли стадії EOL (End-Of-Life). Ці програми становлять загрозу, оскільки вони більше не підтримуються відповідним постачальником і є основною ціллю для хакерів, які прагнуть використати відомі невиправлені вразливості. За допомогою Panda Patch Management адміністратори можуть легко знайти всі програми EOL в організації та розробити стратегію для контрольованого видалення цього типу програмного забезпечення.

Крім того, у разі конфліктів сумісності або несправності виправлених програм Panda Patch Management дозволяє організаціям відкатувати/видаляти ті виправлення, які підтримують цю функцію, або виключати їх із завдань встановлення, запобігаючи їх інсталяцію.

*Послуга повного шифрування Panda (не є обов'язковою)*

Можливість шифрувати інформацію, що зберігається у внутрішніх пристроях зберігання комп'ютерів у мережі, є ключем до захисту збережених даних у разі втрати чи крадіжки або коли організація переробляє пристрої зберігання даних, не

видаляючи їх повністю. Panda Security використовує технологію Windows BitLocker для шифрування вмісту жорсткого диска на рівні сектора, централізовано керуючи ключами відновлення у разі втрати або зміни конфігурації обладнання.

Модуль Panda Full Encryption дозволяє використовувати модуль довіреної платформи (TPM), якщо він доступний, і надає кілька варіантів аутентифікації, додаючи гнучкості захисту даних комп'ютера.

***Профіль користувача продукту***

Незважаючи на те, що Panda Adaptive Defense 360 – це керована служба, яка забезпечує безпеку без втручання адміністратора мережі, вона також надає чітку та детальну інформацію про активність процесів, які виконують всі користувачі в мережі організації. Ці дані можуть використовуватися адміністраторами безпеки для чіткої оцінки впливу проблем безпеки та адаптації протоколів компанії для запобігання подібним ситуаціям у майбутньому.

У цьому розділі були розглянуті призначення, можливості та функції рішення Panda Adaptive Defense 360. Також було приділено увагу можливостям, перевагам та архітектурі платформи Aether, яка є хмарною веб консоллю та призначена для управління рішенням Panda Adaptive Defense 360. Були визначені основні компоненти та сервіси рішення.

Далі більш детально будуть розглянуті вимоги для інсталяції рішення, його функціонал та рекомендації по використанню для захисту кінцевих точок інформаційної системи організації.

# 3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ НА БАЗІ РЕШЕННЯ PANDA ADAPTIVE DEFENSE 360

## 3.1. Вимоги для системи для інсталяції Panda Adaptive Defense 360

Більшість інформації про безпеку, яку генерує та використовує Panda Adaptive Defense 360, створюється у хмарі. Ці дані завантажуються та використовуються програмним забезпеченням безпеки, встановленим на кінцевих пристроях. Щоб програмне забезпечення безпеки працювало правильно, IT-інфраструктура має відповідати таким вимогам.

***Вимоги для платформ Windows***

*Операційні системи, що підтримуються*

1. Робочі станції з мікропроцесором x86 чи x64

- Windows XP SP3 (32-bit)
- Windows Vista (32-bit і 64-bit)
- Windows 7 (32-bit і 64-bit)
- Windows 8 (32-bit і 64-bit)
- Windows 8.1 (32-bit і 64-bit)
- Windows 10 (32-bit і 64-bit)

2. Комп'ютери з мікропроцесором ARM

- Windows 10 Pro
- Windows 10 Home

3. Сервери з мікропроцесором x86 або x64

- Windows 2003 (32-bit, 64-bit і R2) SP2 та вище
- Windows 2008 (32-bit і 64-bit) і 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016 і 2019

- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 і 2019

4. Інтернет речей та Windows Embedded IndustryWindows XP Embedded

- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64 bits)
- Windows Embedded Standard 2009, 7, 7 (64 bits), 8, 8 (64 bits),
- Windows Embedded Pro 8, 8 (64 bits)
- Windows Embedded Industry 8, 8 (64 bits), 8.1, 8.1 (64 bits)
- Windows IoT Core 10, 10 (64 bits)
- Windows IoT Enterprise 10, 10 (64 bits)

5. Вимоги до обладнання

- Процесор: x86 або x64-сумісний процесор із підтримкою SSE2;
- Оперативна пам'ять: 1 ГБ;
- Вільне місце на жорсткому диску: 650 МБ.

Для правильної роботи продукту необхідно підтримувати кореневі сертифікати робочих станцій і серверів. Якщо ця вимога не виконується, деякі функції, такі як здатність агентів встановлювати зв'язок у реальному часі з консоллю управління або модулем Panda Patch Management, можуть не працювати.

***Вимоги до платформ Windows Exchange***

*Підтримувані операційні системи*

- Exchange 2003: Windows Server 2003 (32- bit) SP2 та пізніші і Windows Server 2003 R2 (32- bit)
- Exchange 2007: Windows Server 2003 (64-bit) SP2 та пізніші, Windows Server 2003 R2 (64-bit),
- Windows 2008 (64-bit) і Windows 2008 R2
- Exchange 2010: Windows 2008 (64-bit) і Windows 2008 R2
- Exchange 2013: Windows Server 2012 і Windows Server 2012 R2
- Exchange 2016: Windows Server 2012, Windows Server 2012 R2 і Windows Server 2016.
- Exchange 2019: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 і Windows Server 2019.

*Підтримувані версії Exchange*

- Microsoft Exchange Server 2003 Standard і Enterprise (SP1/SP2)
- Microsoft Exchange Server 2007 Standard і Enterprise (SP0/SP1/SP2/SP3)
- Microsoft Exchange Server 2007 входить до складу Windows SBS 2008
- Microsoft Exchange Server 2010 Standard and Enterprise (SP0/SP1/SP2)
- Microsoft Exchange Server 2010 входить до складу Windows SBS 2011
- Microsoft Exchange Server 2013 Standard і Enterprise
- Microsoft Exchange Server 2016 Standard і Enterprise
- Microsoft Exchange Server 2019 Standard у Enterprise

***Вимоги до платформ macOS***

*Підтримувані операційні системи*

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11.0 Big Sur

*Вимоги до обладнання*

- Процесор: Intel® Core 2 Duo
- ОЗУ: 2 ГБ
- Доступне місце на жорсткому диску для встановлення: 400 МБ
- Порти: порти 3127, 3128, 3129 і 8310 повинні бути доступні для роботи веб-фільтрації та виявлення шкідливих програм.

***Вимоги до платформ Android***

*Підтримувані операційні системи*

- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0

- Pie 9.0
- Android 10
- Android 11

*Вимоги до обладнання*

На цільовому пристрої потрібно мінімум 10 МБ внутрішньої пам'яті. Залежно від моделі, можливо, необхідний простір буде більше [18].

Для використання рішення, спочатку треба створити акаунт та авторизуватися у хмарній консолі управління Aether. Наступним кроком, на сторінці вибору облікового запису, потрібно вибрати зі списку продуктів Panda Adaptive Defense 360 with Advanced Reporting Tool, це рішення у мене одне і в демо-версії (рис.3.1.). Далі необхідно погодитися з ліцензійною угодою.

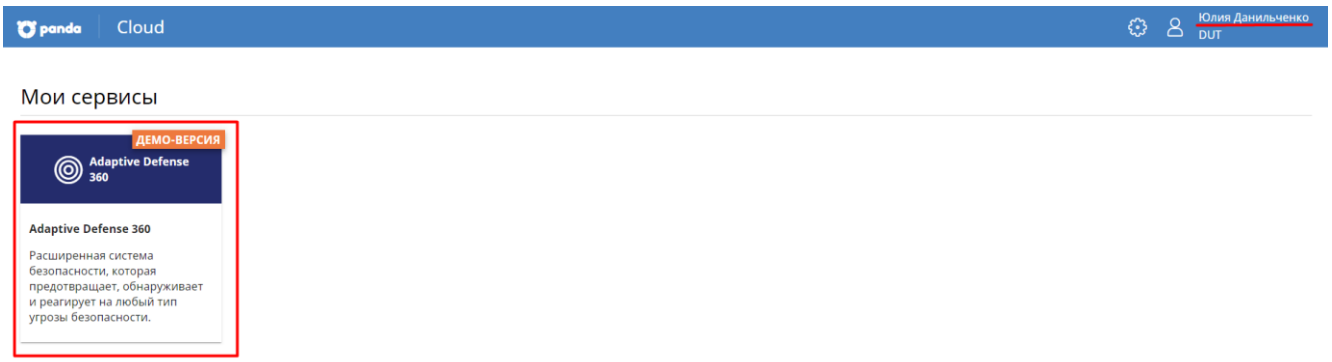


Рис. 3.1. Сторінка вибору облікового запису та продуктів у консолі Aether

Для управляння та перегляду кінцевих точок треба встановити на кожну агент Panda. Для цього у вкладці «Компьютеры» треба натиснути кнопку «Добавить компьютеры» та обрати потрібну операційну систему. В моєму випадку це операційна система Windows (рис.3.2.). Наступим кроком можна обрати певну групу до якої можна додати комп'ютер (рис.3.3.). Інсталятор можна вислати на пошту, а можна завантажити одразу на пристрій. Важливо відзначити, що у цілях безпеки є можливість обмежити термін дії інсталятора.

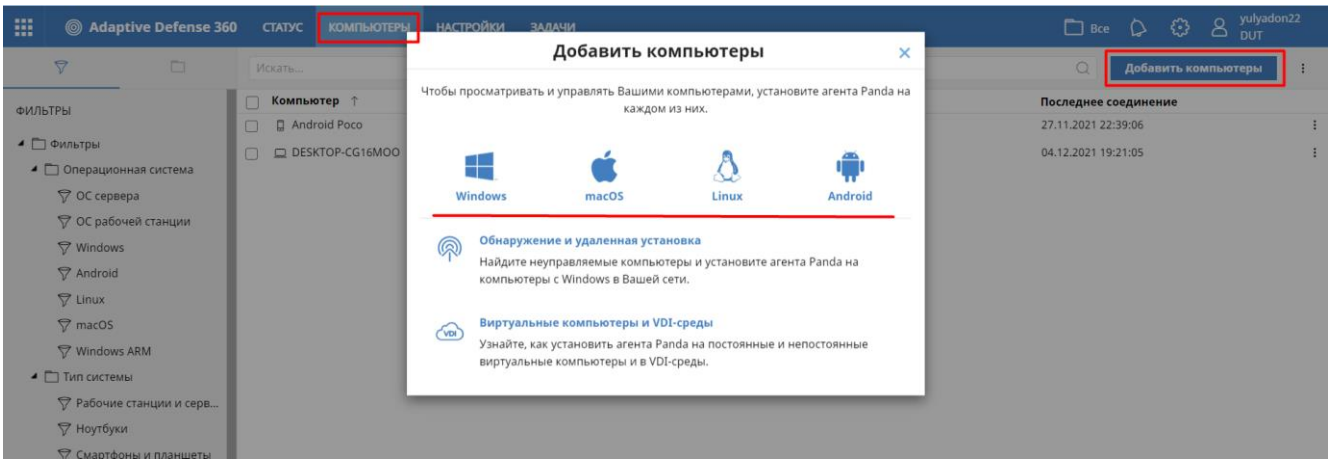


Рис. 3.2. Додавання комп’ютерів у консоль Aether

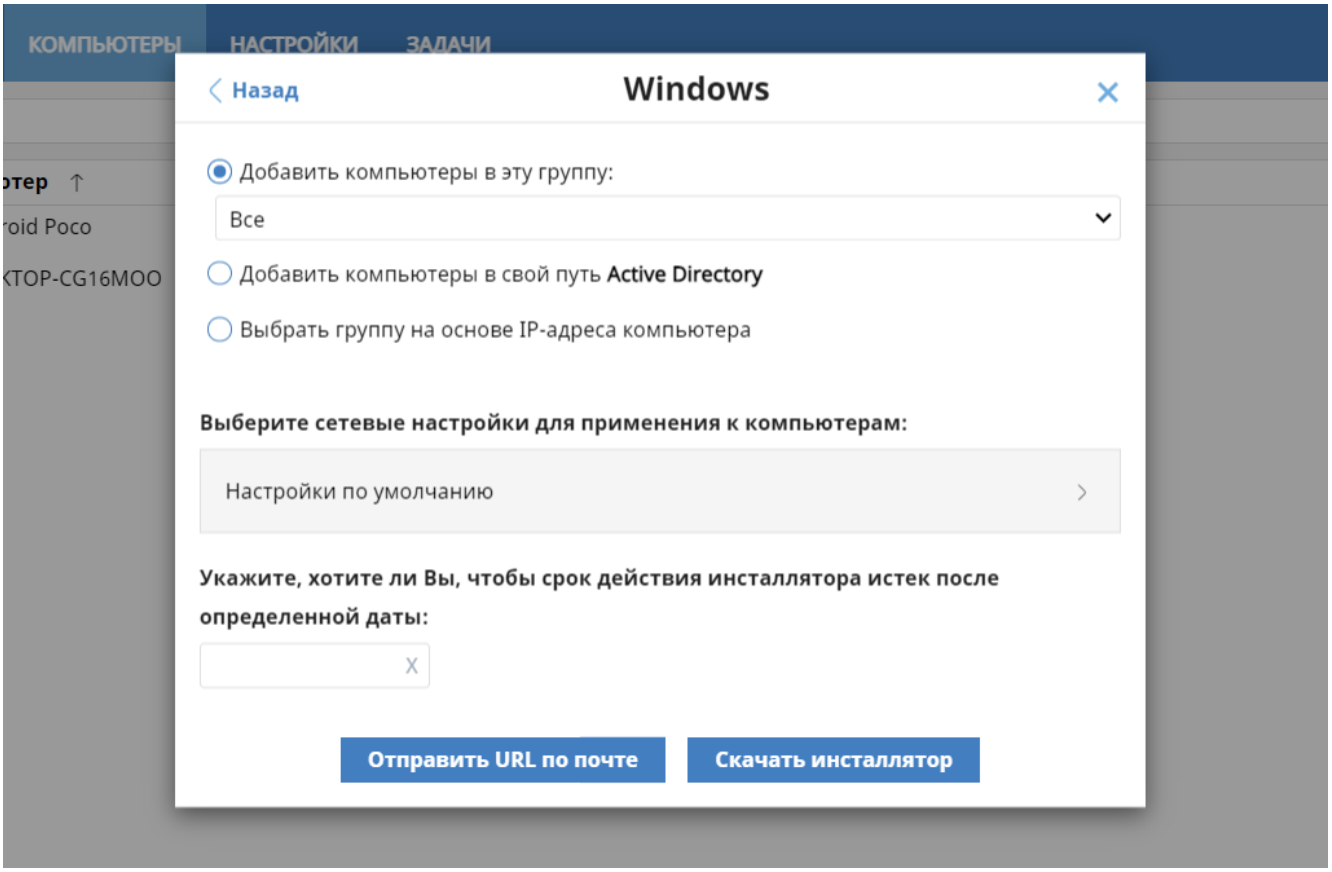


Рис. 3.3. Вибір групи для додавання комп’ютера у консоль Aether

На кінцеву точку встановлюється агент Panda, завдяки якому можна проводити сканування комп’ютера на вразливості (рис.3.4.) та завдяки консолі відстежувати його статус захищеності.

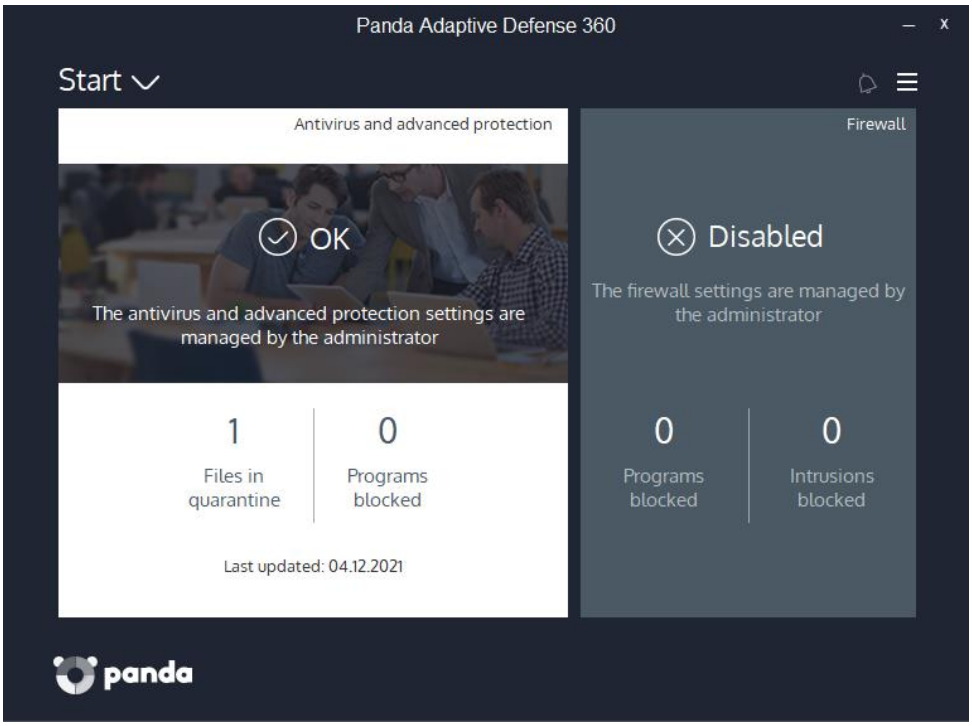


Рис. 3.4. Агент Panda встановлений на комп’ютер

Після встановлення комп’ютер з’являється в переліку пристроїв у консолі, там можна побачити усю інформацію про кінцеву точку: деталі про пристрій, виявлені загрози, компоненти комп’ютера (обладнання) та встановлене ПЗ.

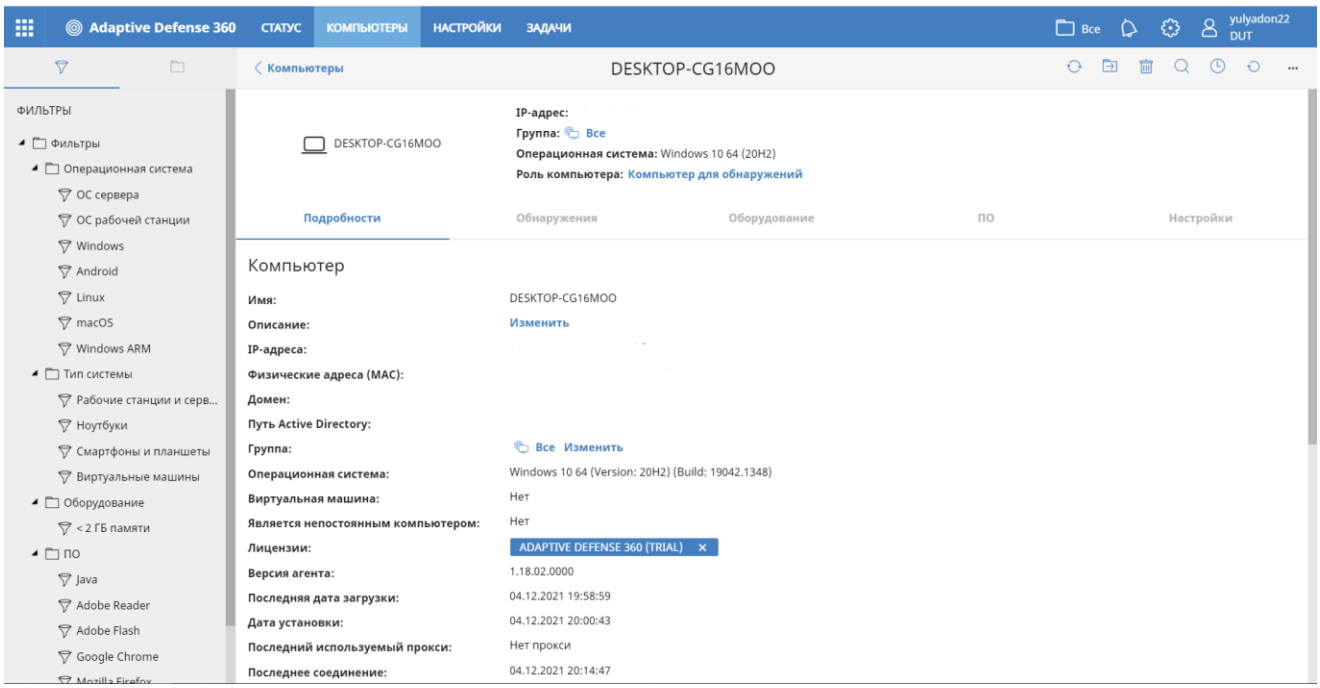


Рис. 3.5. Комп’ютер та детальна інформація про нього у консолі Aether

Важливо відмітити, що продукти, засновані на платформі Aether, в тому числі і Panda Adaptive Defense 360 надають інструменти для пошуку незахищених робочих станцій та серверів у мережі та запуску віддаленої автоматичної установки з консолі керування.

Незахищені кінцеві точки виявляються за допомогою компьютера, що виконує роль комп'ютера виявлення. Усі комп'ютери, що відповідають необхідним вимогам, з'являться у списку «Виявлені некеровані комп'ютери», незалежно від того, чи підтримує їх ОС або тип пристрою встановлення Panda Adaptive Defense 360 (рис.3.6.).

Перший комп'ютер Windows, інтегрований у Panda Adaptive Defense 360, автоматично призначається комп'ютером виявлення (рис.3.7.).

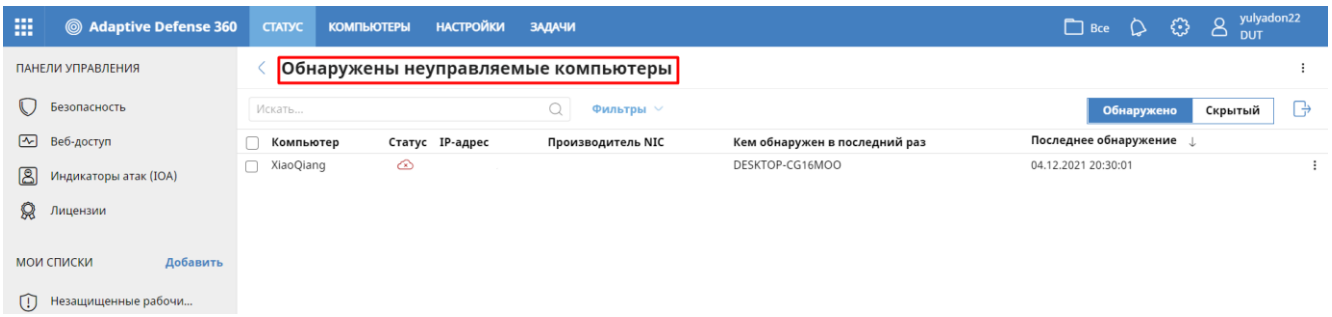


Рис. 3.6. Виявлені некеровані комп’ютери у консолі Aether

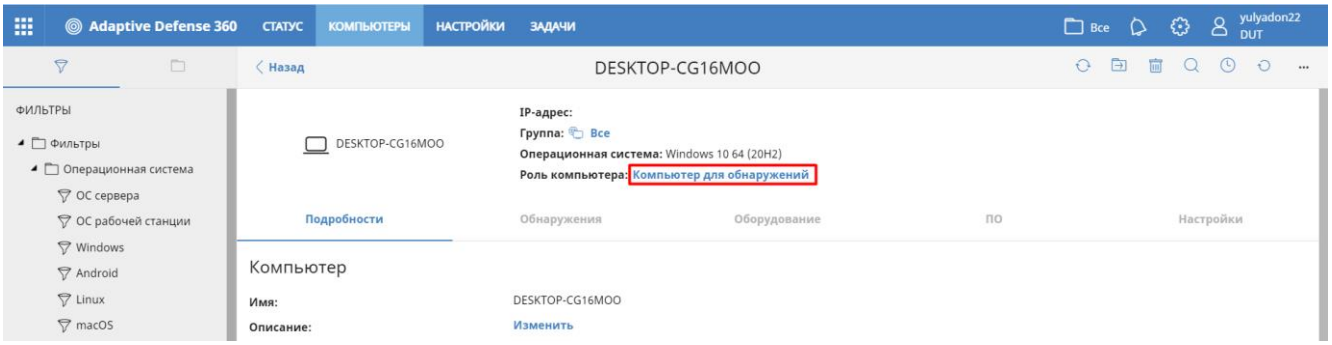


Рис. 3.7. Комп’ютер призначений комп’ютером для виявлень

## 3.2. Технологія захисту кінцевих точок організації на базі рішення Panda Adaptive Defense 360

У попередньому розділі було вказано, що основна робота з рішенням Panda Adaptive Defense 360 відбувається у консолі Aether. Тому варто детально розібрати як працювати з даним продуктом.

***Розділ «Статус»***

На головній сторінці консолі адміністратор безпеки може спостерігати розділ «Статус», в якому можна побіжно оцінити статус безпеки інформаційної системи організації, і контролювати статус ліцензій (рис.3.8.).

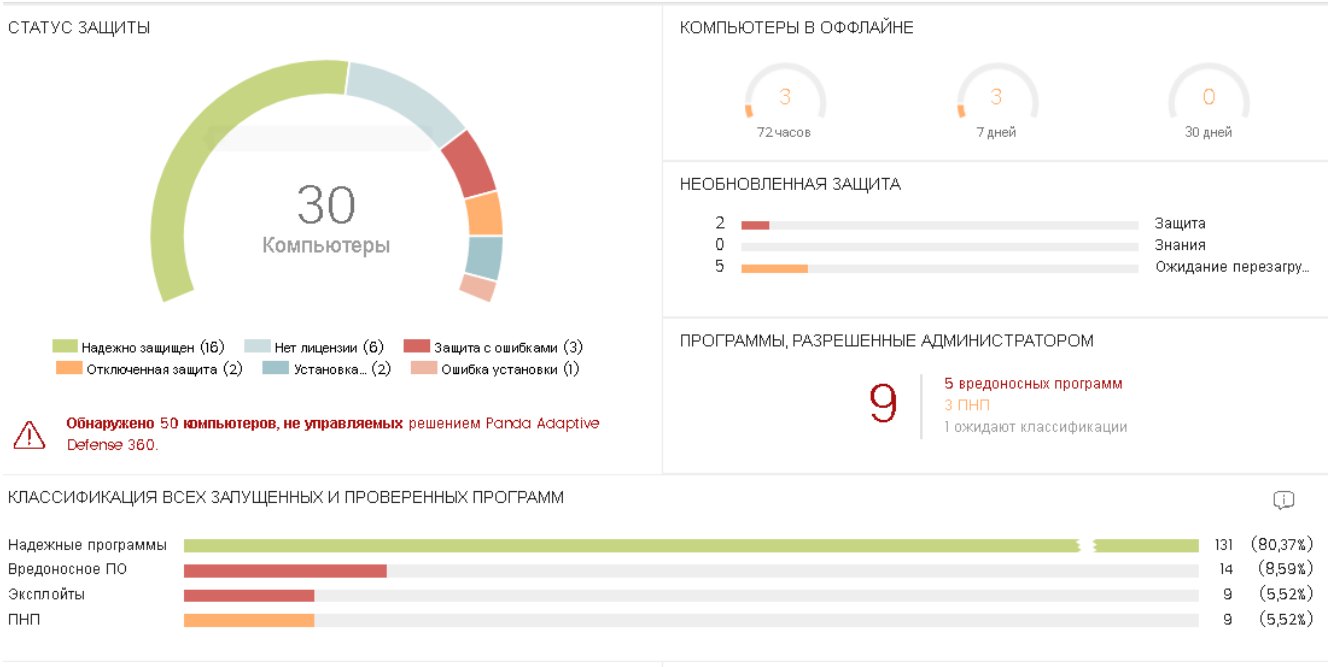


Рис. 3.8. Головна сторінка консолі Aether

У підрозділі Безпека, яка представлена в консолі управління, знаходиться загальна інформація з безпеки та загроз, вона представлена у вигляді віджетів:

- Статус захисту на всіх керованих пристроях. Тут можна побачити кількість кінцевих точок у мережі, їх статус безпеки. Також, при наявності, будуть відображені кінцеві точки, що були виявлені, але не управляються рішенням Panda Adaptive Defense 360.

- Статистика пристроїв, які знаходяться в оффлайні за останні 72 години, 7 днів і 30 днів. У цьому ж розділі можна побачити пристрої, у яких не оновлено захист і ті, які чекають на перезавантаження.
- Програми, дозволені адміністратором, залежно від їхньої класифікації (шкідливе ПЗ, потенційно небажані програми (ПНП) або класифікації, що очікують, у PandaLabs).
- Класифікація всіх запущених або перевірених програм на пристроях з розподілом за видом класифікації (надійна програма, шкідливе програмне забезпечення, експлойти та ПНП).
- Об'єкти, які не були класифіковані, автоматично розміщуються в заблокованих програмах та очікують класифікації. Статистика по них знаходиться у віджеті з аналогічною назвою. За заявою представників класифікація відбувається до 3 днів.
- Віджети Активність шкідливих програм, Активність ПНП та Активність експлойтів інформують адміністратора про активність відповідних видів загроз (рис.3.9.).

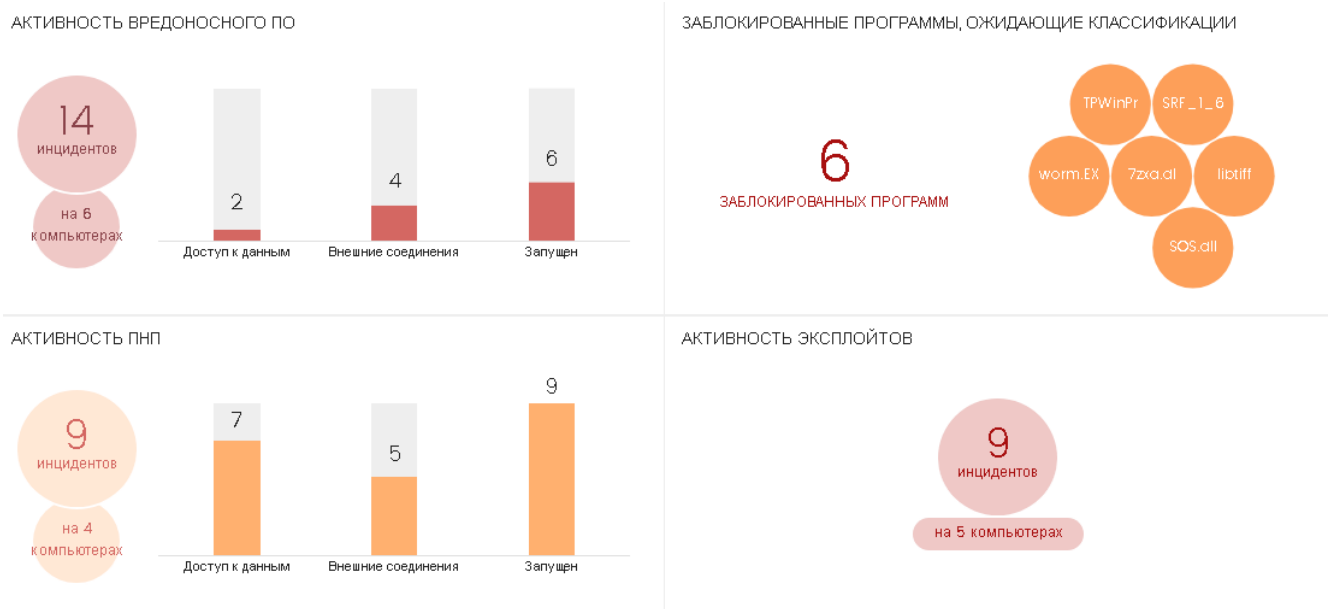


Рис. 3.9. Віджети Активність шкідливих програм, ПНП та експлойтів

Натиснувши у віджетах на сектори діаграм або стовпці гістограм можна перейти до відповідних списків, наприклад списку комп'ютерів, на яких

спостерігалася активність ПНП (рис.3.10.), або списку активностей шкідливого ПЗ (рис.3.11.).

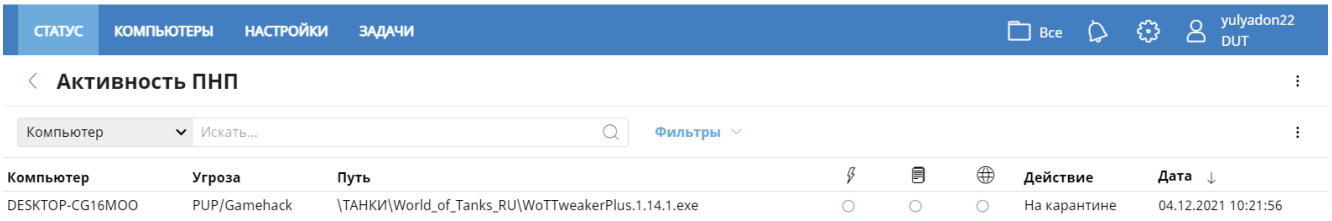


Рис. 3.10. Список комп'ютерів, на яких спостерігалася активність ПНП

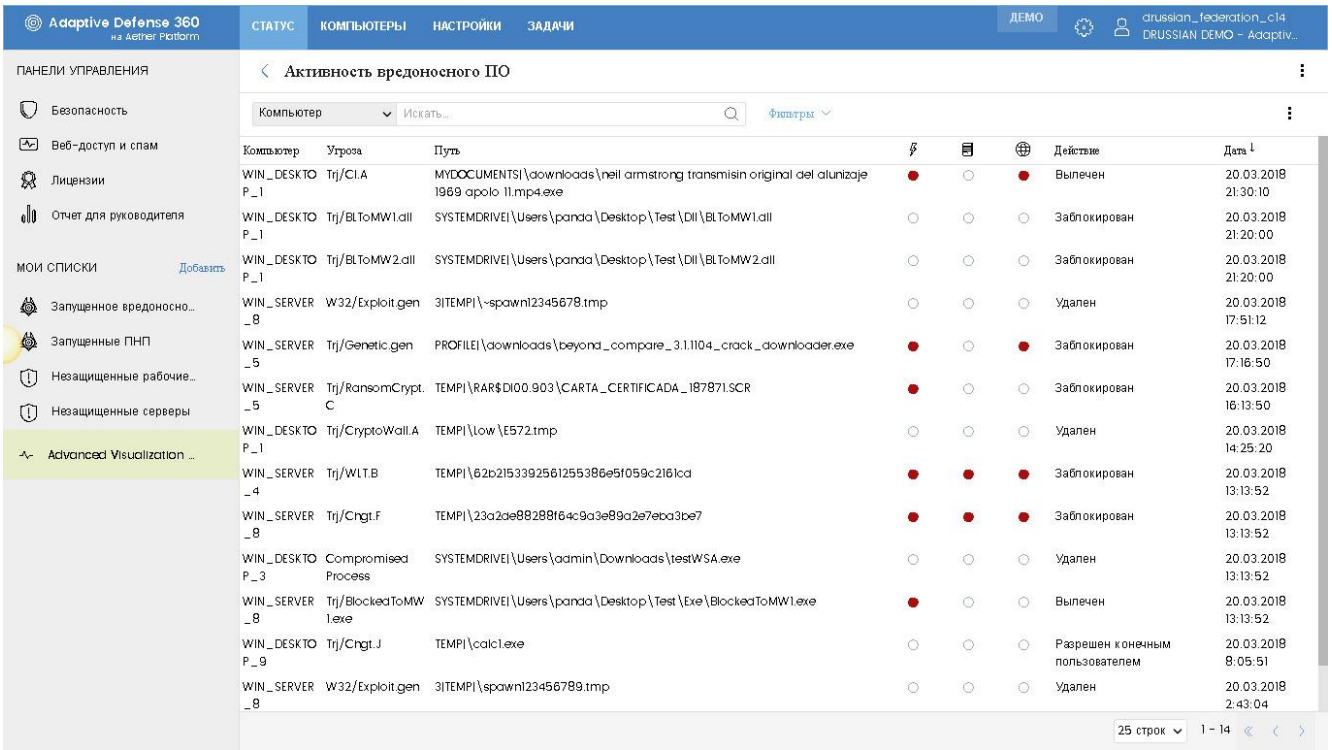


Рис. 3.11. Список комп'ютерів, на яких спостерігалася активність шкідливого ПЗ

У розділі Веб-доступ можна переглянути статистику за категоріями веб-сайтів, до яких зверталися користувачі захищених кінцевих точок. Тут можна детально побачити кількість спроб доступу до різних категорій веб-сайтів, а також більш детально, які саме пристрої звертились на ці сайти (рис.3.12.). Ще в даному підрозділі можна побачити дані про спам, що надходив на сервери Exchange.

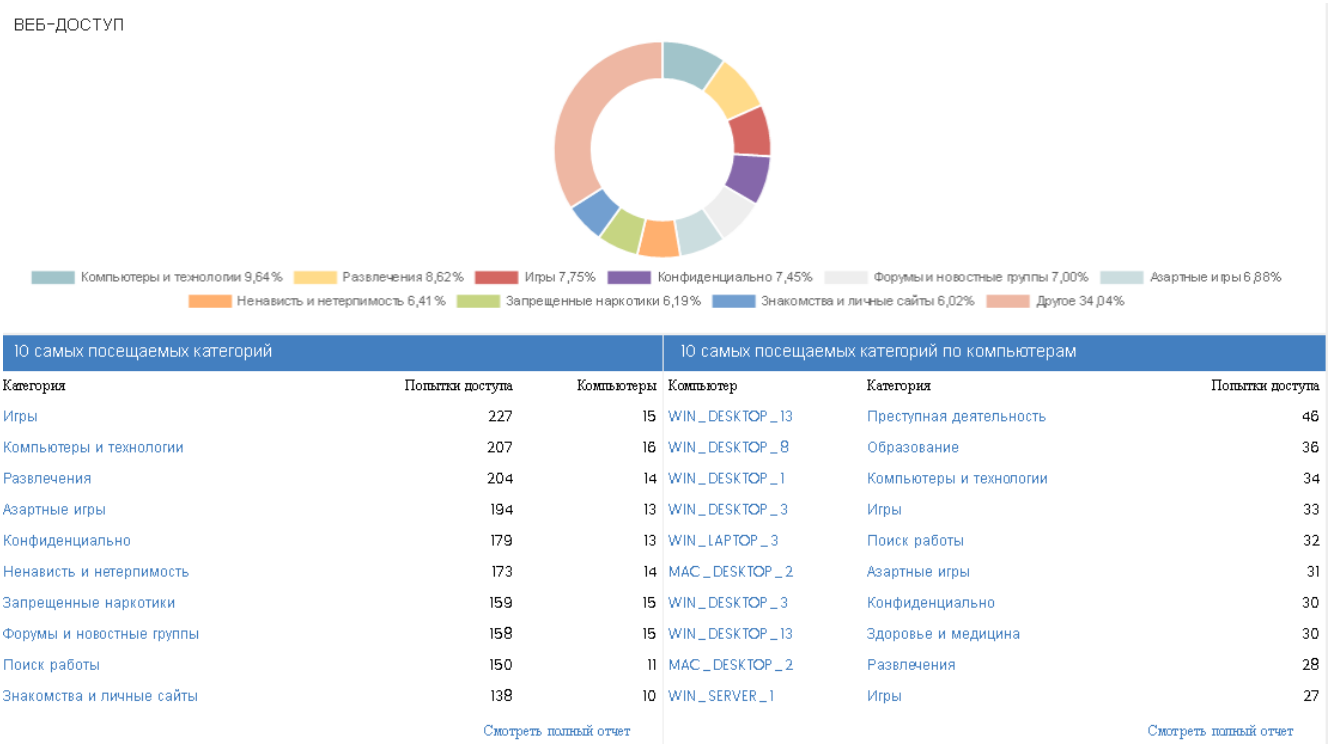


Рис. 3.12. Підрозділ «Веб-доступ» та статистика по зверненням до веб-сайтів

В обох підрозділах: Безпека та Веб-доступ, є можливість вибрати необхідний час за який потрібна статистика: останні 24 години, 7 днів, місяць, рік.

*Підрозділ «Мои списки»*

У розділі «Статус» існує підрозділ «Мои списки», який є дуже зручним інструментом для швидкого відображення даних, які сформовані у списки по ряду певних критеріїв.

Для додавання нового списку треба натиснути кнопку «Добавить» та вибрати потрібний тип списку із запропонованих категорій:

- Основне (ліцензії, виявлені некеровані комп’ютери, комп’ютери з однаковими іменами, ПЗ, обладнання);
- Безпека (статус захищеності комп’ютерів, активність шкідливого ПЗ та ПНП, активність експлойтів, заблоковані програмі, що очікують класифікації, загрози виявлені антивірусом, заблоковані спроби вторгнення, заблоковані пристрої, індикатори атак);
- Контроль активності (веб-доступ по категорії, веб-доступ по комп’ютеру, програми заблоковані адміністратором).

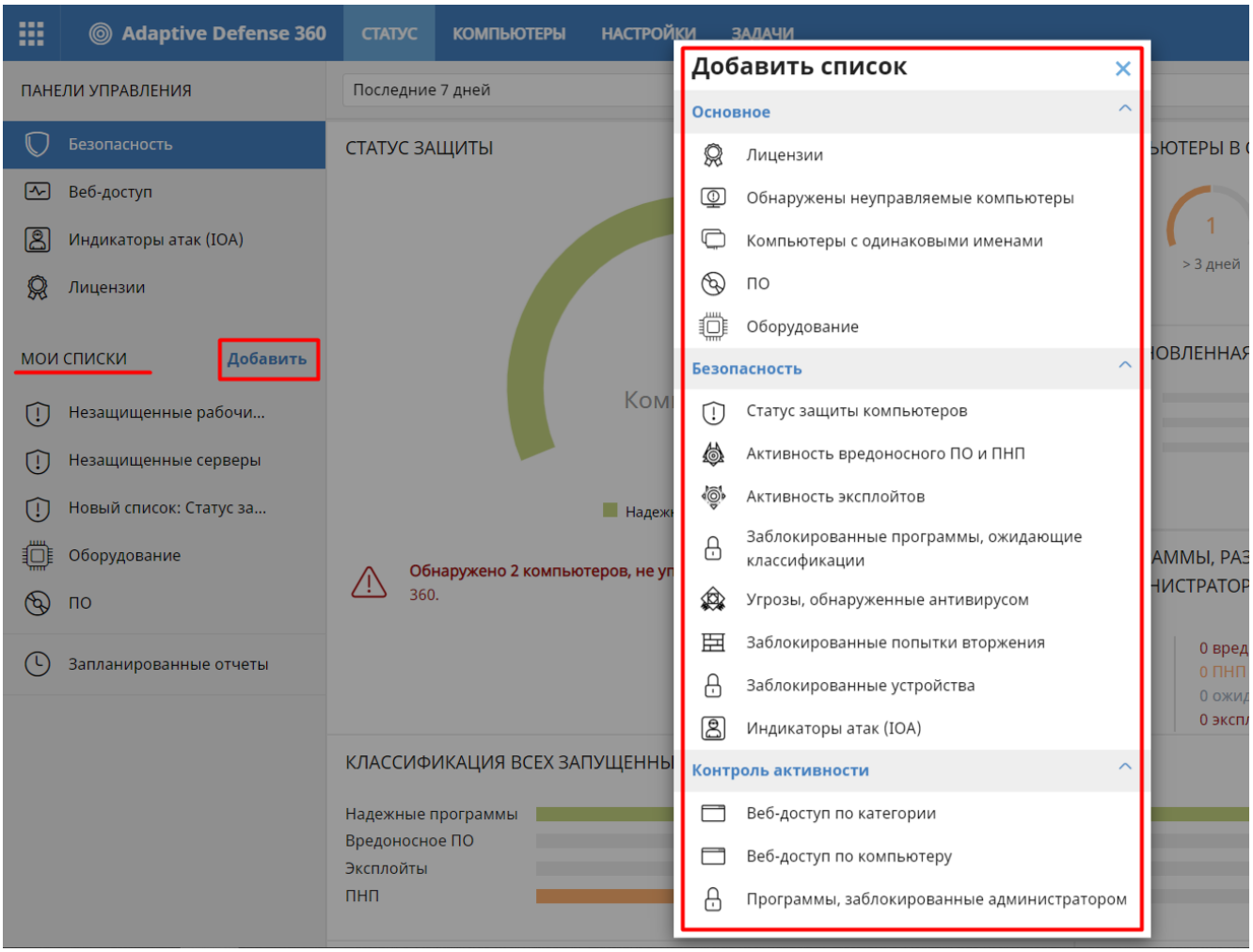


Рис. 3.13. Додавання нового списку

Як приклад, розгляну, як відображається список «Запущене шкідливе ПЗ». У цьому списку перераховуються всі кінцеві точки, на яких було здійснено спробу запуску шкідливого ПЗ.

Інформація у списку подається у вигляді таблиці елементів. У конкретному списку представлена інформація про кожен комп'ютер, на якому було виявлено шкідливе ПЗ, назва самого ПЗ, шлях до його розташування на комп'ютері, інформація про спроби запуску, звернення до даних на пристрої, виконання зовнішніх з'єднань, дії по відношенню до шкідливого ПЗ (виявлено , на карантині, заблоковано, вилікувано, видалено), також можна побачити дату та час виявлення.

Таблицю з елементами можна відсортувати за будь-яким параметром (стовпцем).

Натиснувши на елемент списку, відбувається перехід на сторінку з детальною інформацією по даному елементу.

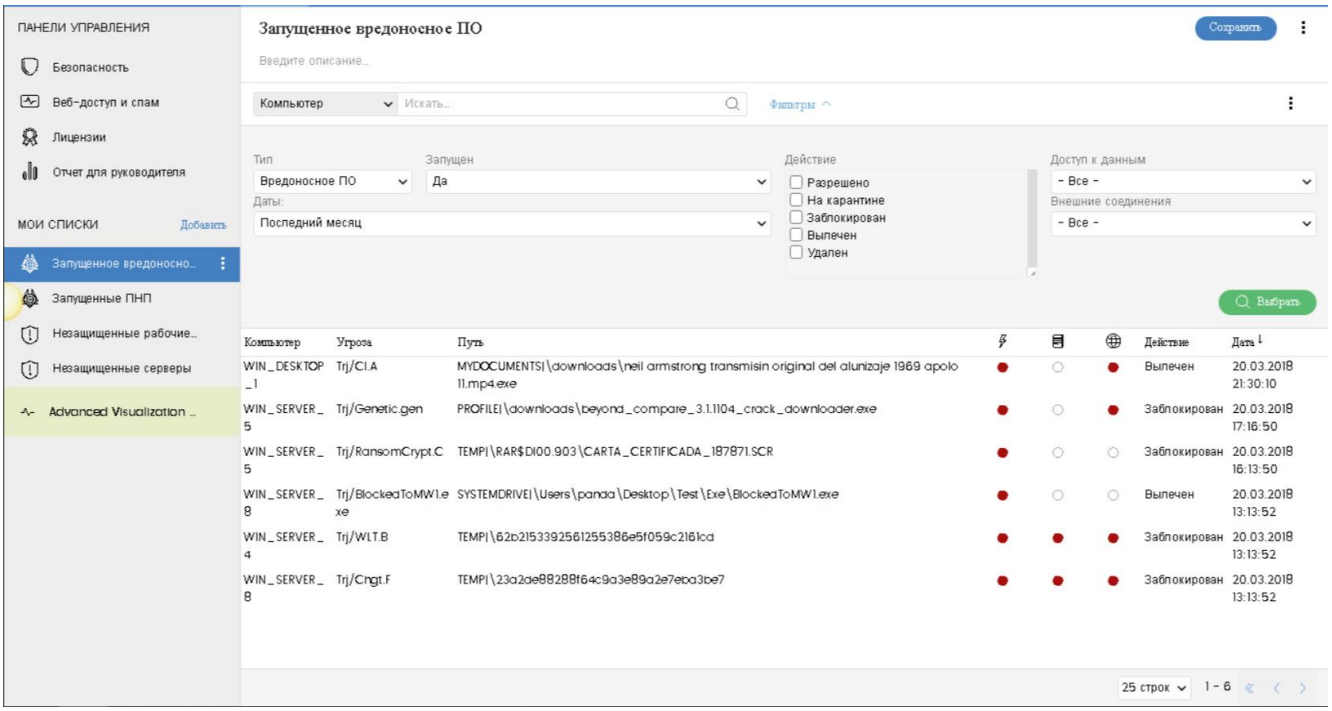


Рис. 3.14. Інформація у списку у вигляді таблиці елементів

*Інформація про пристрій та загрозу*

Як було з'ясовано трохи раніше, натискаючи на елемент у списку, можна перейти на сторінку з експертною інформацією, яка описує кожне виявлення та всі події, які з ним пов'язані.

У верхній частині сторінки знаходиться загальна інформація про загрозу: назва загрози та дія, яка була вчинена по відношенню до неї. Тут можна виключити блокування або навпаки заблокувати процес.

Нижче можна побачити дві вкладки "Подробиці" та "Активність". Безпосередньо у вкладці "Подробиці" міститься така інформація:

- Дані про заражений пристрій - його назва, користувач, який підключений до нього і шлях виявлення (де файл знаходиться на пристрої);
- Інформація про рівень впливу загрози на комп'ютер. Тут знаходиться назва загрози і можна знайти інформацію про неї в Google і VirusTotal, інформація про активність загрози, якщо вона відбувалася. Можна побачити повний графік та

опис активності, натиснувши відповідні кнопки. Також тут можна побачити дату і час виявлення загрози;

- Далі можна подивитися на джерело зараження – назву комп'ютера, де вперше була виявлена дана загроза, IP-адреса пристрою та дані про його користувача, який працював з пристроєм;
- У розділі "Поява на інших комп'ютерах" знаходяться дані щодо виявлення загрози на інших пристроях, шлях до неї та перше виявлення.

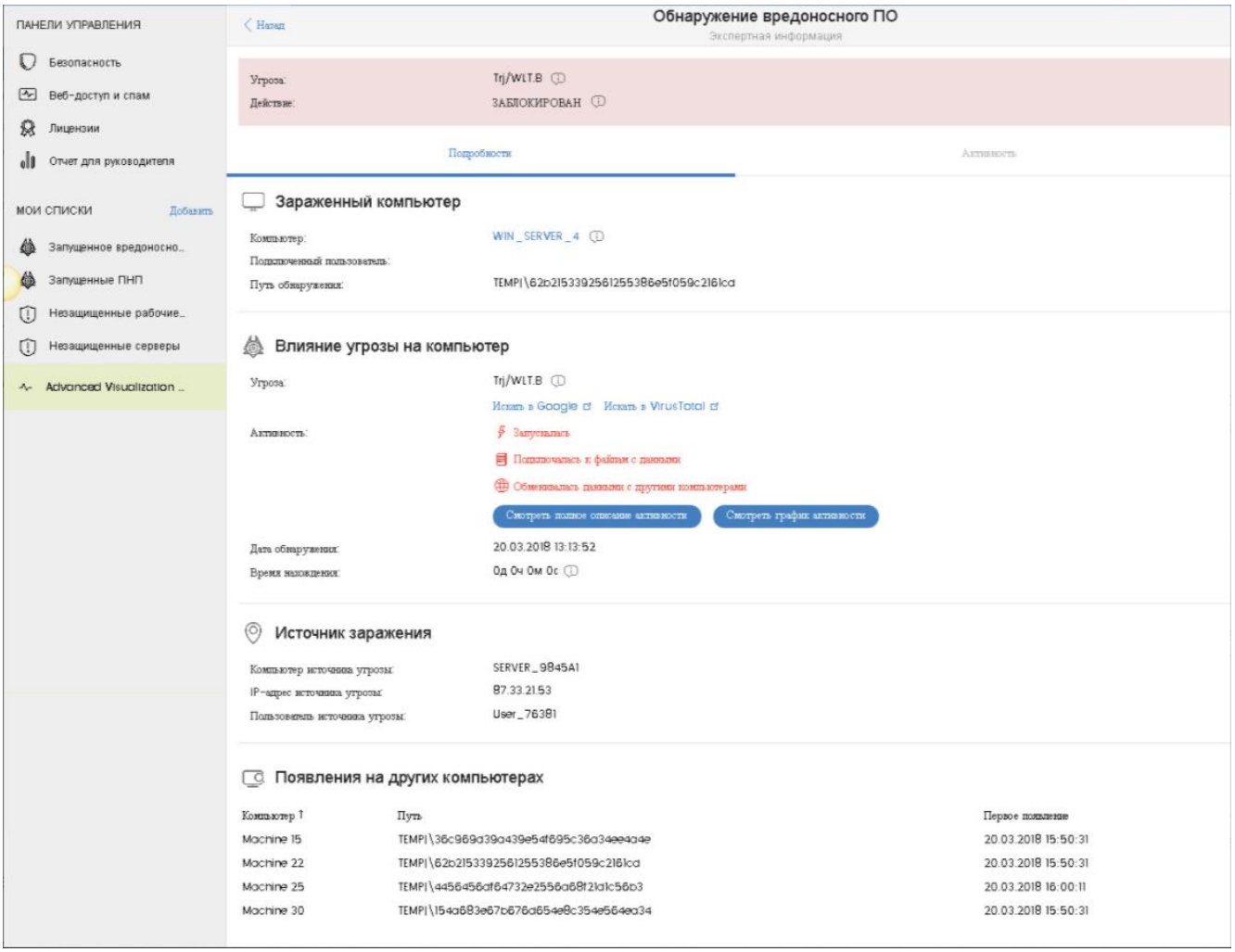


Рис. 3.15. Інформація про заражений пристрій та загрозу

Вкладка "Активність" надає детальну інформацію про життєвий цикл загрози на комп'ютері, тут міститься інформація про всі події, пов'язані з виявленою загрозою. Рішення Panda Adaptive Defense 360 досліджує причинно-наслідкові зв'язки між IT-процесами, що дозволяє йому скласти життєвий цикл загрози, як вона з'явилася і які спричинила процеси: запуски, скачування, передача інформації,

її копіювання, видалення запис в реєстр, дані про командний рядок, хеші файлів, шляхи передачі і т. д.

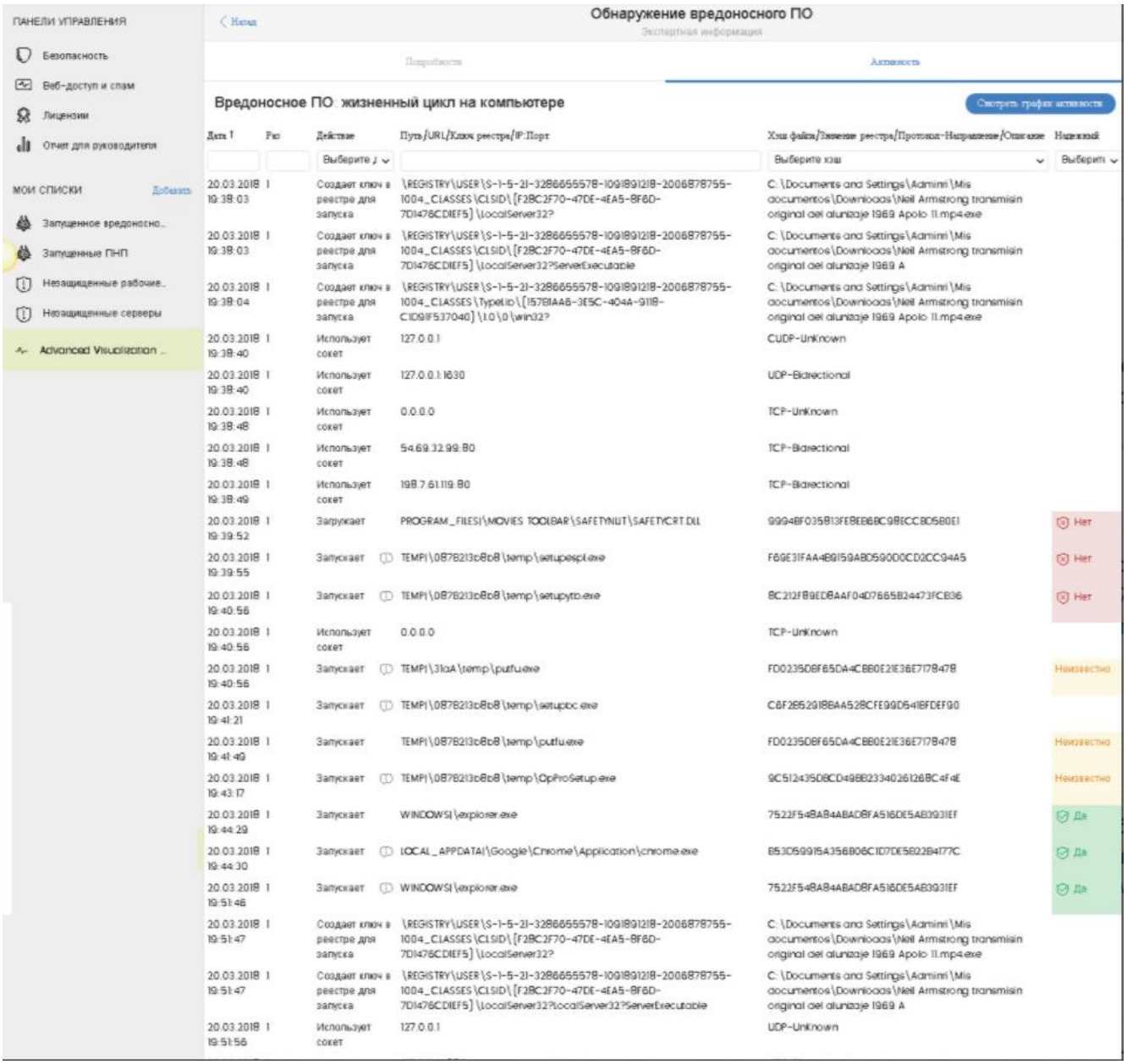


Рис. 3.16. Інформація про життєвий цикл загрози на пристрої

Натиснувши кнопку "Дивитись графік активності", відкривається представлення активності загрози у вигляді графіка, на якому можна подивитися динаміку в часі.

Щоб побачити весь життєвий цикл загрози, необхідно вибрати перший вузол і запустити. Графік показує дії злочинця, за весь час, коли він намагався впровадити загрозу в систему.

Далі можна деталізувати і відфільтрувати відображену інформацію, щоб провести розслідування, для оцінки збитків, які були заподіяні загрозою, і виявити викрадення конфіденційних даних.

Ця інформація дозволить встановити превентивні заходи для запобігання майбутнім атакам, такі як, зміна дозволів користувачів, створення правил роботи брандмауера для захисту периметра мережі і т. д.

На цьому графіку використовуються різні кольори для позначення рівня ризику кожного елемента. Зелений означає справний стан, червоний – шкідливе ПЗ, помаранчевий – елементи, що знаходяться в процесі класифікації, а синій – дії, що здійснюються відслідковуваними процесами.

Аналіз даної інформації дозволяє виявляти слабкі місця у системі безпеки підприємства, підозрілу та небезпечну активність співробітників, можливі інциденти витоку даних.

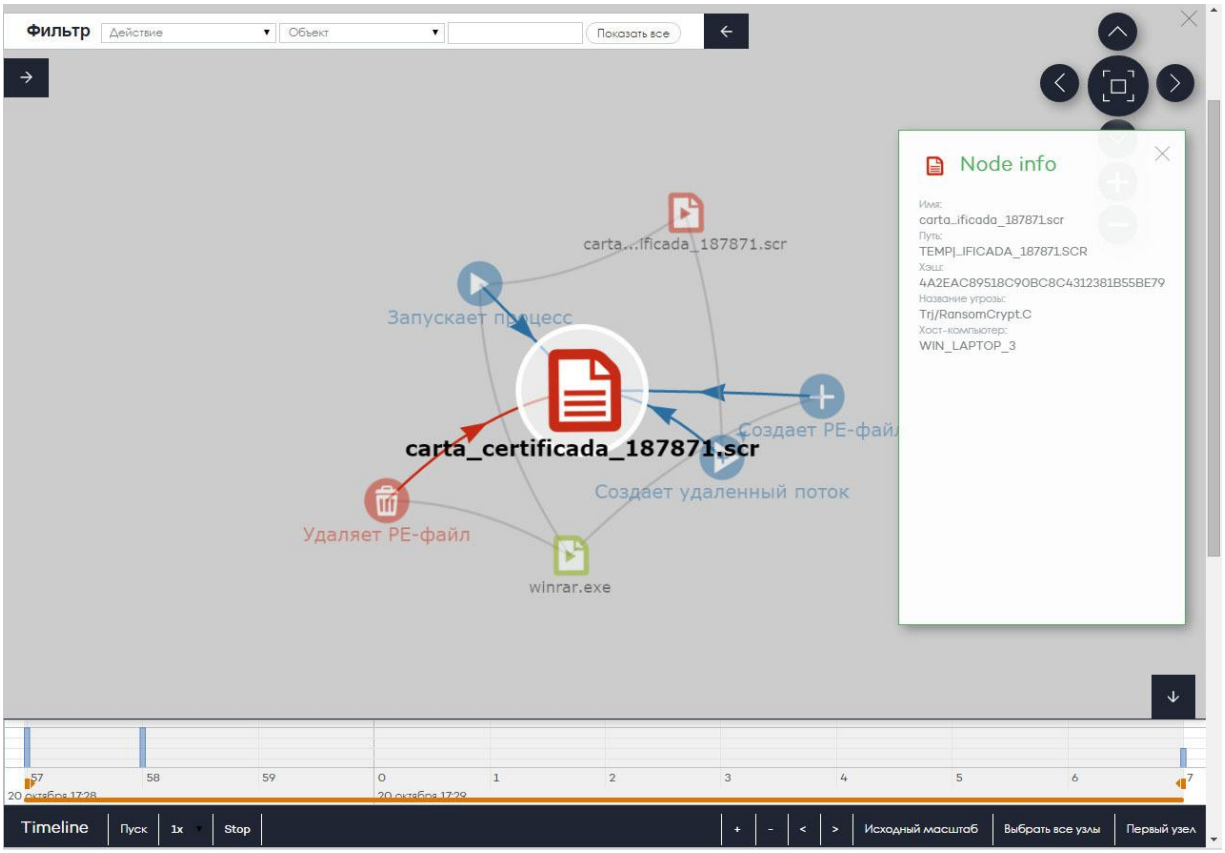


Рис. 3.17. Графік активності загрози

*Розділ «Комп’ютери»*

Далі слід розглянути розділ «Комп’ютери», його призначення та функціонал. Ця вкладка містить інструменти для керування комп'ютерами. Також тут є можливість віддаленого виконання деяких завдань на кінцевих точках.

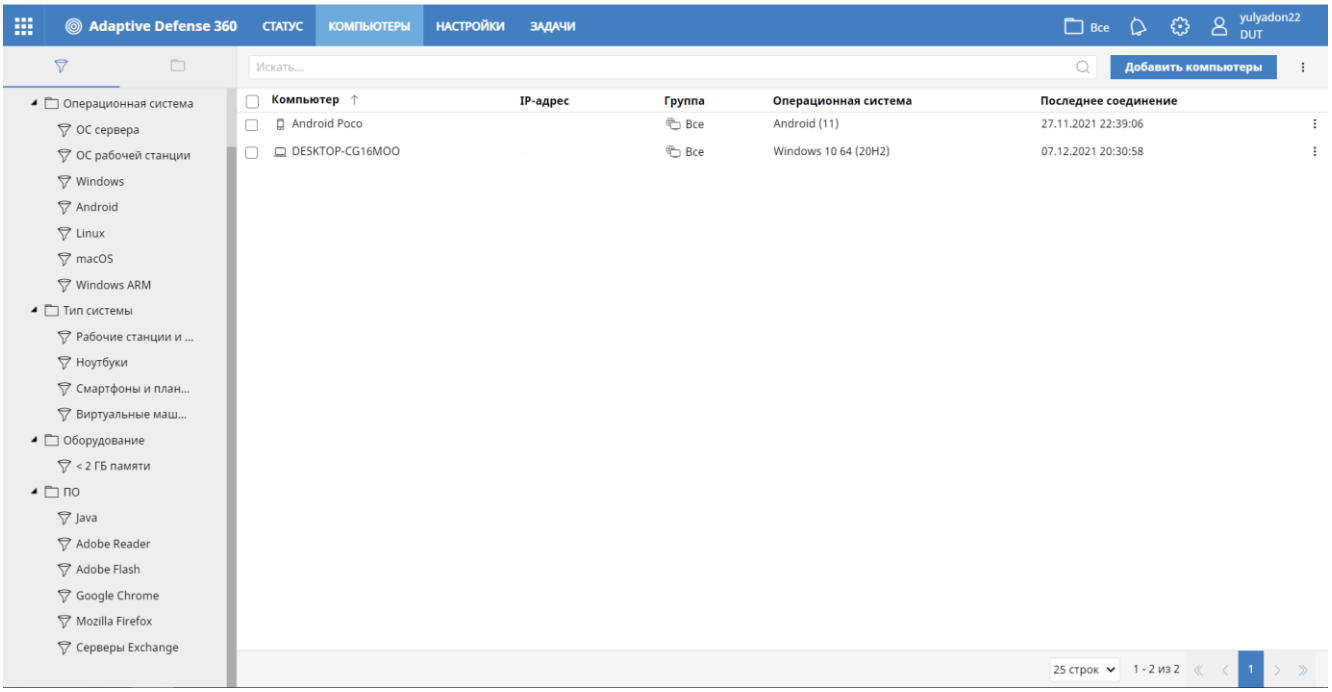


Рис. 3.18. Розділ керування комп’ютерами

*Використання фільтрів*

Зліва консолі знаходиться блок для сортування необхідних пристроїв, використовуючи фільтри або по дереву організації. Стандартні фільтри дозволяють вибрати пристрої за такими типами: тип ОС, тип пристрою, особливості пристрою, наявності встановленого ПЗ. Є можливість створити свій фільтр за допомогою кнопки "Додати фільтр".

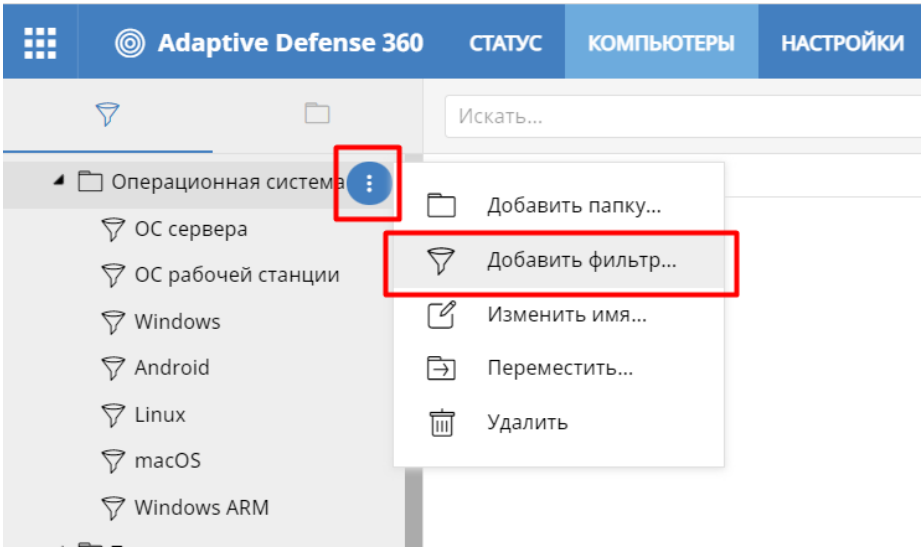


Рис. 3.19. Додавання нового фільтра пристроїв

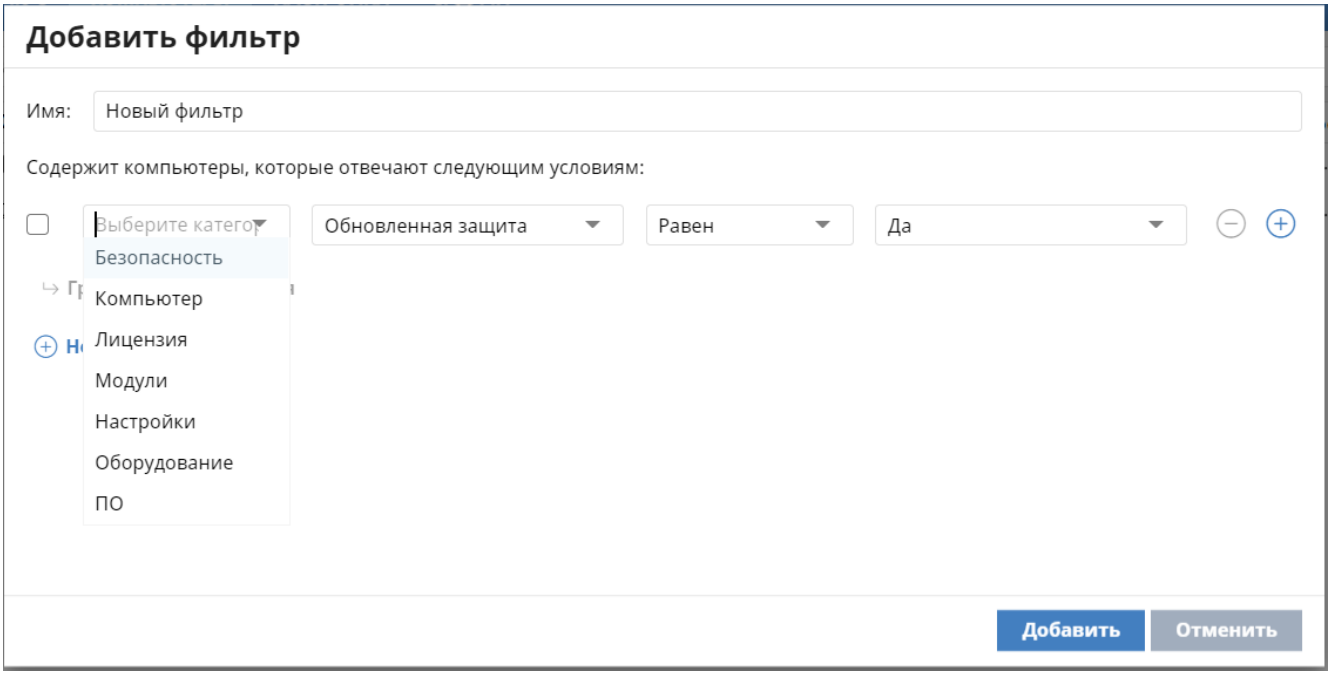


Рис. 3.20. Додавання нового фільтра пристроїв

Налаштування фільтра пропонує на вибір категорію (безпека, комп'ютер, ліцензія, модулі, налаштування, обладнання, ПЗ), далі для категорії вибирається певна властивість, яких багато і вони змінюються в залежності від обраної категорії, далі можна вибрати операцію (рівний, не дорівнює, містить, починається і т. д.) та значення умови. Умов може бути створено кілька, їх можна групувати та вибирати застосувати чи ні. Створення фільтрів відбувається з високою

деталізацією і допомагає контролювати всі необхідні пристрої та процеси на них просто впорядкувавши створений фільтр.

*Використання древа організації*

Поряд із розділом «Фільтри» є розділ «Моя організація», де необхідні папки створюються самостійно або інтергруються з Active Directory.

По відношенню до папок можна здійснювати ряд дій:

- Додавати до них нові папки;
- Перейменовувати, видаляти, переміщувати до іншої папки;
- Змінювати налаштування цієї папки.

Безпосередньо до всіх пристроїв, які знаходяться в папці, можна застосовувати такі дії, наприклад:

- Запуск перевірки на даний момент;
- Запланувати майбутні перевірки (завдання) на певний час;
- Ізолювати комп'ютери з мережі та зупинити їх ізоляцію.

Наявність даних можливостей є дуже чудовою допомогою в критичних ситуаціях, коли необхідно терміново запустити перевірку всіх пристроїв, дані можливості будуть корисні і за наявності і 10 пристроїв у мережі, і 10 тисяч.

В основній частині розділу «Комп'ютери» перелічені всі пристрої, які знаходяться у вибраній папці. Представлені вони у вигляді таблиці, у цій таблиці знаходяться деякі дані про пристрої:

- Назва пристрою;
- IP-адреса;
- Група, до якої він належить;
- Встановлена ОС (її назва та версія);
- Дата та час останнього зафіксованого з'єднання з хмарою.

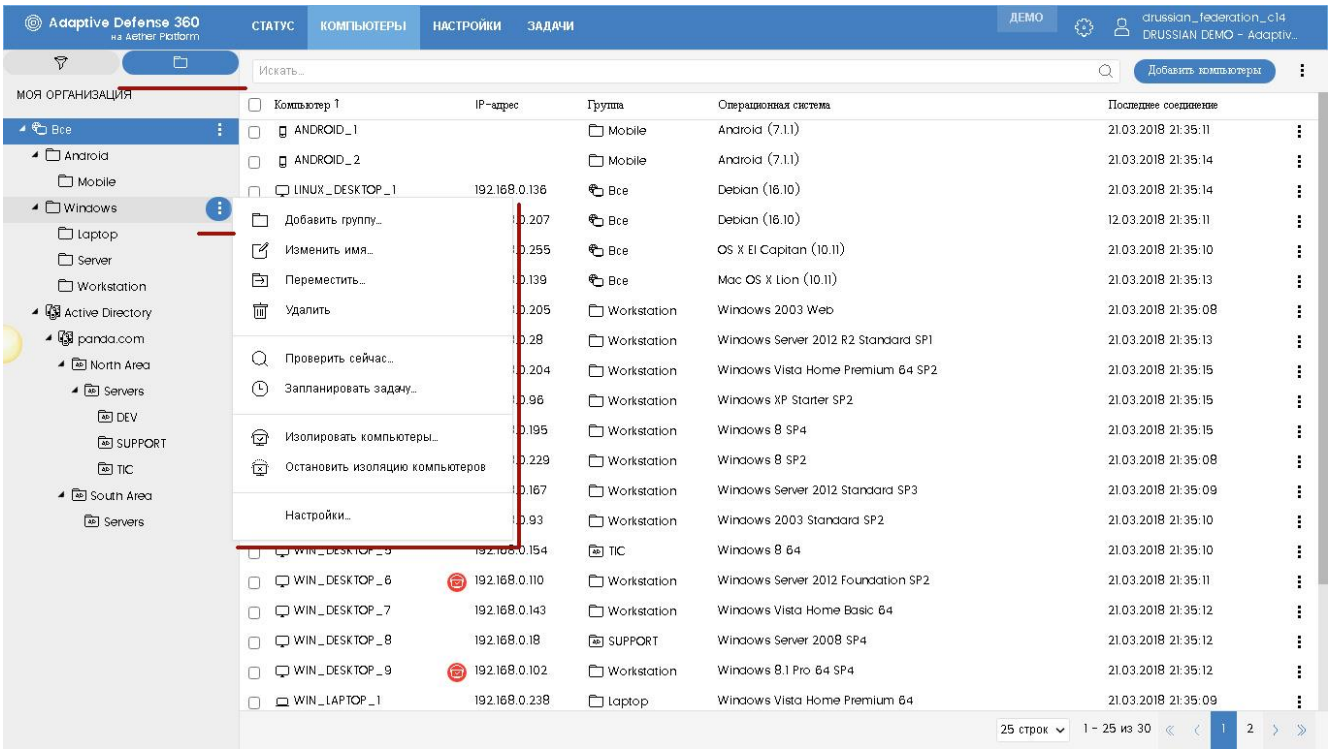


Рис. 3.21. Древо організації

Натиснувши кнопку з трьома точками кожного пристрою у списку, можна викликати контекстне меню. Там знаходиться список дій, які можна виконати з пристроєм прямо з даної таблиці:

- переміщення до іншої папки;
- видалення;
- моментальний запуск перевірки та планування завдання;
- перезавантаження та ізолювання пристрою з мережі;
- переустановлення захисту або агента;
- повідомлення про проблему у службу підтримки.

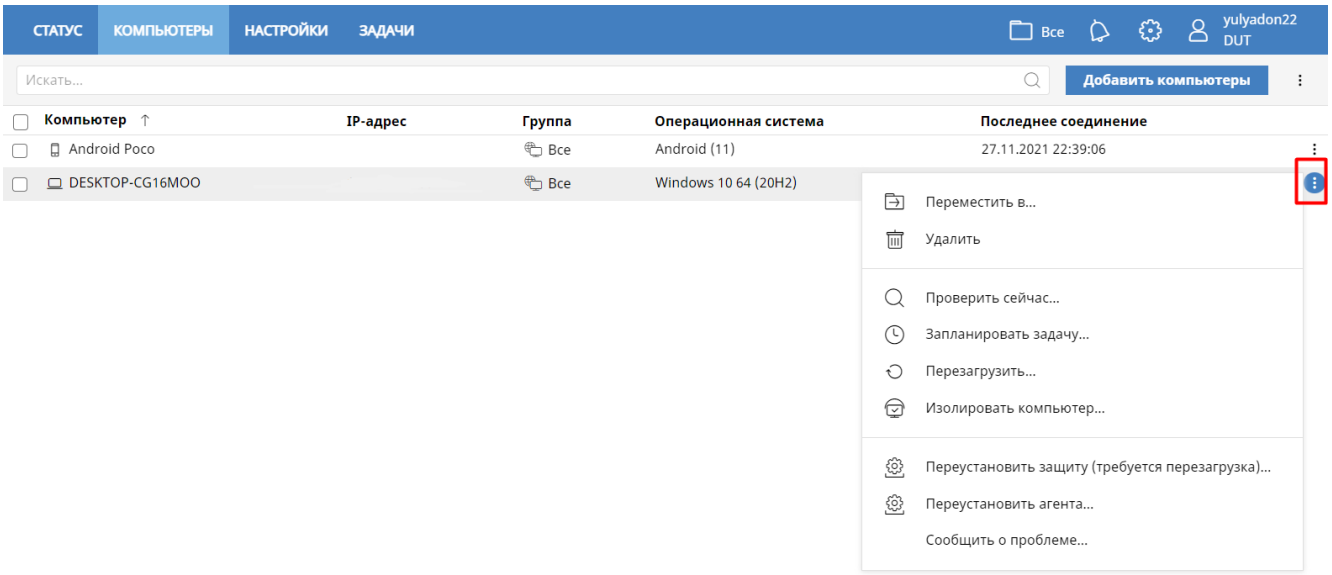


Рис. 3.22. Контекстне меню дій над пристроями

*Подробиці про кінцеву точку*

Натиснувши на певний пристрій, відбувається перехід на сторінку з детальною інформацією про нього.

Вгорі можна побачити загальну інформацію про пристрій:

- назву пристрою;
- IP-адреса пристрою;
- група, до якої входить пристрій;
- встановлена ОС та її версія.

За допомогою кнопок у верхньому правому куті, можна прямо в цьому розділі виконати такі дії: оновити інформацію про комп'ютер, перемістити в іншу папку, видалити, перевірити або запланувати завдання, перезавантажити та ізолювати пристрій.

Важливо відзначити, що під час ізоляції, яка згадувалась і раніше, ізольований пристрій обмінюється інформацією лише з хмарою Panda. У такому пристрою буде показано додаткову червону позначку і буде запропоновано зняти ізоляцію з пристрою.

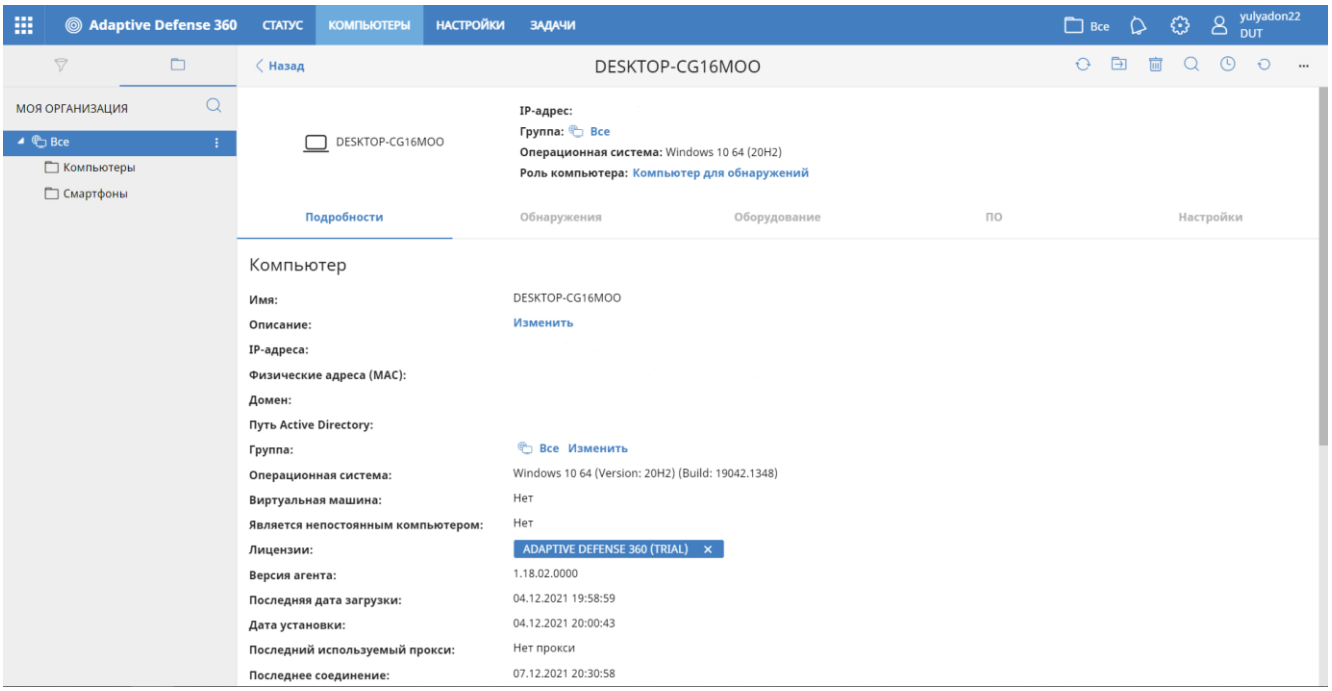


Рис. 3.23. Сторінка детальної інформації про пристрій

Нижче на сторінці про пристрій знаходяться 5 вкладок: Подробиці, Виявлення, Устаткування, ПЗ, Налаштування.

У вкладці «Подробиці» знаходиться вся основна інформація про пристрій та його статус безпеки.

Тут же є можливість "Звільнити ліцензію". У такому випадку пристрій набуває статусу незахищеного, а звільнену ліцензію можна призначити іншому комп'ютеру.

Владка «Виявлення» містить віджети як і стартовий екран консолі (Статус): Активність шкідливого ПЗ та ПНП, перелік заблокованих програм, які очікують на класифікацію, програми заблоковані адміністратором безпеки, активність експлойтів. Тільки в цьому випадку ці віджети демонструють інформацію не про всю мережу, а про конкретний пристрій. На них також можна натиснути та побачити більше інформації по кожному віджету, тільки інформація буде відфільтрована за вибраним пристроєм.

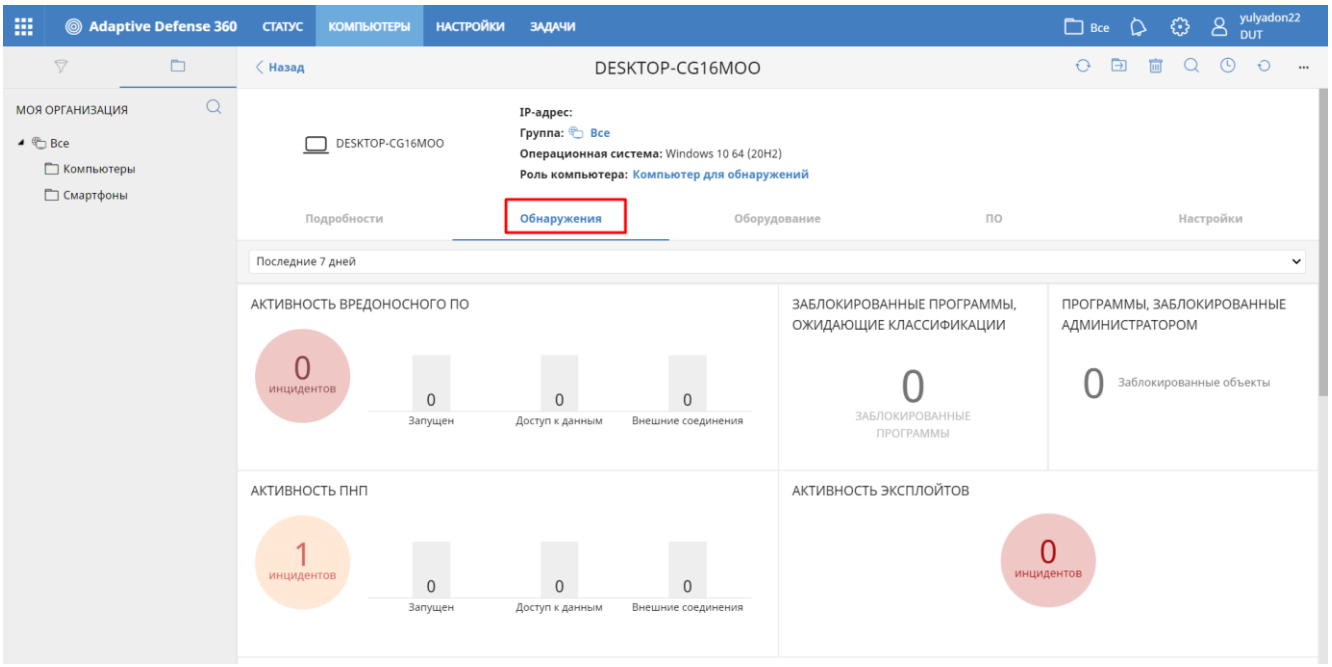


Рис. 3.24. Вкладка «Виявлення» на сторінці детальної інформації про комп’ютер

У вкладці Устаткування міститься докладна інформація про апаратне забезпечення пристрою: процесор, пам'ять пристрою, диски на ньому, серійний номер BIOS, Trusted Platform Module. Кожен пункт являє собою список, що розкривається в якому можна дізнатися докладну інформацію про кожен компонент.

Вкладка «ПЗ» показує інформацію про встановлені програми на пристрій. Відразу ж у таблиці знаходиться інформація про дату установки ПЗ, його назву, виробника, версію та розмір.

Кнопка «Налаштування та видалення» покаже журнал з установками, оновленнями та видаленнями програм з моменту встановлення агента Panda Adaptive Defense 360 на пристрій.

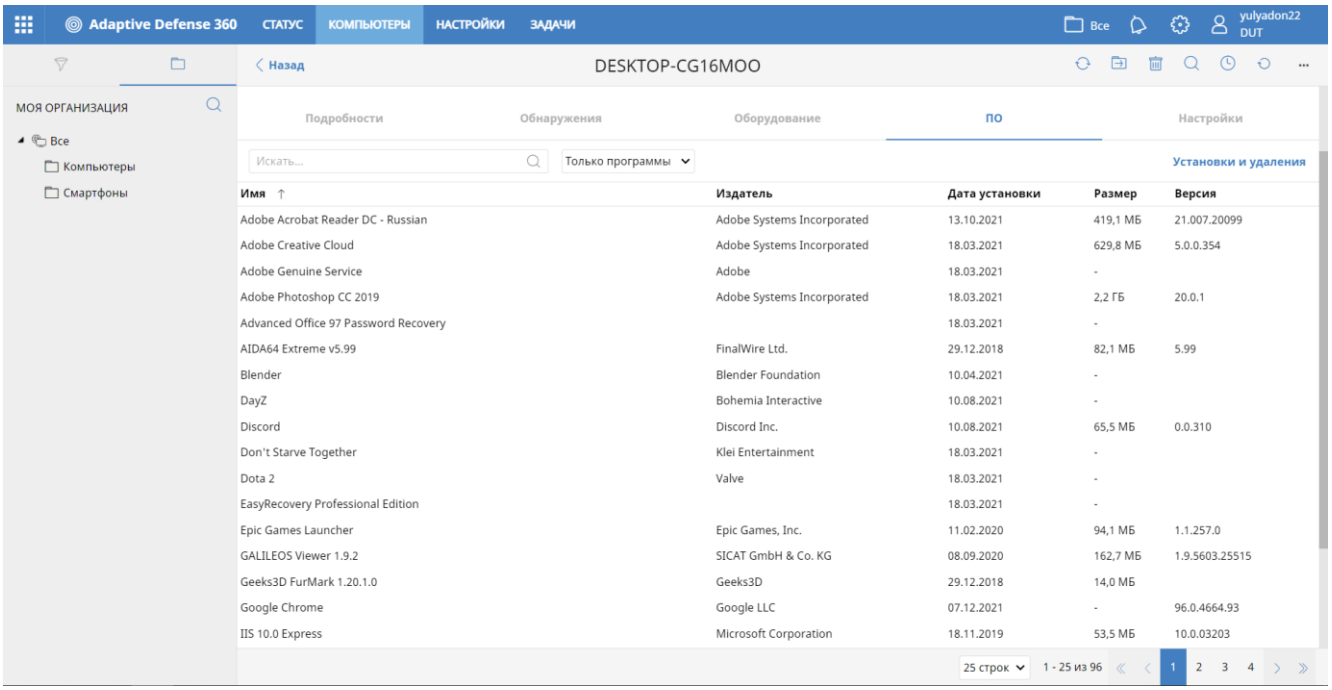


Рис. 3.25. Перелік встановленого ПЗ на обраному пристрої

В цілому, хочу відзначити, що управління пристроями просте, але в той же час дуже докладне та розгорнуте, що дають детальні фільтри та можливість постановки завдань. Є дуже важлива можливість вибору відразу великої кількості пристроїв, пов'язаних загальною характеристикою і здійснювати дії одночасно над усіма пристроями, особливо це важливо в екстрених ситуаціях.

***Розділ «Налаштування»***

У розділі "Налаштування" можна налаштувати користувачів, комп'ютери, мережі та безпеку. Усі налаштування не залежать один від одного, і їх можна налаштовувати окремо. Налаштування гнучкі та прозорі, що дозволяє налаштувати відразу велику кількість пристроїв у великій компанії.

*Налаштування користувачів*

Підрозділ «Користувачі» призначений для налаштування користувачів консолі. Підрозділ поділений на чотири вкладки: Користувачі, Ролі, Безпека, Активність.

У вкладці «Користувачі» знаходиться список користувачів, які мають право на доступ до консолі керування. Тут же у користувачів зазначена їхня роль, наприклад, повний контроль.

У цій же вкладці є дві опції:

- Дозволити співробітникам Panda Security S.L.U. підключатися до моєї консолі. Ця опція включається для дозволу техпідтримці Panda Security підключатися до консолі з правами повного доступу, лише якщо потрібно розібратися в проблемі і вирішити інцидент.
- Дозволити моєму постачальнику підключатися до моєї консолі. Ця опція використовується, якщо постійний постачальник надає сервіси безпеки, які потребують доступу до консолі (управління безпекою тощо).

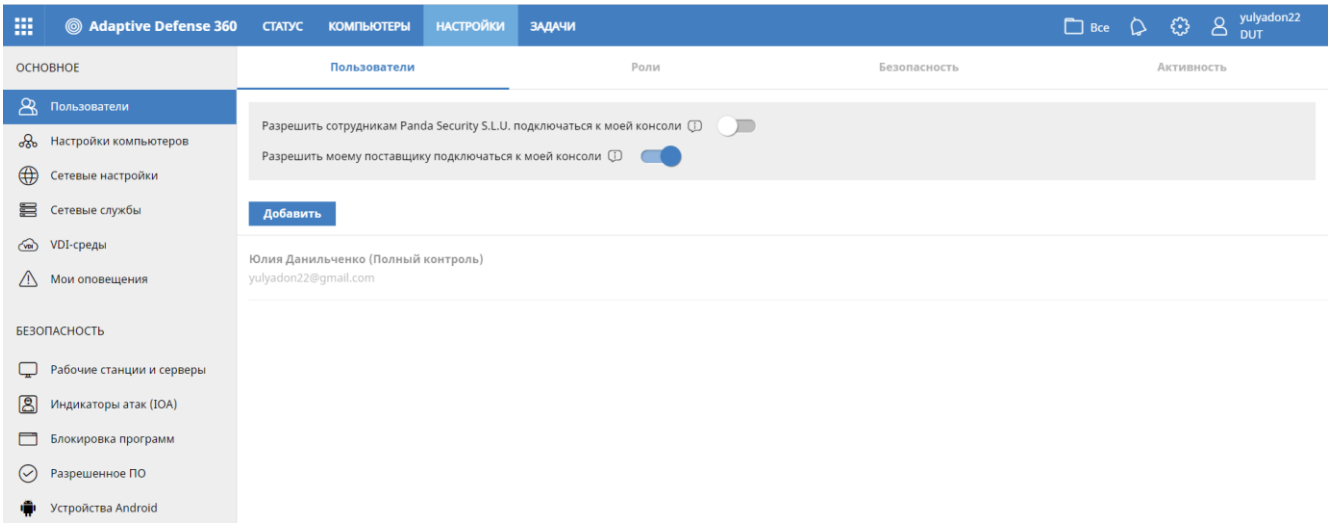


Рис. 3.26. Список користувачів, що мають право на доступ до консолі керування

У вкладці «Ролі» відбувається налаштування шаблонів ролей. За замовчуванням тут представлені лише: Повний контроль та Тільки для читання (що передбачає лише моніторинг). Ці ролі не підлягають перейменуванню або видаленню. Але завжди можна налаштувати власні ролі, потрібно натиснути «Додати».

Кожну роль можна детально налаштувати, дозволити або заборонити: керувати користувачами, призначати ліцензії, виконувати різноманітні дії з пристроями, вчиняти дії, пов'язані з безпекою.

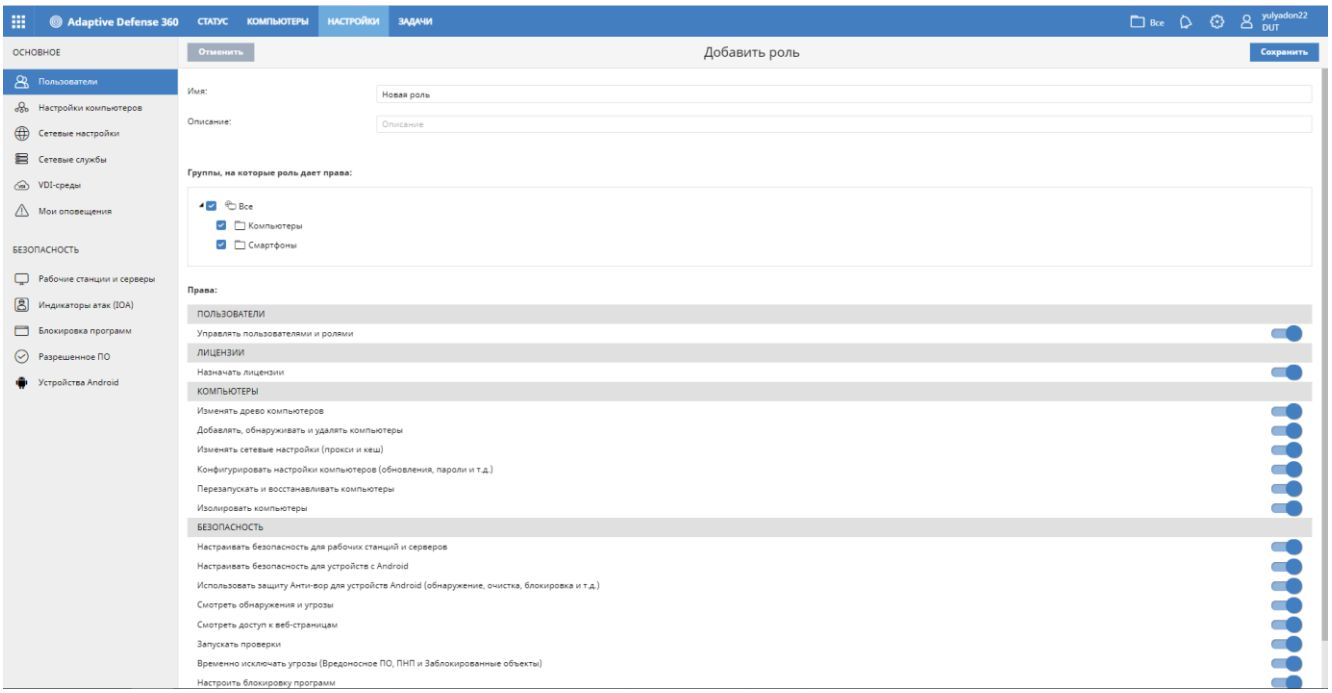


Рис. 3.27. Додавання та налаштування нової ролі

Вкладка «Активність» демонструє журнал активності користувачів, які користуються консоллю керування. Інформацію можна відсортувати за конкретним користувачем та датами користування консоллю. У таблиці активності можна побачити таку інформацію:

- час та дату активності;
- ім'я користувача, який виконував цю дію;
- назва дії;
- тип об'єкта;
- об'єкт, стосовно якого було скоєно дію.

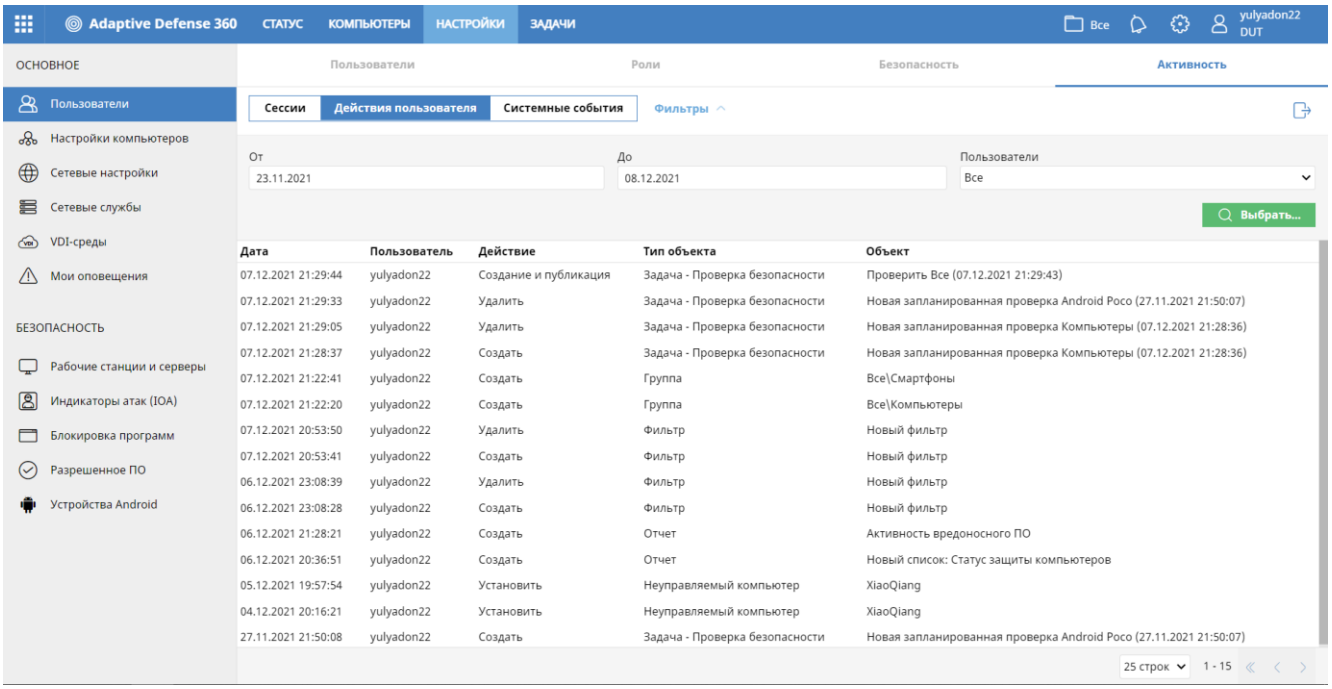


Рис. 3.28. Журнал активності користувачів консолі Aether

Вся інформація, яка описана вище, знаходиться за кнопкою «Дії користувача». Якщо ж натиснути на кнопку «Сесії», то можна побачити всі сесії користувачів з датою та часом, ім'ям користувача, видом активності та IP-адресою користувача.

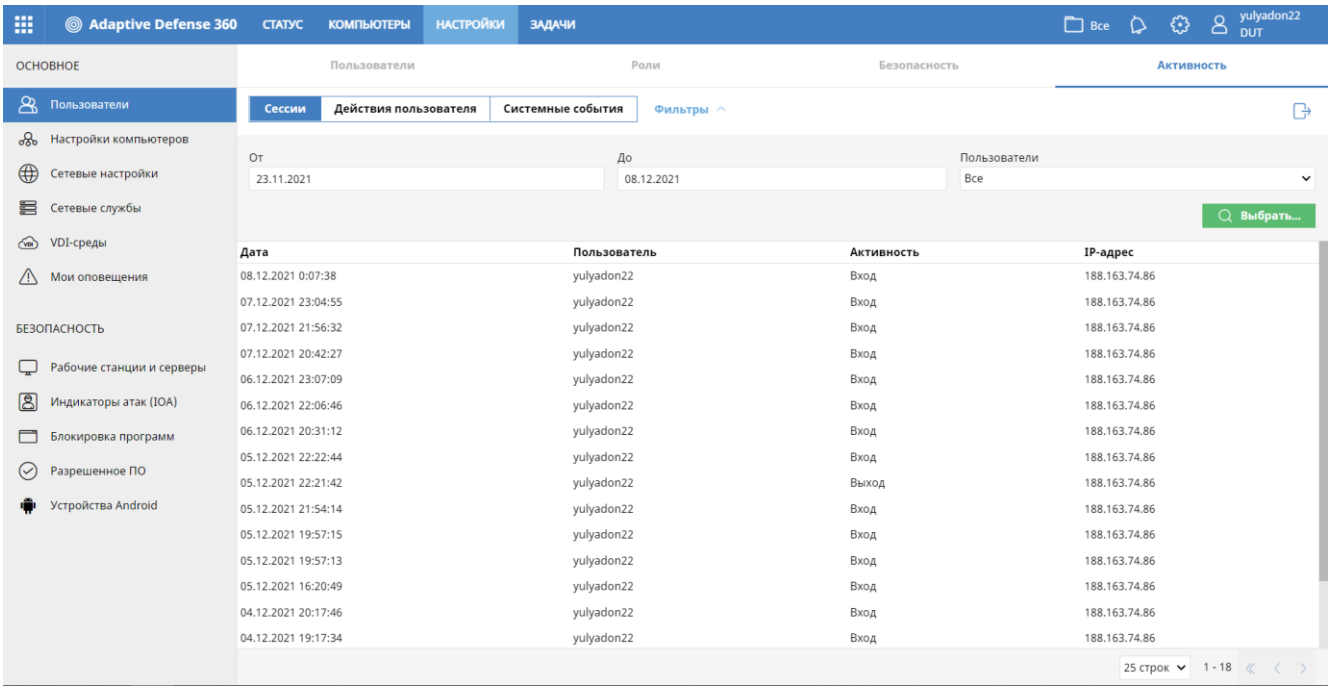


Рис. 3.29. Список сесій користувачів консолі Aether

Після натискання на кнопку «Системні події» відкривається список системних подій з датою та часом, описом вчиненої події, типом пристрою та його назвою.

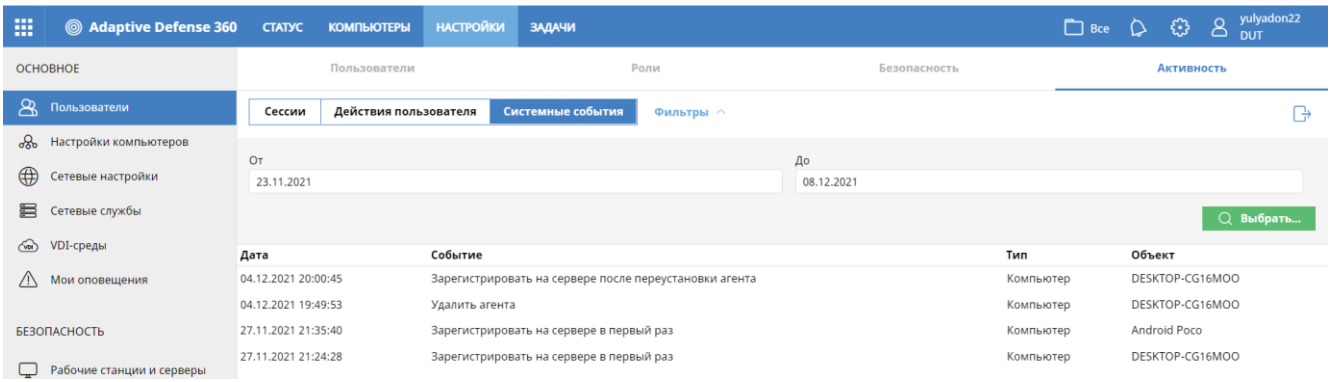


Рис. 3.30. Список системних подій у платформі Aether

*Налаштування комп'ютерів*

Наступним розділом у налаштуваннях є «Налаштування комп'ютерів». У цьому розділі налаштовуються політики з параметрами Panda Adaptive Defense 360 на комп'ютерах.

Спочатку в консолі є політика «Налаштування за замовчуванням». Ця політика не підлягає видаленню, але її можна змінити. Також існує можливість створювати свої власні політики натиснувши кнопку «Додати».

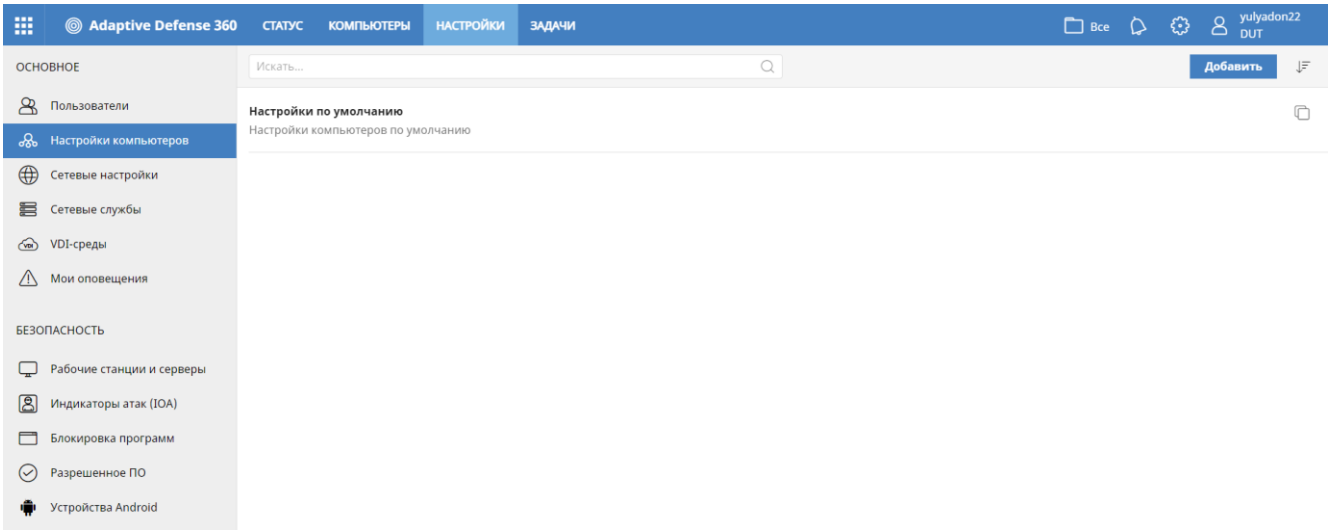


Рис. 3.31. Розділ «Налаштування комп’ютерів» у платформі Aether

У розділі додавання нової політики необхідно дати їй назву та опис, за необхідності. Нижче вибирається отримувач політики. Їм може стати група комп'ютерів з дерева організації або окремі пристрої, не ґрунтуючись на певній групі.

У вкладці «Оновлення» є можливість налаштувати графік оновлення агента на пристроях. Можна також заборонити або дозволити автоматичне оновлення Panda Adaptive Defense 360.

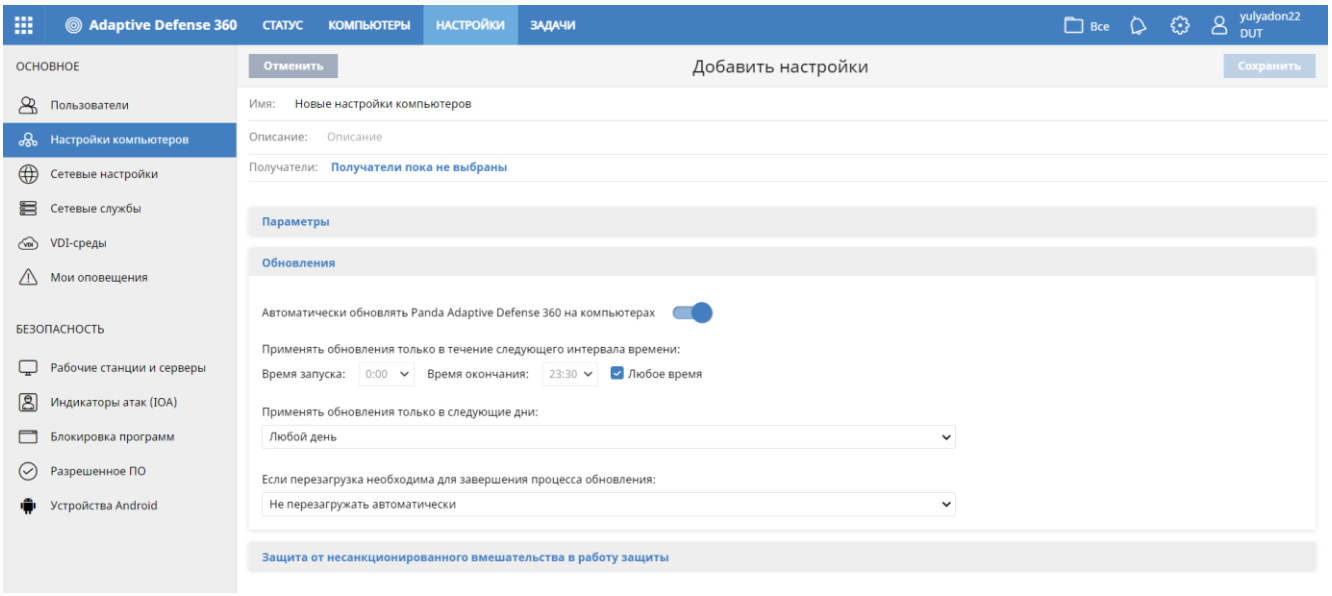


Рис. 3.32. Налаштування параметрів оновлення при додаванні нової політики

Вкладка "Захист від несанкціонованого втручання в роботу захисту" дає можливість налаштувати такі параметри як:

- Дозвіл або заборона запиту пароля при видаленні захисту з пристрою;
- Дозвіл або заборона увімкнення/вимкнення модулів захисту з локальної консолі комп'ютера;
- Увімкнення або вимкнення захисту Anti-Tamper, який не дозволяє користувачам та певним типам загроз зупиняти роботу захисту.

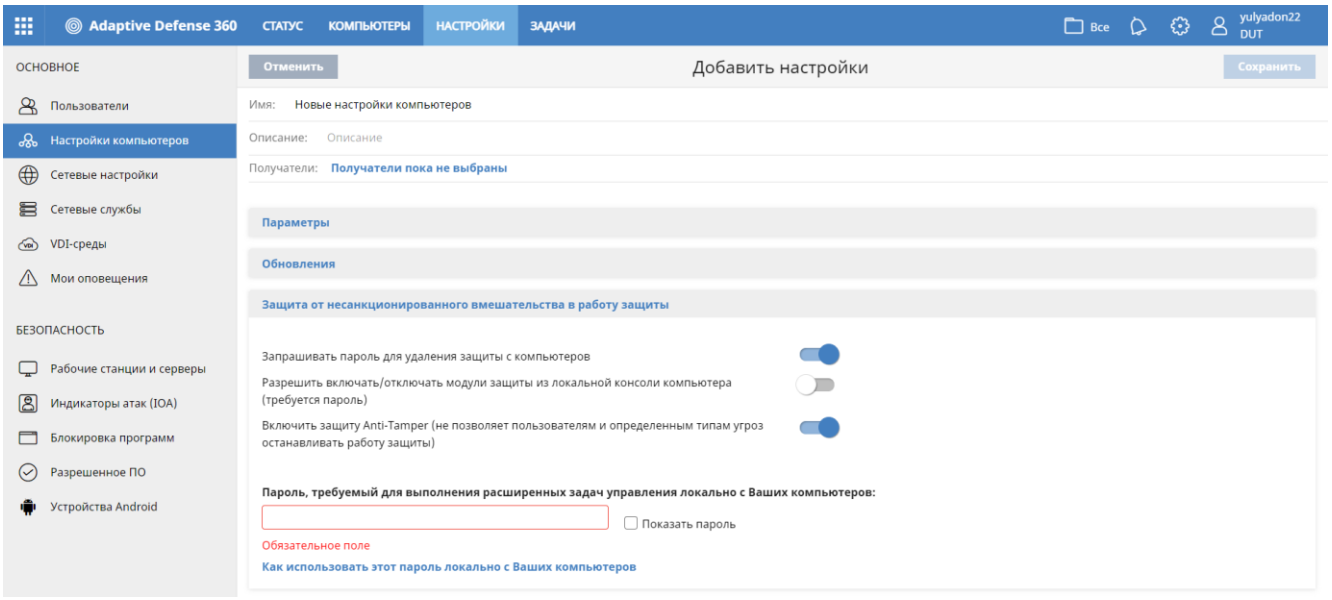


Рис. 3.33. Налаштування параметрів захисту при додаванні нової політики

У цьому розділі було розглянуто всі основні та важливі функції консолі керування Aether, за допомогою якої відбувається керування рішенням Panda Adaptive Defense 360. Ця консоль допомагає адміністратору безпеки більш детально контролювати та керувати безпекою на кінцевих точках в організаціях різного розміру.

Платформа має найважливіші функції, такі як, виявлення незахищених пристроїв, використання фільтрів, налаштування ролей, відстеження дій користувачів. Можна переглядати встановлені на кінцеві пристрої ПЗ та апаратне забезпечення тощо.

Наявність усіх цих функцій в одній платформі допомагає адміністратору безпеки стежити за всіма загрозами в режимі реального часу та реагувати на всі інциденти безпеки кінцевих точок.

## 3.3. Розроблення рекомендацій щодо застосування технології захисту кінцевих точок організації

Після розгляду основних функцій рішення будуть наведенні рекомендації як максимально ефективно впровадити та використовувати технологію Panda Adaptive Defense 360 для захисту кінцевих точок організації.

1. Спершу, як вже було вказано, треба встановити рішення на кінцевий пристрій, що буде використовуватись як комп'ютер для виявлень. Таким комп'ютером буде автоматично визначено той, який першим буде підключений до системи безпеки. Завдяки ньому можна буде відслідковувати усі дії та атаки на інші кінцеві точки, дії користувачів у мережі і т. д.

Для цього потрібно на комп'ютер встановити агент Panda, завдяки якому буде проводитись сканування пристрою та передаватись інформація про стан захищеності у консоль управління.

2. Далі потрібно додати усі кінцеві точки у консоль, для цього у ній генерується файл для встановлення агенту на пристрої. Важливо відмітити, що відстежуватись повинні усі пристрої, що мають доступ до інформаційної системи організації, у тому числі, це мають бути і комп'ютери, що співробітники приносять на роботу по концепції BYOD та смартфони, що мають доступ до системи. Агент Panda важить не багато, тому може бути встановлений на будь-який пристрій, що відповідає вимогам для інсталяції.

Коли усі кінцеві пристрої додано до консолі слід перевірити чи нема некерованих комп'ютерів, якщо такі залишились, можна встановити агента віддалено прямо з консолі, якщо до пристрою є доступ.

3. Наступним кроком треба налаштувати фільтри пристроїв, за замовчуванням вже є фільтри по типу ОС, типу системи, обладнанню та ПЗ. Але завжди за потребою можна створити власний фільтр або папку, аби відстежувати безпеку пристроїв за певними критеріями та вчасно, за лічені секунди, реагувати на інциденти безпеки, якщо це сталось одразу з великою кількістю кінцевих точок.

Корисним також буде відтворити ієрархію кінцевих пристроїв організації у відповідному розділі «Моя організація» для більш зручного контролю за безпекою організації у всіх її підрозділах.

4. Якщо в організації декілька адміністраторів безпеки варто визначити які ролі будуть їм доступні, за замовченням існує роль повного контролю та тільки для читання, останню доцільно дати користувачам, що зможуть спостерігати за станом захищеності, але ніяк не зможуть впливати на нього, зазвичай це керівництво підприємства. Активність кожного користувача завжди можна буде відстежити у розділі «Активність».

5. При налаштуванні кінцевих точок рекомендується включити автоматичні оновлення агента в будь-який час і вказавши конкретний зручний графік. Також слід вказати, чи необхідно автоматичне перезавантаження пристроїв після оновлення.

Від несанкціонованого втручання важливо вказати обов'язкове запитування пароля, при необхідності видалити агента захисту з пристрою, щоб співробітники не мали можливості самостійно навмисно або випадково видалити агента.

Корисною буде установка дозволу на керування (увімкнення/вимкнення) модулями захисту пристроїв з локальної консолі, це може знадобитися при адмініструванні або усуненні несправностей (для керування необхідно буде ввести пароль).

6. Для постійного контролю за безпекою варто налаштувати поштові оповіщення. За замовчуванням вони приходять на пошту за якою було зареєстровано акаунт у консолі. Можна додати додаткові пошти та вибрати інформація про які інциденти буде надходити.

7. Наступним дуже важливим аспектом застосування рішення є налаштування безпеки на кінцевих пристроях. Тут варто відзначити контроль веб-доступу. Можна заборонити доступ до сторінок, що належать до певних категорій, наприклад, матеріали 18+, потенційно небезпечні сайти, соціальні мережі, якщо це передбачено політикою підприємства. Визначити заборонені сайти можна не тільки по категоріям, але й заборонити доступ до конкретних адрес та доменів.

При забороні доступу до певних сайтів для персональних девайсів, що співробітники приносять із собою, можна становити часові рамки (тільки на під час робочого дня та у робочі дні). Додатково можна вказати певні програми, що будуть блокуватись при спробах їх запуску.

На пристроях на ОС Android можна встановити захист «Анти-вор» для відстеження пристрою, якщо його вкрали.

# ВИСНОВКИ

У магістерській роботі було проведено дослідження проблеми захисту кінцевих точок інформаційних систем організацій. Було визначено, що дане питання є важливим, адже щодня інформація в організаціях передається між кінцевими точками, а тому вони є головною метою для зловмисників, що хочуть викрити цю інформацію, для цього вони шукають все нові вразливості кінцевих точок.

В результаті роботи були вирішені такі наукові завдання:

1. Була проаналізована науково-літературна база та визначено, що кінцевими пристроями є ті, що або починають процес передачі даних в інформаційній системі організації, або вимагають отримання даних в інших кінцевих пристроїв. Ними на підприємстві можуть бути: комп'ютери, сервери, мобільні телефони, віртуальні середовища і т. д.

2. Вивчивши дослідження, було з'ясовано, що атаки на кінцеві точки організацій є найпоширенішими. А компанії, що використовують концепцію BYOD, без належного захисту, частіше схильні до найвищого ризику атак на кінцеві точки. Тому що особисті пристрої співробітників частіше заражаються шкідливим ПЗ, ніж аналогічні, що знаходяться тільки в організаціях.

3. Було проаналізовано існуючі технології захисту кінцевих точок та виявлено, що для їх захисту недостатньо звичайного антивірусу. Для якісного захисту кінцевих точок необхідно використовувати інструменти класу (EDR), що створені аби виявляти та вивчати шкідливу активність на кінцевих точках. Важливо, що EDR-рішення здатні виявляти цільові атаки, складні загрози та вразливості «нульового дня».

4. Наступним кроком було проведено огляд програмних для захисту кінцевих точок на основі Gartner Magic Quadrant 2021. В якості прикладів було розглянуто продукти з секції «Лідери», що мають широкі можливості розширеного захисту від

шкідливих програм і перевірені можливості управління великих корпоративних акаунтів.

5. Для розробки варіанту технології захисту кінцевих точок я обрала рішення Panda Adaptive Defense 360, що також знаходилось в Gartner Magic Quadrant 2021, але у секції «Нішевий гравець».

Було розглянуто призначення, можливості та функції рішення Panda Adaptive Defense 360. Приділено не мало уваги важливому компоненту цього рішення – платформі Aether, завдяки якій відбувається керування рішенням. А саме розглянуті можливості, переваги та архітектура консолі.

6. Розглянувши усі особливості технології, її переваги та функціонал, останнім етапом були розроблені рекомендації щодо ефективного застосування технології захисту кінцевих точок організації.

## ПЕРЕЛІК ПОСИЛАНЬ


1. Understanding Endpoints and Endpoint Security [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.webroot.com/us/en/resources/glossary/what-is-endpoint-security. – Загл. з екрану (переглянуто 24 квітня 2020).

2. Основные компонеты сетей [Електронний ресурс] — Режим доступу: World Wide Web. – URL: http://infocisco.ru/network_components.html. – Загл. з екрану (переглянуто 24 квітня 2020).

3. The Third Annual Study on the State of Endpoint Security Risk [Електронний ресурс] // Ponemon Institute LLC, 2020.— Режим доступу: World Wide Web. – URL: https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf. – Загл. з екрану (переглянуто 24 квітня 2020).

4. Caitlin Jones. 50 Endpoint Security Stats You Should Know In 2021. [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://expertinsights.com/insights/50-endpoint-security-stats-you-should-know/. – Загл. з екрану (переглянуто 24 квітня 2020).

5. Что такое атака на конечную точку? [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://tehnografi.com/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D1%83%D1%8E-%D1%82%D0%BE%D1%87%D0%BA%D1%83/. – Загл.З екрану(переглянуто 24 квітня 2020).

6. Эволюция векторов атак на конечные точки предприятия [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://bakotech.ua/news/evolyuciya-vektorov-atak-na-konechnie-tochki-predpriyatiya/. – Загл. З екрану (переглянуто 24 квітня 2020).

7. Пять видов атак, которые ваш обычный антивирус не обнаружит [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://bakotech.ua/news/pyat-vidov-atak-kotorie-vash-obichniy-antivirus-ne-obnaruzhit/. – Загл. З екрану (переглянуто 24 квітня 2020).

8. Денис Саричев. Защита конечных точек в современных условиях. 27 жовтня 2021 р.[Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/EndPoint-Protection-in-modern-conditions. – Загл. З екрану (переглянуто 24 квітня 2020).

9. Олексій Матвєєв. Обзор рынка систем защиты конечных точек (Endpoint Protection Platform). 02 серпня 2018 р. [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-protection-platform. – Загл. З екрану (переглянуто 24 квітня 2020).

10.Magic Quadrant for Endpoint Protection Platforms. 5 травня 2021 р. [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.hsdf.org/wp-content/uploads/2021/06/Magic_Quadrant_for_E_450741_ndx.pdf. – Загл. З екрану (переглянуто 24 квітня 2020).

11.Защита конечных точек [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.mcafee.com/enterprise/ru-ru/products/endpoint-protection-products.html. – Загл. З екрану (переглянуто 24 квітня 2020).

12.Microsoft Defender для кінцевих точок [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.microsoft.com/uk-ua/security/business/threat-protection/endpoint-defender. – Загл. З екрану (переглянуто 24 квітня 2020).

13.Intercept X Endpoint [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.sophos.com/en-us/support/products/intercept-x-endpoint.aspx. – Загл. З екрану (переглянуто 24 квітня 2020).

14.CrowdStrike Falcon Endpoint Protection Pro [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://iitd.com.ua/ru/crowdstrike/falcon-endpoint-protection-pro/. – Загл. З екрану (переглянуто 24 квітня 2020).

15.Panda Adaptive Defense 360 [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.cloudav.ru/upload/iblock/2b0/PAD360%20-%20%D0%91%D1%80%D0%BE%D1%88%D1%8E%D1%80%D0%B0.pdf. – Загл. З екрану (переглянуто 24 квітня 2020).

16.Panda Adaptive Defense 360 [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.cloudav.ru/upload/iblock/715/PAD360%20-%20%D0%9E%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82%D0%B0.pdf. – Загл. З екрану (переглянуто 24 квітня 2020).

17.Решения для защиты от атак и расследования нарушений [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.cloudav.ru/upload/iblock/391/Panda%20-%20%D0%A2%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D0%B0%20%D0%BA%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D1%85%20%D1%80%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D0%B9.pdf. – Загл. З екрану (переглянуто 24 квітня 2020).

18.Panda Security. Panda Adaptive Defense 360 administration guide. 12 липня 2021 р. [Електронний ресурс] — Режим доступу: World Wide Web. – URL: https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/v12/ADAPTIVEDEFENSE360oAP-guide-EN.pdf. – Загл. З екрану (переглянуто 24 квітня 2020).

**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)**