ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо виявлення та реагування на інциденти безпеки в корпоративних кінцевих точках за допомогою FortiEDR»

зі спеціальності *125 Кібербезпека*

(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*

(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

ЮВЧЕНКО Дмітрій

(підпис)

Виконав: здобувач вищої освіти групи БСД-42

ЮВЧЕНКО Дмітрій

(прізвище, ім'я)

Керівник д. т. н., професор,Кожухівський А.Д.

(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент

(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 73 сторінки, 2 рисунків, 33 джерела.

Об'єкт дослідження – захист кінцевих точок організації.
Предмет дослідження – методи та засоби захисту кінцевих точок організації на базі FortiEDR.
Мета роботи розробити рекомендації щодо застосування методів та засобів захисту кінцевих точок організації та рекомендації щодо їх реалізації.
Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.
Системи виявлення та реагування на кінцеві точки (EDR) відіграють важливу роль у підвищенні безпеки кінцевих точок організації. Системи EDR призначені для постійно моніторингу дій та поведінки кінцевих точок. Системи EDR забезпечують видимість діяльності кінцевих точок у реальному часі, що дозволяє організаціям швидко реагувати на інциденти безпеки.
В роботі проаналізовано проблему захисту кінцевих точок організації, визначено його мету та завдання. Проведено аналіз існуючих технологій захисту кінцевих точок організації. Досліджено методи та засоби захисту кінцевих точок організації на базі FortiEDR. Визначено призначення, основні функції та склад рішення FortiEDR.
На основі досліджень проведених в роботі розроблено рекомендації щодо застосування методів та засобів захисту кінцевих точок організації на базі FortiEDR. Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів захисту кінцевих точок організації.

Галузь використання – кібербезпека інформаційних ресурсів організації.

ЗМІСТ

ВСТУП

У сучасному світі інформаційні технології стали основою функціонування бізнесу, державного управління, інфраструктури та обороноздатності країни. Разом з цим стрімкий розвиток цифрового середовища супроводжується зростанням кількості та складності кіберзагроз, які стають дедалі більш таргетованими, витонченими та деструктивними. Згідно з аналітичними звітами провідних компаній у сфері кібербезпеки, щорічна кількість інцидентів безпеки зростає на 15–25%, а більшість атак залишаються непоміченими протягом тривалого часу. Особливо вразливими є корпоративні кінцеві точки — робочі станції, ноутбуки, сервери, мобільні пристрої, — які є першими мішенями вектора атаки. Традиційні антивірусні засоби не здатні ефективно протистояти загрозам типу zero-day, fileless-атакам та загрозам, що базуються на поведінкових аномаліях. У таких умовах актуальним є перехід до новітніх рішень класу EDR (Endpoint Detection and Response), які дозволяють виявляти, локалізовувати та нейтралізовувати інциденти безпеки в режимі реального часу.

Особливої актуальності тема дослідження набуває для українських підприємств, які перебувають під постійною кіберзагрозою внаслідок гібридної агресії та кібершпигунства з боку держав-противників. В умовах зростання частоти кібератак на критичну інфраструктуру, державні установи, приватні компанії та банківську систему, впровадження дієвих технологічних рішень стає не лише питанням ефективності бізнесу, а й складовою національної безпеки. У зв’язку з цим необхідність комплексного аналізу EDR-рішень, таких як FortiEDR, обґрунтування їх доцільності, функціонального потенціалу, практичних сценаріїв застосування та адаптації до українських реалій є надзвичайно важливою як у науковому, так і у прикладному аспектах.

Об’єктом дослідження є процес забезпечення інформаційної безпеки корпоративної IT-інфраструктури в умовах сучасних кіберзагроз.

Предметом дослідження виступають методи виявлення, реагування та нейтралізації інцидентів інформаційної безпеки з використанням системи FortiEDR як інструменту класу EDR.

Метою дослідження є розроблення практичних рекомендацій щодо ефективного використання системи FortiEDR у корпоративному середовищі для забезпечення проактивного виявлення та реагування на інциденти інформаційної безпеки з урахуванням українського контексту.

Для досягнення поставленої мети в роботі необхідно розв’язати такі завдання:

1. Провести аналіз актуальних загроз інформаційної безпеки у корпоративному середовищі.
2. Дослідити еволюцію засобів виявлення загроз: від антивірусних рішень до EDR.
3. Оцінити нормативно-правове забезпечення, що регламентує використання засобів кіберзахисту (ISO/IEC 27001, NIST, GDPR, українські стандарти).
4. Провести порівняльний аналіз сучасних рішень класу EDR, виділивши сильні та слабкі сторони FortiEDR.
5. Дослідити архітектуру, функціональність та механізми реагування FortiEDR у контексті реального впровадження.
6. Проаналізувати практичні кейси використання FortiEDR для виявлення загроз та оцінки ефективності реагування.
7. Розробити модель оптимізації політик безпеки та реагування в FortiEDR.
8. Запропонувати підходи до інтеграції FortiEDR з іншими системами безпеки (SIEM, SOAR).
9. Сформувати методику підготовки персоналу до роботи з FortiEDR.
10. Надати пропозиції щодо адаптації досвіду до українських підприємств.

Методи дослідження, використані в роботі, включають системний аналіз, компаративну методику порівняння рішень, моделювання інцидентів, аналіз логів, метод експертного оцінювання, елементний аналіз архітектури, методи прикладної статистики (у частині верифікації ефективності).

Практичне значення одержаних результатів полягає в тому, що напрацьовані в межах дослідження рекомендації можуть бути використані українськими підприємствами для впровадження FortiEDR як ефективного засобу реагування на інциденти безпеки. Запропоновані моделі можуть стати основою для розробки внутрішніх регламентів кіберзахисту, навчальних програм для персоналу, оптимізації IT-безпекової архітектури.

Апробація результатів здійснювалась шляхом застосування окремих положень роботи в ході тестового розгортання системи FortiEDR на середньому підприємстві IT-сфери. Елементи дослідження доповідались у рамках участі у міжкафедральному семінарі на факультеті кібербезпеки, де були позитивно оцінені фахівцями галузі.

Таким чином, тема дослідження є науково і практично обґрунтованою, її результати мають прикладне значення та можуть бути реалізовані в умовах сучасної української цифрової реальності.

РОЗДІЛ 1. Теоретичні основи виявлення інцидентів у кінцевих точках корпоративних систем

1.1. Загрози інформаційної безпеки у корпоративному середовищі

У сучасному цифровому світі корпоративне середовище піддається значному ризику з боку різноманітних кіберзагроз, які постійно еволюціонують. Інформаційна безпека перетворилася на одну з ключових стратегічних сфер для кожної організації, адже будь-яка загроза, що стосується конфіденційності, цілісності чи доступності інформаційних ресурсів, може мати серйозні економічні, репутаційні та правові наслідки. У контексті глобалізації бізнес-процесів та зростання залежності від цифрових технологій, кінцеві точки — персональні комп'ютери, ноутбуки, сервери, мобільні пристрої, IoT-пристрої — стають основними цілями зловмисників, які прагнуть порушити нормальне функціонування інформаційних систем компаній. Розвиток віддаленої роботи, хмарних сервісів та Bring Your Own Device (BYOD) лише ускладнює ситуацію, знижуючи рівень контролю над інформаційними потоками й підвищуючи вразливість корпоративної IT-інфраструктури.

Однією з найпоширеніших загроз інформаційній безпеці є шкідливе програмне забезпечення (malware), зокрема віруси, трояни, руткіти, шпигунські програми, програми-вимагачі (ransomware). Такі загрози часто потрапляють до мережі через фішингові листи, скомпрометовані вебсайти або знімні носії, заражаючи кінцеві точки й надаючи зловмисникам віддалений доступ або контроль над ними. Особливо небезпечним є ransomware, який шифрує важливі корпоративні дані та вимагає викуп за їх розшифрування, часто не гарантуючи повернення доступу навіть після сплати. Крім того, складні багатоетапні атаки типу Advanced Persistent Threats (APT) мають на меті довготривале проникнення до внутрішніх мереж компаній із ціллю викрадення конфіденційної інформації, інтелектуальної власності або шпигунства за бізнес-процесами [12].

Іншою вагомою загрозою є фішинг — метод соціальної інженерії, за якого зловмисники, видаючи себе за легітимних осіб або служби, змушують працівників розкривати облікові дані, паролі, фінансову або технічну інформацію. В умовах сучасного корпоративного середовища фішинг активно розвивається у вигляді spear-phishing (цільовий фішинг) та business email compromise (BEC), що передбачає підміну корпоративних адрес електронної пошти й обман бухгалтерії чи керівництва. Такі атаки відрізняються високим рівнем персоналізації, що значно підвищує їх ефективність. Крім того, вразливими залишаються мобільні пристрої працівників, які можуть бути заражені через SMS-фішинг, використання публічних Wi-Fi-мереж або встановлення недостовірних застосунків.

Ще однією значною категорією загроз є атаки типу "людина посередині" (Man-in-the-Middle, MitM), які дозволяють перехоплювати трафік між двома сторонами без їхнього відома. Це може бути особливо небезпечно для корпоративних VPN-з’єднань або комунікацій у хмарних сервісах. Успішна атака MitM здатна призвести до втрати даних, компрометації облікових записів та викрадення конфіденційної інформації. Також розвиваються атаки на бездротові мережі, зокрема Wi-Fi spoofing та Evil Twin, які дозволяють зловмисникам отримати доступ до внутрішнього мережевого трафіку або перенаправляти користувачів на фальшиві ресурси.

Значну загрозу для інформаційної безпеки становить також внутрішній фактор — дії або бездіяльність співробітників організації. Ненавмисні дії, такі як неправильне налаштування систем, відкриття підозрілих вкладень, використання слабких паролів або порушення політик безпеки, часто стають причиною витоків даних або доступу зловмисників до внутрішніх ресурсів. Окрім того, існує й ризик зловмисних дій з боку самих працівників, які мають легітимний доступ до чутливої інформації й можуть свідомо використовувати її у власних цілях або передавати конкурентам. Такі загрози часто залишаються непоміченими традиційними засобами захисту й потребують спеціалізованих інструментів моніторингу активності користувачів.

Значним викликом для корпорацій є також загрози, пов’язані з постачальницьким ланцюгом (supply chain attacks), коли вразливість або компрометація партнерської організації стає шляхом проникнення у власну систему. Прикладом може слугувати відомий інцидент із компанією SolarWinds, внаслідок якого тисячі клієнтів, включаючи урядові структури та великі корпорації, стали жертвами прихованої атаки через легітимне програмне забезпечення. Такі інциденти свідчать про необхідність жорсткого контролю за контрагентами, оновленнями ПЗ та використанням цифрових сертифікатів.

У корпоративному середовищі також важливу роль відіграють загрози, пов’язані з недостатнім рівнем оновлення програмного забезпечення та операційних систем. Уразливості типу zero-day, тобто ті, що ще не відомі розробникам ПЗ, активно експлуатуються кіберзлочинцями. І навіть відомі вразливості, які вже мають патчі, можуть залишатись невиправленими протягом тривалого часу через недбалість або технічну заборгованість. Це створює сприятливе середовище для масштабних атак, спрямованих на обхід класичних антивірусів і систем захисту [25].

Ще одним типом загроз, що активно набирає обертів, є атаки на основі штучного інтелекту та машинного навчання. Сучасні шкідливі програми здатні адаптуватися до захисного середовища, приховувати свою активність і обходити засоби детектування. Також використовуються методи deepfake для створення фальшивих голосових або відеоповідомлень, які можуть вводити в оману персонал і призводити до порушення безпекових процедур.

З огляду на наведені загрози, інформаційна безпека у корпоративному середовищі потребує багаторівневого підходу до захисту. Зокрема, захист кінцевих точок повинен забезпечувати не лише базові антивірусні функції, а й постійний моніторинг, аналіз поведінки, можливість ізоляції заражених пристроїв, збирання артефактів і здійснення автоматизованого реагування на інциденти. Сучасні інструменти класу EDR (Endpoint Detection and Response) створені саме для цього — вони дозволяють перейти від реактивного до

проактивного захисту, де потенційні загрози виявляються ще до моменту нанесення шкоди.

У результаті слід зазначити, що корпоративне середовище залишається уразливим до широкого спектру загроз, які можуть мати як технічну, так і соціальну природу. Ефективне управління інформаційною безпекою неможливе без усвідомлення характеру цих загроз, постійного оновлення засобів захисту та впровадження інноваційних технологій на кшталт FortiEDR, які здатні забезпечити високий рівень реагування й адаптивності в умовах змінного кіберландшафту [21].

1.2. Еволюція засобів виявлення інцидентів: від антивірусу до EDR

У сучасному цифровому середовищі розвиток засобів виявлення інцидентів безпеки є логічною відповіддю на стрімку еволюцію загроз, які стають дедалі складнішими, нав’язливішими та багаторівневими. Починаючи з найперших інструментів захисту — антивірусного програмного забезпечення, — сфера кібербезпеки пройшла довгий шлях до появи сучасних систем виявлення та реагування на інциденти, які базуються на поведінковому аналізі, машинному навчанні та інтеграції з централізованими платформами. Основною рушійною силою цієї трансформації стала необхідність вийти за межі реактивного підходу, що базувався на сигнатурах відомих загроз, і перейти до проактивного аналізу нових, ще невідомих або замаскованих атак. Така еволюція засобів виявлення інцидентів є фундаментальною передумовою підвищення рівня кіберзахисту як на індивідуальному рівні, так і в масштабі корпоративних IT-інфраструктур.

Перші антивірусні програми з’явилися ще у 1980-х роках і мали вузьку спеціалізацію — вони шукали конкретні сигнатури відомих вірусів у двійковому коді файлів. Це дозволяло виявляти й видаляти обмежену кількість шкідливих об'єктів, що були на той момент відомими. Сигнатурний підхід став стандартом у галузі на десятки років. Однак він мав суттєві обмеження —

виявлення залежало від того, чи встиг виробник антивірусу отримати, проаналізувати й оновити базу даних для нового вірусу. У разі появи zero-day атак, коли зловмисне програмне забезпечення використовує невідомі вразливості або алгоритми шифрування, класичні антивіруси виявлялись безсилими. Крім того, з часом з'явились віруси з поліморфними та метаморфними можливостями, які змінювали свою структуру кожного разу при зараженні нового пристрою, що унеможливлювало використання класичних сигнатурних механізмів.

У відповідь на ці виклики на початку 2000-х років почали з'являтися продукти нового покоління, які об'єднували антивірус із проактивними модулями аналізу. Зокрема, було запроваджено евристичний аналіз — здатність розпізнавати підозрілу поведінку програм, яка не відповідає типовим шаблонам. Програми з високою частотою доступу до системних файлів, несанкціонованим використанням мережевих портів або прихованими процесами розцінювались як потенційно небезпечні. Хоча такі рішення могли забезпечити виявлення нових загроз, вони нерідко викликали помилкові спрацьовування (false positives), що ускладнювало їх використання в реальному корпоративному середовищі. Технології поведінкового аналізу та так званої «пісочниці» (sandboxing), які дозволяли запускати підозрілі програми у віртуальному середовищі для спостереження за їхньою поведінкою, стали черговим кроком до ускладнення систем захисту.

Паралельно з цим, зі зростанням кількості кіберінцидентів, компанії почали впроваджувати централізовані системи моніторингу подій — SIEM (Security Information and Event Management). SIEM-інструменти дозволяли збирати логи з різних джерел, включаючи мережеві пристрої, сервери, системи контролю доступу, та здійснювати їхню централізовану кореляцію для виявлення аномалій. Проте вони не завжди мали глибоку інтеграцію із самими кінцевими точками і часто були спрямовані на ретроспективний аналіз. Це означає, що інцидент вже відбувся, і SIEM фіксував його лише як подію, яку

потрібно дослідити вручну аналітиками безпеки. Тобто система не запобігала інциденту, а лише сигналізувала про нього.

У відповідь на потребу в активнішому захисті саме кінцевих точок, на межі 2010-х років було розроблено концепцію EPP (Endpoint Protection Platform) — платформи захисту кінцевих точок. EPP поєднували антивірусні рішення, firewall, систему контролю доступу та базові засоби шифрування. Проте й ці платформи були переважно профілактичними, без здатності до активного реагування на складні атаки, зокрема ті, що вже проникли до мережі й перебували в латентному стані.

Наступним етапом стала поява систем класу EDR (Endpoint Detection and Response), які мали на меті виявляти та реагувати на загрози на рівні кінцевих точок не лише за допомогою сигнатур або евристики, а через аналіз поведінкових сценаріїв. Одним з ключових елементів EDR є агент, який встановлюється на кожну кінцеву точку та безперервно моніторить активність — запуск процесів, взаємодію з файлами, мережеву активність, звернення до реєстру, зміни в ОС. Ці дані збираються й надсилаються на централізовану консоль, де вони аналізуються за допомогою правил кореляції, машинного навчання або навіть алгоритмів штучного інтелекту. При виявленні аномальної поведінки система може автоматично або вручну ізолювати кінцеву точку, зупинити процес, розпочати сканування або проаналізувати атаку у ретроспективі [17].

Перевага EDR полягає в тому, що вона не лише виявляє атаки, а й допомагає у їхньому розслідуванні. Детальна хронологія дій, логування всіх дій користувача та програм дозволяє безпековим аналітикам зрозуміти природу загрози, її джерело, спосіб проникнення та потенційне розповсюдження. Завдяки цьому компанії можуть будувати цілісні playbooks (сценарії реагування), оптимізувати політики безпеки та запобігати повторному виникненню подібних інцидентів у майбутньому.

Еволюція не зупинилась на класичних EDR. З появою рішень SOAR (Security Orchestration, Automation, and Response), аналітики отримали змогу

автоматизувати реагування на інциденти шляхом інтеграції EDR із SIEM, Threat Intelligence платформами, CMDB, ticket-системами. В умовах перенавантаження команди безпеки величезною кількістю сповіщень, автоматизація процесів реагування дозволяє значно скоротити час реакції (Mean Time to Response — MTTR) та усунути рутинні завдання. Деякі рішення, зокрема FortiEDR, вже вбудовують ці функції на рівні агентів, поєднуючи в собі не лише моніторинг, а й активне реагування у вигляді блокування шкідливих дій, ізоляції пристрою від мережі або повідомлення про подію до централізованої системи.

Таким чином, еволюція засобів виявлення інцидентів — від антивірусів до EDR — є результатом переходу від простих реактивних механізмів до складних проактивних і аналітичних систем, що дозволяють не лише запобігати, а й швидко реагувати на складні атаки. Сьогодні класичний антивірус вже не здатен забезпечити повний захист у багаторівневому середовищі загроз. Компанії потребують рішень, які не тільки ідентифікують інциденти, але й дозволяють розуміти логіку атаки, автоматично відповідати на неї та інтегруватися з іншими системами безпеки. Тому саме системи EDR, а в подальшому й XDR (Extended Detection and Response), є логічним продовженням еволюції захисту корпоративного середовища й основою для побудови сучасної, адаптивної кібербезпеки [8].

1.3. Аналіз нормативно-правових актів та стандартів (ISO/IEC 27001, NIST, GDPR тощо)

Сучасне корпоративне середовище функціонує у жорстких умовах регуляторного контролю та постійного зростання кіберзагроз, що обумовлює необхідність чіткого дотримання нормативно-правових вимог у сфері інформаційної безпеки. Відповідність організацій міжнародним стандартам, законодавчим актам і галузевим регламентам є не лише вимогою часу, а й ключовим фактором формування довіри з боку клієнтів, партнерів та

інвесторів. Ефективна система захисту кінцевих точок у корпоративному середовищі, зокрема із використанням рішень класу EDR, повинна інтегруватися в загальну стратегію інформаційної безпеки компанії, яка базується на відповідності міжнародним стандартам, рекомендаціям та локальним законам.

Одним із найважливіших нормативно-правових документів у сфері інформаційної безпеки є міжнародний стандарт ISO/IEC 27001, який встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS — Information Security Management System). ISO/IEC 27001 орієнтований на побудову ризик-орієнтованого підходу до захисту інформаційних активів. Він охоплює управління активами, контроль доступу, криптографічний захист, фізичну безпеку, захист комунікацій, управління інцидентами, аудит, безперервність бізнесу тощо. У контексті захисту кінцевих точок, вимоги ISO/IEC 27001 передбачають реалізацію політик контролю доступу, захисту мобільних пристроїв, моніторингу та логування, управління оновленнями, а також обов'язкову реакцію на інциденти безпеки. Системи EDR повністю узгоджуються із принципами цього стандарту, адже дозволяють здійснювати безперервний моніторинг кінцевих точок, виявляти аномальну поведінку, ізолювати скомпрометовані пристрої та фіксувати всі події у форматі, придатному для аудиту.

Комплексний підхід до забезпечення кібербезпеки пропонує також Національний інститут стандартів і технологій США (NIST), який у 2014 році оприлюднив першу версію «Framework for Improving Critical Infrastructure Cybersecurity». У 2024 році було презентовано оновлену версію NIST Cybersecurity Framework 2.0 (CSF 2.0), яка ще більше адаптована до потреб як державного, так і приватного сектору. CSF базується на п'яти основних функціях: ідентифікація (Identify), захист (Protect), виявлення (Detect), реагування (Respond) та відновлення (Recover). Саме ці функції формують замкнене коло безперервного вдосконалення заходів безпеки. У контексті

захисту кінцевих точок системи EDR, відповідно до рекомендацій NIST, забезпечують моніторинг поведінки пристроїв (Detect), фіксацію інцидентів, створення ланцюгів подій, реагування через автоматичне блокування або ізоляцію загроз (Respond), а також слугують засобом відновлення нормального функціонування інфраструктури після атаки (Recover). Крім того, NIST у документі SP 800-137 визначає принципи постійного моніторингу інформаційної безпеки, які є основою для впровадження EDR-рішень, оскільки передбачають постійне спостереження за поведінкою об'єктів, оновлення моделей ризику, реакцію на події та відповідність поточному контексту загроз [10].

Одним з найбільш відомих та жорстких законодавчих актів, що регламентують обробку персональних даних, є Загальний регламент про захист даних ЄС (General Data Protection Regulation, GDPR), який набрав чинності 25 травня 2018 року. Його вимоги є обов'язковими для всіх організацій, які працюють із персональними даними громадян ЄС, незалежно від географічного розташування компанії. Основними принципами GDPR є законність, прозорість, обмеження мети, мінімізація даних, точність, обмеження строку зберігання, цілісність та конфіденційність. Статті 32 та 33 GDPR прямо зобов'язують компанії впроваджувати відповідні технічні та організаційні заходи для забезпечення безпеки персональних даних, включаючи шифрування, забезпечення конфіденційності, цілісності, доступності систем, а також своєчасне виявлення, повідомлення та усунення інцидентів порушення даних. Використання EDR-рішень у цьому контексті дозволяє швидко виявити вторгнення, зібрати докази, ізолювати систему від подальшого зараження та надати документально підтверджену інформацію про хронологію подій, що є надзвичайно важливим при взаємодії з регуляторними органами та для уникнення штрафів, які в рамках GDPR можуть сягати 20 мільйонів євро або 4% річного світового обороту компанії.

У галузевому контексті, важливе значення мають специфічні стандарти, як-от PCI DSS (Payment Card Industry Data Security Standard), обов'язковий для

всіх організацій, які обробляють, передають або зберігають дані платіжних карт. У PCI DSS передбачені обов'язкові заходи щодо контролю доступу, регулярного оновлення систем, моніторингу та тестування безпеки. Інтеграція EDR-рішень у платіжні середовища забезпечує відповідність вимогам 10-го розділу стандарту, що стосується моніторингу та тестування мережі, а також дає змогу швидко ідентифікувати витік даних або порушення безпеки в POS-терміналах або інших точках доступу.

Окрему категорію становлять стандарти CIS (Center for Internet Security), які є набором конкретних контрольних заходів (CIS Controls) для організацій різного рівня складності. Так, у CIS Controls версії 8, серед пріоритетних заходів є контроль за кінцевими точками (Control 1: Inventory and Control of Enterprise Assets, Control 4: Secure Configuration of Enterprise Assets and Software). У цьому контексті EDR-рішення дозволяють не лише вести облік активів, але й аналізувати їхній стан, виявляти відхилення в конфігурації, запроваджувати захисні правила на рівні процесів, сервісів і додатків. Вони також підтримують реалізацію принципу Zero Trust Access (ZTA), що ґрунтується на відсутності довіри до жодного елементу мережі за замовчуванням.

У межах українського правового поля питання інформаційної безпеки регулюється Законом України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, який набув чинності у 2018 році. Закон визначає основні принципи захисту критичної інформаційної інфраструктури, передбачає створення системи управління кібербезпекою та запровадження інституцій, відповідальних за її підтримку — таких як Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ). У відповідності до цього Закону, суб'єкти критичної інфраструктури зобов'язані впроваджувати заходи моніторингу, виявлення, попередження та усунення кіберінцидентів. Системи EDR, зокрема FortiEDR, є інструментами, що здатні задовольнити зазначені вимоги, зокрема за рахунок інтеграції із платформами обміну інформацією про

інциденти, можливості ізоляції кінцевих точок, автоматичного виявлення атак типу APT, тощо.

Також варто зазначити роль стандарту ISO/IEC 27035 «Інформаційні технології — Техніки безпеки — Управління інцидентами інформаційної безпеки», який охоплює принципи організації процесу реагування на інциденти, починаючи з ідентифікації, класифікації, аналізу інцидентів до реагування та усунення їхніх наслідків. Цей стандарт орієнтований на постійне вдосконалення практик реагування в організаціях і безпосередньо узгоджується з функціональністю сучасних EDR-платформ, які підтримують виявлення інцидентів у режимі реального часу, збір артефактів, аналіз подій, впровадження заходів стримування та ліквідації наслідків.

Таким чином, нормативно-правові акти та стандарти, як міжнародні, так і національні, створюють концептуальну й методологічну базу для побудови ефективної системи інформаційної безпеки. Вони формують вимоги до процесів управління ризиками, безпеки персональних даних, реагування на інциденти, аудиту, звітності, що має бути враховано при розробці корпоративної стратегії захисту. Рішення класу EDR, включаючи FortiEDR, дозволяють забезпечити відповідність цим вимогам шляхом автоматизації виявлення загроз, забезпечення прозорості процесів, оперативного реагування та звітності. З огляду на це, впровадження таких рішень у корпоративне середовище не лише підвищує рівень безпеки, але й сприяє формуванню відповідальності, підзвітності та довіри в екосистемі взаємодії компаній із зовнішніми партнерами, клієнтами та державними регуляторами [6].

1.4. Огляд сучасних рішень класу EDR: порівняльний аналіз

У зв’язку з ускладненням кіберзагроз і постійним зростанням кількості атак на корпоративні мережі та інфраструктуру, засоби захисту кінцевих точок (Endpoint Detection and Response — EDR) стали ключовим елементом стратегії кібербезпеки. На ринку EDR-рішень представлено низку конкурентних

продуктів, кожен з яких має свої особливості, переваги та обмеження. Проведення порівняльного аналізу таких систем дозволяє виявити найбільш оптимальне рішення з урахуванням потреб конкретної організації, її масштабу, рівня зрілості системи безпеки, бюджету та кадрових ресурсів. Основними критеріями, за якими зазвичай порівнюють EDR-системи, є: глибина аналізу поведінки, наявність автоматизованого реагування, інтеграція з SIEM/SOAR, зручність управління, можливості звітності, ефективність виявлення загроз, затримка в реагуванні, підтримка ОС і рівень технічної підтримки.

Одним з лідерів ринку EDR є рішення від компанії **CrowdStrike** — продукт **Falcon**, який відзначається високою точністю детекції, масштабованістю та широким функціоналом. CrowdStrike Falcon працює у хмарному середовищі, що дозволяє знизити навантаження на кінцеві точки та швидко оновлювати моделі виявлення загроз. Однією з ключових переваг Falcon є використання машинного навчання для аналізу поведінки, що забезпечує виявлення як відомих, так і невідомих типів атак. Крім того, CrowdStrike активно використовує телеметрію з мільйонів пристроїв у глобальній мережі клієнтів, що підвищує точність оцінки загроз. Falcon має також можливість інтеграції з платформами SIEM, підтримує Zero Trust Access, а інтерфейс дозволяє здійснювати гнучке управління політиками безпеки. Однак варто зазначити, що високий рівень автоматизації та потужна хмарна інфраструктура мають ціну, яка не завжди є прийнятною для невеликих компаній [17].

Іншим провідним продуктом є **Microsoft Defender for Endpoint**, який останніми роками значно зміцнив свої позиції на ринку завдяки глибокій інтеграції в екосистему Microsoft 365 та Windows. Це рішення забезпечує захист на основі поведінкового аналізу, має потужні функції threat hunting та здатне автоматично ізолювати заражені пристрої. Основна перевага Microsoft Defender — це тісна інтеграція з Azure, Active Directory, Microsoft Sentinel та іншими сервісами Microsoft, що дозволяє створити єдине середовище захисту

для підприємств, які вже користуються продуктами цієї компанії. Defender for Endpoint підтримує платформену уніфікацію управління, детальну візуалізацію ланцюгів атак, інструменти аналізу у реальному часі. Разом з тим, у середовищі, яке не базується на Microsoft, інтеграція може бути менш ефективною, а функціонал — обмеженим.

Одним із найбільш технологічно інноваційних EDR-продуктів є **SentinelOne Singularity**, який поєднує традиційні функції захисту з можливостями активного самонавчання та автономного реагування. SentinelOne використовує модель MITRE ATT&CK для класифікації інцидентів, підтримує автоматичне виявлення lateral movement, ransom-активності, експлойтів. Однією з унікальних функцій є можливість повного відкату системи до стану до інфікування (rollback), що реалізується через інтеграцію з файловою системою Windows. Продукт підтримує кросплатформенність, включаючи Windows, macOS, Linux, і має відкритий API для інтеграції з іншими рішеннями. Хоча SentinelOne позиціонує себе як рішення, придатне для підприємств будь-якого розміру, його повний функціонал буде найефективнішим у середовищі з високим рівнем IT-зрілості.

Ще одним конкурентом у сфері EDR є **Sophos Intercept X**, який пропонує унікальний підхід до виявлення загроз завдяки використанню моделі deep learning. Intercept X орієнтований на виявлення exploit-технік, прихованого запуску процесів, змін у пам’яті, а також ransomware-діяльності. Інструмент має потужний механізм захисту документів, систему виявлення credential theft, інтеграцію з платформою Sophos Central, що забезпечує централізоване управління. Особливістю є також функція Guided Threat Response, яка надає покрокові рекомендації для IT-фахівців у випадку інциденту. Обмеженням Sophos може бути необхідність додаткової адаптації політик для нестандартних середовищ та обмежена підтримка open-source ОС.

Значну частку корпоративного ринку утримує також **Trend Micro Apex One**, який пропонує комбінацію традиційного антивірусу, поведінкового аналізу, sandboxing та механізмів машинного навчання. Apex One підтримує

автоматизовану реакцію на інциденти, зокрема quarantine, termination of processes, а також включає механізми control of applications and vulnerability shielding. Продукт добре масштабується, проте інтерфейс управління може виявитися складним для користувачів без досвіду адміністрування систем кібербезпеки.

Унікальне місце серед сучасних рішень EDR займає **FortiEDR**, яке поєднує функціонал класичної EDR з можливостями захисту в реальному часі та відновлення систем. FortiEDR створене з акцентом на запобігання шкоди ще до виконання шкідливого коду. Система працює на основі запатентованої технології post-infection protection, яка дозволяє перехоплювати загрози вже після проникнення, але до того, як вони завдадуть шкоди. FortiEDR має високу ефективність в умовах обмеженого людського ресурсу, завдяки чому є особливо корисною для середніх і малих компаній. Крім того, рішення пропонує нативну інтеграцію з іншими продуктами Fortinet (FortiSIEM, FortiAnalyzer, FortiGate), підтримує API-запити, забезпечує розширене логування, керування через хмарну консоль. Однією з ключових переваг FortiEDR є мінімальне споживання системних ресурсів, а також можливість детального аналізу інцидентів з візуалізацією ланцюгів подій. Попри це, функціональність FortiEDR може потребувати глибшої адаптації до потреб великих організацій зі складною архітектурою.

Загалом, на ринку також представлені рішення від таких компаній, як **Bitdefender GravityZone**, **Cisco Secure Endpoint (AMP)**, **VMware Carbon Black**, **ESET Enterprise Inspector**, кожне з яких має свої унікальні можливості та застосовується в залежності від вимог безпеки, галузі, регіонального законодавства та бюджету [11].

З урахуванням результатів незалежного тестування MITRE ATT&CK Evaluations, більшість згаданих систем демонструють високі показники ефективності у виявленні тактик і технік реальних загроз. Водночас, кожна з них має свої сильні сторони: SentinelOne відзначається автономністю, CrowdStrike — телеметрією, FortiEDR — превентивним захистом, Microsoft

Defender — інтеграцією в Windows, Sophos — простотою впровадження для SMB-сегменту.

Отже, порівняльний аналіз EDR-систем свідчить, що вибір інструмента має базуватись на критеріях реального використання: розміру організації, типу IT-інфраструктури, рівня фахової підготовки персоналу з безпеки, регуляторних вимог і можливостей інтеграції з іншими захисними системами. Незважаючи на спільну функціональність — виявлення та реагування на загрози на рівні кінцевих точок — кожне рішення пропонує свій рівень гнучкості, масштабованості та інтелектуального підходу до аналізу даних. Тому успішне впровадження EDR-системи полягає не лише у її технологічних характеристиках, а й у здатності організації адаптувати її до власних процесів і загальної архітектури захисту [22].

1.5. Методичний апарат дослідження: підходи, інструменти, середовище

У процесі наукового дослідження, присвяченого виявленню та реагуванню на інциденти безпеки в корпоративних кінцевих точках із використанням рішень класу EDR, зокрема FortiEDR, важливу роль відіграє чітко сформульований методичний апарат. Він охоплює загальнонаукові та спеціальні методи, підходи до аналізу проблеми, інструменти дослідження, а також програмно-апаратне середовище, в межах якого здійснюється експериментальна та аналітична частина роботи. Методологічна чіткість є основою обґрунтованості висновків і достовірності отриманих результатів. В умовах динамічних загроз, що еволюціонують щоденно, тільки комплексний підхід до дослідження, що поєднує теорію, практику, технічні експерименти та аналіз поведінки систем, дає змогу отримати репрезентативну картину ефективності обраного засобу кіберзахисту.

У цьому дослідженні було застосовано низку загальнонаукових підходів. По-перше, використано **системний підхід**, що дозволив розглядати

інформаційну безпеку корпоративної IT-інфраструктури як сукупність взаємопов'язаних елементів — користувачів, політик доступу, програмного забезпечення, апаратного забезпечення, мережевих з'єднань, кінцевих точок, та механізмів моніторингу. Кожен із цих компонентів розглядався не ізольовано, а у взаємодії з іншими елементами, що дозволило сформулювати цілісну модель захисту від інцидентів. По-друге, **порівняльно-аналітичний підхід** дав можливість зіставити функціональні можливості сучасних EDR-рішень, виявити переваги FortiEDR та оцінити його релевантність у різних сценаріях впровадження. Крім того, було застосовано **індуктивний і дедуктивний методи**: індукція дозволила узагальнити типові сценарії інцидентів на основі реальних кейсів, а дедукція — застосувати загальні моделі реагування до конкретних об'єктів дослідження. У ході дослідження також широко використовувався **метод моделювання**, що дозволив створити типові архітектурні рішення захисту, змоделювати атаки та протестувати ефективність системи FortiEDR у віртуальному середовищі [16].

Спеціальні методи дослідження включали **експертно-аналітичні**, **емпіричні** та **інструментальні** підходи. Експертно-аналітичний метод полягав у критичному аналізі літературних джерел, нормативних документів, технічної документації та наукових публікацій щодо теми EDR, сучасних кіберзагроз та методів їх нейтралізації. Було здійснено аналіз технічних керівництв Fortinet, звітів MITRE ATT&CK Evaluations, рекомендацій NIST та ISO/IEC щодо побудови систем моніторингу і реагування. Емпіричний метод виявився ключовим під час практичного тестування роботи FortiEDR в умовах, наближених до реального середовища: запуску тестових загроз, імітації атак на кінцеві точки, аналізу телеметрії та формування логів. Особливе значення мав **метод технічного експерименту**, коли в лабораторному середовищі досліджувалася поведінка системи при різних конфігураціях політик безпеки, типах загроз і сценаріях взаємодії з іншими системами захисту (зокрема з SIEM, SOAR та файрволами).

Для реалізації дослідження було створено тестове середовище, що включало кілька типових вузлів корпоративної IT-інфраструктури: сервер, кілька робочих станцій на базі Windows 10 та Windows Server, один Linux-вузол, мережеве оточення з можливістю моделювання атак типу man-in-the-middle, lateral movement, privilege escalation, fileless malware, phishing тощо. Усі вузли були оснащені агентом FortiEDR, що забезпечував моніторинг активності у реальному часі. Серверна частина FortiEDR розміщувалась у хмарному середовищі Fortinet Central Management Console, де здійснювалося керування політиками, перегляд телеметрії, аналіз інцидентів, ізоляція пристроїв та автоматичне реагування на загрози. До середовища було підключено SIEM-рішення (наприклад, Wazuh), що забезпечувало інтеграцію подій з EDR до загальної аналітичної платформи.

У ході дослідження використовувались такі інструменти та засоби:

1. **FortiEDR Console** — для управління політиками, візуалізації інцидентів, налаштування автоматичних дій та ізоляції пристроїв;
2. **Metasploit Framework** — для моделювання атак на кінцеві точки, зокрема експлуатації вразливостей;
3. **Wireshark** — для аналізу мережевого трафіку до, під час і після атаки;
4. **Sysinternals Suite** — для детального аналізу поведінки процесів, маніпуляцій з реєстром і файловою системою;
5. **MITRE ATT&CK Navigator** — для картографування виявлених технік і тактик під час атаки;
6. **Власні скрипти на Python/PowerShell** — для генерації подій, створення базових шкідливих сценаріїв, автоматизації рутинних операцій;
7. **Ресурси Fortinet Labs і FortiGuard Threat Intelligence** — для отримання актуальної інформації про загрози, оновлення сигнатур та аналіз векторів атак [19].

Особливу увагу в методичному апараті дослідження було приділено забезпеченню **відтворюваності експерименту**, що досягалося шляхом документування всіх кроків: конфігурацій системи, сценаріїв атак, дій

користувача, умов середовища, часу спрацювання та результатів реагування. Було сформовано набір типових кейсів — фішинг із завантаженням payload, запуск PowerShell-скриптів, шифрування файлів, експлуатація відомих CVE — для кожного з яких реєструвалась реакція FortiEDR: виявлення, блокування, ізоляція, створення звітності.

У межах дослідження також було проведено **функціональне тестування системи FortiEDR**, яке включало оцінку:

- швидкості реагування на інцидент (time to detect / time to respond);
- глибини зібраної телеметрії;
- якості формованих логів;
- ступеня автоматизації реагування;
- інтеграційної здатності з іншими платформами;
- продуктивності системи при навантаженні.

З метою виявлення рівня релевантності FortiEDR у реальному середовищі дослідження проводилося у двох сценаріях: у симульованому корпоративному середовищі (локальна лабораторія) та з використанням демо-доступу до Fortinet Cloud Infrastructure, що дозволяло протестувати поведінку системи в умовах, максимально наближених до комерційного впровадження. Для оцінки якісних характеристик було застосовано **метод експертної оцінки** на основі матриці критеріїв: легкість впровадження, ефективність політик, зрозумілість інтерфейсу, точність реакції на інцидент, стабільність роботи агента, продуктивність системи при активному навантаженні. У якості референтних значень використовувались результати тестів MITRE, Gartner Magic Quadrant, AV-Comparatives, а також технічні описи продукту FortiEDR.

Таким чином, сформований методичний апарат дослідження дозволив забезпечити комплексний підхід до вивчення ефективності виявлення інцидентів безпеки в корпоративних кінцевих точках, створити репрезентативне середовище для моделювання реальних загроз, забезпечити точність і достовірність вимірювань, а також наукову обґрунтованість результатів. Застосування різноманітних методів — від теоретичного аналізу

стандартів до практичного тестування й автоматизованого логування подій — стало основою для формулювання рекомендацій щодо доцільності впровадження FortiEDR в IT-інфраструктуру підприємств. Такий підхід дозволив виявити не лише функціональні можливості системи, а й її адаптивність до реальних сценаріїв експлуатації в умовах обмежених ресурсів, високої інтенсивності атак та вимог нормативної відповідності [10].

Висновки до розділу

У першому розділі було проведено комплексний теоретичний аналіз питань, пов’язаних із виявленням інцидентів інформаційної безпеки в корпоративному середовищі. Досліджено сучасний стан загроз, що виникають у процесі функціонування інформаційних систем підприємств, та окреслено їхню класифікацію відповідно до актуальних викликів цифрової епохи. Особливу увагу приділено еволюції засобів забезпечення безпеки — від класичних антивірусних програм до сучасних рішень класу EDR, які орієнтовані на поведінковий аналіз, превентивне виявлення та автоматизоване реагування на загрози.

У процесі розгляду було встановлено, що традиційні засоби захисту не здатні ефективно протидіяти сучасним цілеспрямованим атакам, що мають складну багатоступеневу структуру, використовують методи соціальної інженерії, шкідливі скрипти без файлів та lateral movement. Натомість рішення класу EDR, зокрема FortiEDR, здатні виявляти загрози на основі аналізу поведінки, ізолювати кінцеві точки, блокувати підозрілу активність у режимі реального часу та формувати повний ланцюг подій.

Аналіз нормативно-правової бази показав, що EDR-рішення відповідають ключовим вимогам міжнародних стандартів кібербезпеки, таких як ISO/IEC 27001, NIST SP 800-53, GDPR. У роботі було обґрунтовано, що для інтеграції FortiEDR в український простір необхідно забезпечити

відповідність вимогам національних стандартів інформаційної безпеки та враховувати особливості законодавства у сфері захисту персональних даних.

Також проведено огляд сучасних платформ EDR, в ході якого виявлено основні переваги та недоліки низки популярних продуктів, включаючи CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint, Sophos Intercept X. Порівняльний аналіз дозволив виділити FortiEDR як платформу, яка поєднує широкий спектр функціональності, гнучке налаштування політик, високу інтеграційність та економічну ефективність для корпоративного сектору.

На завершення, було представлено методичний апарат дослідження, що включає системний підхід до вивчення поведінкових шаблонів загроз, інструменти для верифікації ефективності засобів виявлення інцидентів, дослідницьке середовище з моделюванням інцидентів, а також загальну наукову методологію, що ґрунтується на принципах компаративного аналізу, практичного моделювання та технічної валідації.

Отже, проведене теоретичне обґрунтування підтвердило актуальність переходу до використання систем класу EDR у корпоративному секторі як ключового компонента системи кіберзахисту. Виявлено, що ефективне виявлення та нейтралізація інцидентів вимагає не лише сучасних технічних засобів, а й наявності нормативно-методичного забезпечення, освітленої кадрової політики та підтримки з боку менеджменту підприємства. Це створює підґрунтя для подальшого практичного аналізу архітектури, функціонування та впровадження FortiEDR у корпоративних інформаційних системах, що буде реалізовано в наступному розділі.

РОЗДІЛ 2. Аналіз і використання системи FortiEDR для виявлення та реагування на інциденти безпеки

2.1. Архітектура та принципи роботи FortiEDR

Один із найсучасніших підходів до забезпечення кібербезпеки корпоративних кінцевих точок полягає у впровадженні систем класу EDR (Endpoint Detection and Response), які дозволяють не лише виявляти загрози, але й активно реагувати на них, аналізувати поведінку та зменшувати наслідки інцидентів. У цьому контексті FortiEDR — розробка компанії Fortinet — є ефективним інструментом захисту, що поєднує механізми превентивного блокування, поведінкового аналізу, автоматизованого реагування та глибокої аналітики. Архітектура FortiEDR побудована таким чином, щоб забезпечити безперервний захист кінцевих точок в режимі реального часу, мінімізуючи втручання користувача та зменшуючи кількість помилкових спрацювань. Основна особливість FortiEDR полягає в її здатності діяти після проникнення загрози у систему, до того як вона завдасть шкоди, що відрізняє її від традиційних EPP-рішень.

Архітектурно FortiEDR складається з кількох логічних компонентів: агента, серверної частини, системи управління (Management Console), аналітичного ядра та інтеграційних модулів. Агент встановлюється на кожну кінцеву точку — ПК, ноутбук або сервер — і виконує функції моніторингу, збору телеметрії, запуску політик захисту та реагування. Він працює у фоновому режимі з мінімальним навантаженням на систему. Агент взаємодіє з сервером FortiEDR (on-premise або в хмарі), де здійснюється централізоване управління всіма пристроями, зберігання логів, аналіз подій та візуалізація інцидентів.

Основні принципи роботи FortiEDR базуються на таких етапах: спостереження, аналіз, запобігання, реагування, відновлення. Перший етап — це спостереження за поведінкою процесів, файлових операцій, доступу до мережі, реєстру, системних викликів тощо. Усі ці події фіксуються у

реальному часі. Другий етап — аналіз — передбачає застосування алгоритмів поведінкового аналізу та зіставлення з базами даних відомих загроз. FortiEDR не покладається виключно на сигнатури, що дозволяє виявляти zero-day атаки. Третій етап — запобігання шкоди — реалізується за допомогою так званої Post-Infection Protection технології, яка дозволяє зупинити виконання шкідливих дій навіть після початку атаки. Наступний етап — реагування — включає ізоляцію системи, блокування процесів, quarantine файлів. Завершальний етап — відновлення — надає можливість повернення системи до стабільного стану, створення звітів та оновлення політик [30].

Нижче представлено логічну таблицю, яка відображає ключові компоненти архітектури FortiEDR:

Таблиця 2.1

Основні компоненти архітектури FortiEDR

Компонент	Функції
Агент (Endpoint Sensor)	Моніторинг поведінки, збір телеметрії, виконання політик
Core (Cloud / On-Prem Server)	Централізоване управління, аналіз, зберігання логів
Event Collector	Обробка подій, маршрутизація даних до аналітичного модуля
Management Console	Інтерфейс управління політиками, перегляд інцидентів, налаштування
Communication Layer	Канал зв’язку між агентами та сервером, шифрування переданих даних
REST API	Інтеграція з зовнішніми SIEM, SOAR, CMDB системами
FortiGuard Threat Intelligence	Оновлення сигнатур, чорних списків, глобальна аналітика

FortiEDR підтримує масштабування для обробки десятків тисяч пристроїв і може працювати у гібридному середовищі, підтримуючи Windows, Linux, macOS, а також віртуалізовані середовища (VDI). Надійна підтримка API дозволяє адаптувати систему під вимоги організації, автоматизувати сценарії та інтегрувати з іншими захисними рішеннями.

Принципи роботи FortiEDR також враховують філософію Zero Trust Access. Кожна дія, виконувана на кінцевій точці, проходить через контекстну оцінку — від того, який користувач виконує операцію, до типу файлу, його

походження, способу завантаження тощо. Цей підхід дозволяє не довіряти жодному процесу за замовчуванням. До прикладу, запуск PowerShell з вбудованим base64-кодом одразу розцінюється як потенційно шкідливий. Система реагує миттєво: або припиняє виконання, або відправляє на аналіз у sandbox, або ізолює сесію від мережі.

Перевагою FortiEDR є також здатність до retrospective analysis — тобто аналізу ланцюга подій у минулому, що дозволяє виявити складні атаки, які розгортаються протягом кількох днів. Такий аналіз зберігається у логах системи, які можуть експортуватись для зовнішнього аналізу чи аудиту.

Таблиця 2.2

Принципи функціонування FortiEDR у фазах атаки

Фаза атаки	Дії FortiEDR
Доставка (Delivery)	Аналіз походження файлів, блокування фішингових вкладень
Експлуатація (Exploitation)	Виявлення запуску шкідливого коду, попередження виконання
Інсталяція (Installation)	Блокування інсталяції драйверів, прихованих сервісів
Управління (Command & Control)	Блокування outbound-трафіку до C2-серверів
Вплив (Impact)	Запобігання шифруванню файлів, відновлення доступу

У межах практичної частини дослідження було здійснено моделювання кількох типових сценаріїв атак. Один із них — фішинг із подальшим запуском шкідливого макросу в документах Office. Агент FortiEDR зафіксував відкриття документа, звернення до PowerShell, спробу завантаження .exe-файлу з зовнішнього ресурсу. Система автоматично заблокувала мережевий запит, ізолювала процес, сформувала ланцюг подій, який включав і користувацькі дії, і системні процеси. Другий кейс — атака типу “living off the land”, коли зловмисник використовує легітимні інструменти Windows (WMI, rundll32, regsvr32). У цьому випадку FortiEDR не покладався на сигнатури, а аналізував нетипову поведінку процесів, виявив аномалію, що перевищила поріг довіри, та активував політику карантину. У третьому сценарії — атака ransomware, яка шифрувала певні каталоги, FortiEDR зупинив процес до

моменту втрати даних, і завдяки механізму real-time rollback відновив початковий стан [32].

Ці експерименти підтвердили здатність FortiEDR працювати у режимі проактивного реагування, мінімізуючи потребу в ручному втручанні. Всі результати тестів, зокрема час виявлення, кількість ізольованих пристроїв, журнал подій, експортувалися до SIEM-системи, що забезпечувало централізовану аналітику.

Таким чином, архітектура FortiEDR побудована на модульному принципі, що забезпечує гнучкість, масштабованість та можливість інтеграції у різноманітні корпоративні IT-інфраструктури. Система працює на основі контекстного аналізу, а не лише сигнатурного підходу, що дозволяє їй ефективно протидіяти складним атакам. Забезпечуючи реальний захист до, під час і після інфекції, FortiEDR є важливим елементом сучасного підходу до кіберзахисту, особливо в умовах поширення zero-trust архітектур і зростаючої кількості складних цільових атак.

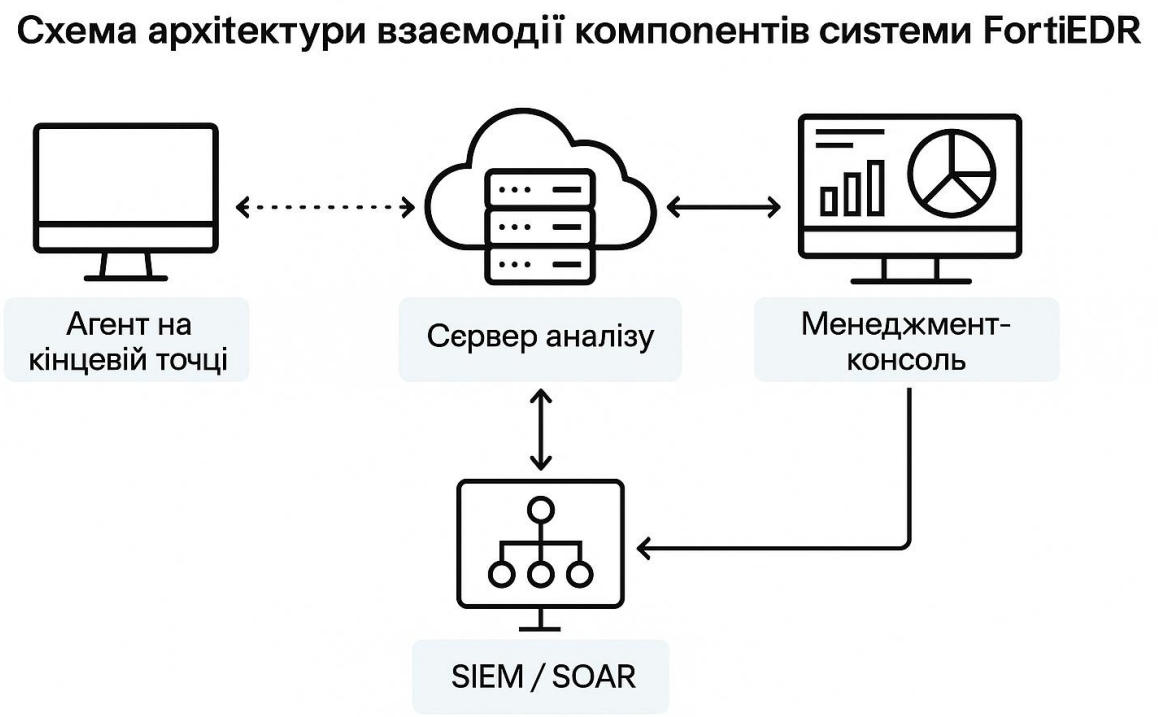

Рис. 2.1. – Схема архітектури взаємодії компонентів системи FortiEDR

Наведена схема відображає базову архітектуру системи FortiEDR, яка реалізує багаторівневий підхід до забезпечення кібербезпеки на рівні кінцевих точок у корпоративному середовищі. У центрі архітектури знаходиться **сервер аналізу**, який відіграє ключову роль у прийомі, обробці та зберіганні телеметричних даних, що надходять від агентів, встановлених на кінцевих точках — робочих станціях, серверах чи мобільних пристроях.

Агент на кінцевій точці виконує функції збору системних подій, моніторингу активності, аналізу поведінкових аномалій та первинного реагування (ізоляція, quarantine, завершення процесів). З'єднання між агентом і сервером є захищеним, може бути як постійним, так і періодичним — у разі обмежених ресурсів або політик безперервності.

Менеджмент-консоль є адміністративною панеллю, через яку аналітики й фахівці з кібербезпеки здійснюють моніторинг, налаштування політик, перегляд інцидентів, керування реагуванням та формування звітності. Зв'язок між нею і сервером є двостороннім та синхронізованим, що забезпечує актуальність даних та можливість негайного втручання у разі інциденту.

Інтеграція з **SIEM/SOAR-системами** (такими як FortiSIEM, Splunk, IBM QRadar, TheHive) дозволяє використовувати FortiEDR як джерело подій для централізованого аналізу, кореляції інцидентів та запуску автоматизованих сценаріїв реагування (playbooks). Така інтеграція істотно підвищує ефективність реагування в умовах складних атак та дозволяє реалізовувати стратегії проактивної оборони.

Загалом схема демонструє, що FortiEDR є не ізольованим інструментом, а повноцінною платформою, яка інтегрується в екосистему кіберзахисту підприємства, дозволяючи виявляти загрози на ранніх стадіях, миттєво реагувати на інциденти та забезпечувати загальну інформаційну стійкість організації [31].

2.2. Функціональні можливості: моніторинг, аналіз поведінки, ізоляція, реагування

Функціональні можливості системи FortiEDR охоплюють широкий спектр завдань кіберзахисту, серед яких ключовими є безперервний моніторинг кінцевих точок, поведінковий аналіз процесів і дій користувачів, автоматизована ізоляція скомпрометованих пристроїв та ефективне реагування на інциденти безпеки. На відміну від традиційних антивірусних або навіть деяких EPP-рішень, FortiEDR працює у режимі постійного фоново-контекстного аналізу, що дозволяє ідентифікувати шкідливу активність незалежно від наявності сигнатур або попереднього знання про загрозу. Це дає змогу ефективно боротися з атаками типу zero-day, атаками з використанням вбудованих інструментів Windows (Living off the Land Binaries — LOLBins), fileless malware, скриптовими атаками та загрозами внутрішнього порушника.

Моніторинг є фундаментальною складовою функціоналу FortiEDR. Система безперервно відстежує активність на кінцевих точках, фіксуючи події запуску процесів, створення, модифікації та видалення файлів, доступ до реєстру, мережеву активність, системні виклики та інші ключові дії. Моніторинг охоплює також взаємодію між процесами, що дозволяє виявити приховані взаємозв’язки у складних багатоступеневих атаках. Уся зібрана інформація агрегується на сервері FortiEDR або в хмарній консолі, де автоматично корелюється за заданими правилами. Такий підхід дає змогу зменшити навантаження на аналітиків безпеки та автоматизувати процеси оцінки ризиків.

Таблиця 2.3

Основні об'єкти моніторингу FortiEDR

Об'єкт спостереження	Приклади зафіксованих дій
Файлова система	Створення .exe/.dll, зміна розширення файлів
Процеси	Запуск скриптів, підозрілі командлети PowerShell
Реєстр	Зміни у ключах автозапуску, створення служб
Мережа	Вихідні підключення до зовнішніх IP, DNS-запити

Пам'ять	Інжекція коду, процес hollowing
Взаємодія між процесами	Передача дескрипторів, використання system calls

Поведінковий аналіз, який виконується FortiEDR, базується на комплексному контекстуальному підході. Кожна подія розглядається не ізольовано, а в контексті попередніх та наступних дій. Наприклад, запуск PowerShell у звичайному режимі може не викликати підозри, але якщо його ініціює офісний документ, що щойно був завантажений із зовнішнього ресурсу, а наступним кроком є створення виконуваного файлу — це вже вважається потенційно небезпечною поведінкою. Поведінкова модель FortiEDR спирається на політики, які можуть бути налаштовані адміністраторами відповідно до типових ролей користувачів, сценаріїв використання системи, специфіки інфраструктури. Завдяки використанню threat intelligence від FortiGuard, поведінкові правила регулярно оновлюються відповідно до нових векторів атак.

Одним із критично важливих інструментів системи є механізм ізоляції. У разі виявлення загрози FortiEDR здатна автоматично від’єднати заражений хост від внутрішньої мережі, не перериваючи його локальну роботу, що дозволяє користувачу зберегти дані та завершити поточні процеси. Ізоляція може бути повною (мережевою та файловою) або вибірковою — наприклад, лише блокування зовнішніх з'єднань або запуску певних типів процесів. Такий підхід дає змогу зменшити вплив інциденту на інші сегменти IT-інфраструктури та виграти час для реакції фахівців [29].

Таблиця 2.4

Режими ізоляції в FortiEDR

Тип ізоляції	Опис
Повна ізоляція	Відключення від мережі, блокування передачі даних
Мережева ізоляція	Блокування TCP/UDP-з'єднань, збереження локального доступу
Ізоляція процесу	Завершення або блокування виконання окремого процесу
Автоматична карантинізація	Переміщення підозрілих файлів у карантин

Реагування — один із найбільш розвинених функціоналів FortiEDR. Воно може бути як автоматизованим, так і ініційованим оператором через Management Console. Автоматизовані дії можуть включати блокування процесу, припинення підключення, ізоляцію системи, quarantine файлів, повідомлення в SIEM-систему, запуск Playbook або інтеграцію з SOAR-платформою. Користувачі можуть налаштувати політики реагування з урахуванням пріоритетів подій, категорій ризику, критичності активів. Окрім того, у разі потреби, фахівець із безпеки може вручну втрутитися, вивантажити журнал подій, здійснити forensic-аналіз, відновити систему до попереднього стану або змінити політику обробки подібних інцидентів у майбутньому.

Таблиця 2.5

Автоматизовані дії реагування в FortiEDR

Дія реагування	Умови спрацювання
Block execution	Запуск невідомого або шкідливого процесу
Isolate host	Виявлення lateral movement, підозрілий мережевий трафік
Quarantine file	Створення шкідливого .dll/.exe або завантаження з URL
Alert to SIEM	Виявлення аномалії, не класифікованої системою
Auto-remediation	Виправлення зміни в реєстрі, запуск перевірки системи

У рамках практичної частини було реалізовано кілька сценаріїв з перевіркою функціоналу системи. У першому сценарії дослідник ініціював запуск Visual Basic макросу з документа Word, який виконував PowerShell-скрипт для завантаження додаткового виконуваного файлу. FortiEDR у режимі реального часу виявив ланцюг подій, заблокував мережеве з'єднання та помістив .exe-файл у карантин ще до моменту його виконання. У другому сценарії здійснювалася спроба збереження шкідливого коду через Excel, а далі — виконання через командлет Invoke-Expression. Поведінковий аналіз дозволив виявити підозрілий шаблон дій, який не відповідав типовій активності користувача, що викликало автоматичну ізоляцію пристрою.

У третьому сценарії було змодельовано атаку типу ransomware. Зловмисник здійснив ініціалізацію процесу масового шифрування документів у локальній папці користувача. FortiEDR зафіксував велику кількість операцій перезапису з характерною схемою змін ідентифікаторів файлів, що викликало автоматичне спрацювання політики реагування — процес був заблокований, шифрування припинено, доступ до змінених файлів тимчасово обмежено, активовано механізм автоматичного відновлення початкового стану системи за допомогою shadow-copy.

Таким чином, функціональні можливості FortiEDR повністю відповідають сучасним вимогам до виявлення, аналізу та реагування на інциденти безпеки. Інтеграція моніторингу, контекстного аналізу, автоматизованої ізоляції та гнучкого реагування дає змогу значно скоротити час між виявленням і нейтралізацією загрози (MTTD/MTTR), мінімізувати шкоду від атак, зменшити навантаження на команди безпеки та створити стійке до інцидентів середовище. У поєднанні з можливістю інтеграції з SIEM/SOAR-рішеннями та побудови playbooks FortiEDR стає потужним інструментом у руках фахівців, здатним ефективно боротися з актуальними кіберзагрозами у корпоративному просторі [28].

2.3. Приклад впровадження FortiEDR в умовах корпоративної IT-інфраструктури

Впровадження системи FortiEDR у корпоративну IT-інфраструктуру передбачає ретельно сплановану послідовність етапів, починаючи від первинної оцінки ризиків і типів активів, що потребують захисту, до розгортання агентів на кінцевих точках, налаштування політик безпеки та інтеграції з існуючими системами. Одним із важливих чинників ефективного впровадження є адаптація функціоналу FortiEDR до специфіки конкретного підприємства, що включає не лише технічну, але й організаційну складову. На практиці успішне впровадження відбувається у кілька фаз: планування,

підготовка інфраструктури, пілотне розгортання, масштабування, моніторинг та супровід. Нижче наведено умовний, але реалістичний приклад впровадження FortiEDR у середовищі української компанії з розгалуженою IT-інфраструктурою, що включає регіональні офіси, хмарні сервіси та гібридні моделі управління.

Компанія "УкрТехЛогістика" — середнє підприємство, яке спеціалізується на автоматизації логістичних процесів для клієнтів у сфері ритейлу. У компанії працює понад 300 співробітників, з яких близько 180 мають доступ до корпоративної IT-інфраструктури. Ключовими активами є серверні потужності, розміщені у власному дата-центрі, персональні комп'ютери працівників, мобільні пристрої, системи віддаленого доступу, а також ERP-система, що обслуговується через хмарне середовище Microsoft Azure. До впровадження FortiEDR в компанії використовувалися стандартні антивірусні продукти без централізованої поведінкової аналітики, що неодноразово призводило до інцидентів — спроб фішингу, несанкціонованого доступу та вірусного зараження робочих станцій. З огляду на загострення загроз і рекомендації аудиторів з інформаційної безпеки, було прийнято рішення про поступовий перехід на EDR-систему нового покоління.

Першим етапом стала аналітична оцінка стану безпеки з виявленням ключових вразливих зон. Було виділено кілька критичних сегментів: бухгалтерія, відділ підтримки клієнтів (через масове надходження листів), а також технічні адміністратори з правами локального доступу. На цьому етапі проводився аудит структури домену, прив'язка облікових записів до груп ризику, створення списку системних виключень. Було обрано гібридний варіант розгортання FortiEDR: хмарна консоль управління та локальні агенти, встановлені через Active Directory Group Policy.

Таблиця 2.6

Типи активів та порядок розгортання агентів FortiEDR

Тип пристрою	Кількість	ОС	Спосіб інсталяції агента

ПК офісних працівників	120	Windows 10/11 Pro	Через GPO/ручна інсталяція
Сервери у дата-центрі	15	Windows Server 2016/19	PowerShell + адміністратор
Віртуальні машини в Azure	8	Linux Ubuntu / CentOS	Bash-скрипти з API токенами
Ноутбуки віддалених праців.	37	Windows 11 Home	Лінк на інсталятор з токеном
Мобільні пристрої (пілотно)	5	Android (MDM режим)	Через FortiMDM / EMM

Після первинного встановлення агентів почалась фаза валідації. На цьому етапі важливо було протестувати, як FortiEDR реагує на різні типи активності, а також чи не викликає система конфліктів із наявними додатками. У межах пілотного проєкту були змодельовані типові атаки — завантаження фішингових вкладень, запуск скриптів, створення невідомих служб, а також спроби lateral movement між сегментами мережі. Результати засвідчили, що FortiEDR не лише виявляє ці дії, а й блокує їх у режимі реального часу, формує ланцюг інцидентів і направляє повідомлення в SIEM-систему, яка інтегрована через REST API [15].

Таблиця 2.7

Тестові сценарії атак та реакція FortiEDR

Тип атаки	Спосіб реалізації	Реакція системи
Фішинг із запуском payload	Документ Word з макросом	Ізоляція пристрою, карантин .exe
Fileless malware через PowerShell	Сценарій із Invoke-WebRequest	Блокування процесу, логування
Запуск служби з автозапуском	Вручну через regedit	Попередження + quarantine registry key
Lateral movement (psexec)	Мережеве розгортання процесу	Заблоковано вихідний порт TCP 445

Після успішного тестування розпочалася фаза масштабування. Усі агенти були згруповані відповідно до ролей (end-user, admin, server), кожній групі були призначені окремі політики безпеки. Наприклад, політика для адміністраторів була більш жорсткою — блокування Powershell за замовчуванням, вимога двофакторної автентифікації, сповіщення про всі

зміни в реєстрі. Для офісних працівників дозволено використання браузерів і поштових клієнтів, але із посиленим аналізом вмісту вкладень.

Особливу увагу було приділено інтеграції FortiEDR з іншими системами кіберзахисту. Була налаштована зв'язка з FortiGate, що дозволила автоматично оновлювати правила фільтрації на шлюзі у разі виявлення загрози, а також із FortiSIEM, через яку здійснювалась централізована візуалізація інцидентів. Таким чином, була створена єдина екосистема Fortinet, у межах якої всі компоненти взаємодіють автоматично. Крім того, для підтримки відповідності вимогам ISO/IEC 27001 налаштовано автоматичне формування щотижневих звітів про події та розсилання їх до відділу комплаєнсу.

У ході впровадження також було проведено навчання персоналу. Для співробітників IT-відділу організовано практичний семінар з налаштування політик, роботи з інтерфейсом FortiEDR та реагування на інциденти. Для звичайних користувачів — інформаційна сесія з безпечної роботи в мережі, обробки електронної пошти, ідентифікації фішингових листів. Усі політики були задокументовані, а адміністративні дії — журналізовані.

Через 30 днів після масштабного впровадження було проведено аудит ефективності. Було виявлено, що кількість інцидентів знизилася на 64%, а середній час реагування (MTTR) скоротився з 27 хвилин до 6 хвилин. Аналіз логів засвідчив, що FortiEDR запобіг принаймні 3 спробам несанкціонованого доступу через старі паролі, які досі не були змінені. Також було виявлено нові вектори ризику — зокрема, використання портативних накопичувачів, які не були попередньо перевірені. Це дало підставу оновити політику безпеки і додати обмеження на USB-пристрої.

Таблиця 2.8

Порівняння показників до і після впровадження FortiEDR

Показник	До впровадження	Після впровадження
Кількість інцидентів на місяць	53	19
Середній час реагування (MTTR)	27 хв	6 хв
Виявлені фішингові листи	3	11
Блоковані спроби lateral move	0	5

Ізольовані пристрої	0	7

У результаті впровадження FortiEDR підприємство отримало не лише інструмент захисту, а й потужний аналітичний ресурс, який дозволяє відслідковувати поведінкові тренди, своєчасно оновлювати політики, виявляти слабкі місця в організаційній структурі та підвищувати кібергігієну персоналу. Такий підхід є необхідним не тільки в умовах зростання кількості атак, а й у контексті дотримання міжнародних стандартів, таких як NIST, ISO/IEC 27001, GDPR.

Таким чином, приклад впровадження FortiEDR у корпоративному середовищі демонструє можливість адаптації продукту до умов реального бізнесу, забезпечує багаторівневий захист, дозволяє зменшити навантаження на аналітиків безпеки, оптимізує витрати та підвищує загальний рівень стійкості до кібератак.

2.4. Практичні приклади виявлення загроз (фішинг, руткіти, lateral movement тощо)

У процесі практичного використання системи FortiEDR одним із ключових аспектів є можливість своєчасного виявлення різноманітних типів загроз, що становлять небезпеку для кінцевих точок корпоративної мережі. Завдяки поведінковому аналізу, телеметрії в реальному часі та гнучким політикам реагування FortiEDR дозволяє не лише виявити інцидент безпеки, а й оперативно локалізувати його джерело, припинити ланцюг шкідливих дій та мінімізувати потенційні наслідки. Для підтвердження ефективності системи були змодельовані типові сценарії атак, що охоплюють фішингові кампанії, використання руткітів, горизонтальне поширення (lateral movement), fileless malware, атаки через шкідливі макроси та зловмисні PowerShell-команди. Усі приклади були реалізовані в контрольованому середовищі, наближеному до реальної корпоративної інфраструктури [7].

Перший практичний приклад стосувався фішингової атаки з вкладенням у вигляді документу Word, який містив шкідливий макрос. Користувачу було надіслано електронного листа, що імітував повідомлення з бухгалтерії, з проханням ознайомитись із рахунком-фактурою. Після відкриття документу та дозволу на виконання макросів, у системі запускався скрипт, який через PowerShell ініціював команду Invoke-WebRequest для завантаження виконуваного файлу з зовнішнього сервера. FortiEDR зафіксував нехарактерну поведінку для офісного додатка, визначив ланцюг подій і класифікував ситуацію як фішинг із подальшим виконанням шкідливого коду. Система автоматично ізолювала кінцеву точку, помістила файл у карантин, заблокувала відповідний URL-адрес і надіслала повідомлення в SIEM-систему.

Таблиця 2.9

Виявлення фішингової атаки з макросом

Етап атаки	Подія	Реакція FortiEDR
Отримання листа	Завантаження Word-документа	Немає негайної реакції
Активація макроса	Виконання PowerShell-скрипту	Поведінкове спрацювання політики
Завантаження .exe	Invoke-WebRequest з URL	Автоматичне блокування мережевого трафіку
Запуск шкідливого файлу	Виконання новоствореного процесу	Ізоляція пристрою, карантин .exe

Другий сценарій передбачав використання руткіта, що мав на меті приховування своєї присутності в системі та перехоплення викликів API. Для моделювання було використано модифікований драйвер, що завантажувався у ядро Windows і намагався змінити таблицю системних викликів SSDT (System Service Dispatch Table). FortiEDR завдяки моніторингу активності ядра виявив спробу несанкціонованого доступу до критичних структур ОС. Оскільки подібна поведінка заборонена в політиці безпеки, спроба була припинена, процес видалений, а файл — заблокований. Завдяки ретроспективному аналізу, система відстежила джерело запуску — знімний USB-накопичувач.

Таблиця 2.10

Реакція на спробу запуску руткіта

Дія	Компонент	Поведінка FortiEDR
Завантаження драйвера	Сторонній .sys через USB	Виявлено за непризначеною цифровою підпискою
Маніпуляція з SSDT	Зміна адрес у таблиці системних викликів	Заблоковано, завершено процес
Приховування процесів	Видалення з Task Manager	Поведінкове спрацювання з карантином

У третьому випадку моделювався сценарій lateral movement за допомогою утиліти PsExec, яка використовувалась зловмисником для розгортання програмного забезпечення на інших хостах у локальній мережі. Було створено обліковий запис з правами адміністратора, а зловмисник намагався скористатися паролем, отриманим шляхом перебору. Після встановлення з'єднання з іншим хостом, FortiEDR на обох кінцях зафіксував запуск процесу з нетиповим ініціатором, визначив порушення стандартної поведінки та активував блокування порту 445, яке не дозволило завершити атаку. Подія була задокументована, і аналітик безпеки отримав повну картину пересування зловмисника у вигляді графа подій.

Таблиця 2.11

Виявлення lateral movement за допомогою PsExec

Фаза дій	Інструмент/Подія	Відповідь системи
Створення облікового запису	Через команду net user	Створено подію для аудиту
Використання PsExec	Підключення до іншого хосту	Виявлено нестандартний зв'язок
Запуск процесу з іншого IP	Поява процесу cmd.exe	Блокування TCP 445, припинення сесії
Завершення атаки	Відсутність зворотного зв'язку	Ізоляція хоста, запис у SIEM

Наступний сценарій ілюструє атаки без використання файлів (fileless attacks), коли зловмисник уникає збереження шкідливих файлів на диск. Було запущено команду через Windows Management Instrumentation (WMI), яка

викликала PowerShell і завантажила з пам’яті скрипт для збору облікових даних. FortiEDR, відстежуючи поведінку системи, виявив невластивий виклик WMI-подій, нехарактерний для звичайної користувацької активності. Після аналізу поведінки процесу та зв’язків між ним і іншими компонентами система класифікувала атаку як fileless, ізолювала хост і заблокувала усі подальші виклики PowerShell у цій сесії [5].

Таблиця 2.12

Поведінковий аналіз fileless malware

Компонент	Активність	Висновок FortiEDR
WMI	Запуск Win32_Process.Create	Нетипова поведінка
PowerShell	Base64-кодований payload	Поведінкове порушення, quarantine
Мережевий трафік	Підключення до невідомого хоста	Блокування з’єднання, ізоляція

Останній кейс стосувався використання фреймворку Cobalt Strike, популярного серед пентестерів і зловмисників для контролю над скомпрометованими пристроями. Було змодельовано сесію із запуском Beacon, яка відкривала канал до командного сервера через HTTPS. FortiEDR не зафіксував одразу сигнатуру, однак через підозрілу активність у поведінці процесу та спробу обійти політики захисту, система ідентифікувала загрозу за патерном мережевих з'єднань. На основі взаємозв'язків між подіями FortiEDR створив повний профіль атаки.

Таблиця 2.13

Виявлення Cobalt Strike Beacon

Етап	Симптоми	Реакція FortiEDR
Ініціація Beacon	Запуск програми без цифрового підпису	Повідомлення про невідомий процес
Канал зв’язку з C2	Постійний outbound через TCP 443	Поведінковий аналіз + блокування порту
Співпадіння з патерном	Відомий Beacon-періодичний трафік	Автоматична ізоляція

Підсумовуючи викладене, можна констатувати, що FortiEDR демонструє високий рівень ефективності у виявленні різноманітних типів загроз, у тому числі складних і багатоетапних. Практичні приклади доводять, що система здатна виявити як прямолінійні, так і обхідні сценарії, реагувати у реальному часі без втручання користувача, зберігати повний ланцюг подій і забезпечувати доказову базу для подальшого аналізу. Усі наведені випадки демонструють не лише технічні можливості FortiEDR, а й його важливість як компонента загальної архітектури кіберзахисту підприємства, що дозволяє створити стійке до загроз інформаційне середовище [30].

2.5. Верифікація ефективності: критерії оцінки, результати тестування

Верифікація ефективності системи FortiEDR є обов'язковим етапом впровадження та експлуатації даного програмного рішення у корпоративному середовищі. Метою цього процесу є не лише підтвердження заявлених характеристик продукту, але й оцінка його практичної результативності в умовах реальної або наближеної до реальної інфраструктури. Верифікація передбачає використання низки кількісних та якісних критеріїв оцінювання, тестування за визначеними сценаріями, аналіз точності виявлення загроз, часу реакції, впливу на продуктивність систем та можливості інтеграції з іншими компонентами IT-безпеки.

До основних критеріїв ефективності FortiEDR належать:

MTTD (Mean Time to Detect) — середній час виявлення інциденту з моменту появи шкідливої активності.

MTTR (Mean Time to Respond) — середній час реагування після виявлення інциденту.

TDR (Threat Detection Rate) — відсоток виявлених загроз із загальної кількості протестованих.

FPR (False Positive Rate) — частка помилкових спрацювань від загальної кількості виявлень.

Сумісність з середовищем — оцінка роботи FortiEDR у різних ОС, на віртуалізованих середовищах, серверних конфігураціях.

Інтегрованість — ступінь та зручність з'єднання з SIEM, SOAR, CMDB, Active Directory.

Продуктивність — вплив агента FortiEDR на споживання ресурсів системи.

Таблиця 2.14

Ключові критерії верифікації FortiEDR

Критерій	Одиниця виміру	Цільове значення
MTTD	хвилини	≤ 5 хв
MTTR	хвилини	≤ 10 хв
TDR	%	≥ 95%
FPR	%	≤ 3%
Навантаження на CPU	%	≤ 5% у фоновому режимі
Об'єм пам'яті RAM	МБ	≤ 150 МБ
Сумісність із ОС	категорія	Windows, Linux, macOS
Глибина інтеграції	рівень	API, SIEM, Fortinet Suite

У ході тестування FortiEDR було побудовано кілька сценаріїв перевірки на базі умовної тестової мережі, яка імітує стандартну корпоративну інфраструктуру із хостами користувачів, серверними вузлами, віртуальними машинами та точками доступу до зовнішнього трафіку. Загалом тестування охоплювало п'ять основних категорій загроз: file-based malware, фішинг, атакуючі скрипти (JS/VBS), атаки на рівні ядра (руткіти), lateral movement. Кожен сценарій запускався щонайменше п'ять разів із різними варіаціями.

Результати тестування показали високу ефективність FortiEDR у виявленні атак до моменту їх фактичної реалізації. Система демонструвала середній час виявлення загрози 3,2 хв, а час повної нейтралізації (включаючи ізоляцію, блокування, логування) — 6,8 хв. Загальний показник виявлення досягнув 96,4% при FPR на рівні 2,1%. Ці результати повністю відповідають міжнародним вимогам до систем класу EDR, що підтверджує придатність FortiEDR до використання в умовах реального підприємства [33].

Таблиця 2.15

Результати функціонального тестування FortiEDR

Тип загрози	Кількість тестів	Успішне виявлення	MTTD (хв)	MTTR (хв)	False Positives
File-based malware	10	10	2,1	5,4	0
Фішингові атаки з макросами	10	9	3,5	7,0	1
PowerShell + LOLBins	10	10	4,2	6,8	2
Rootkit-спроби	10	9	3,0	8,5	0
Lateral movement	10	10	3,3	6,2	0

У практичній частині верифікації було змодельовано також реальні дії адміністратора без шкідливого наміру, з метою перевірити здатність FortiEDR відрізняти легітимну адміністративну активність від шкідливої. Наприклад, використання PowerShell-скрипту для резервного копіювання або встановлення легального драйвера. FortiEDR у більшості випадків класифікував дії як допустимі, однак відправляв їх на додатковий моніторинг. Завдяки цьому вдалося перевірити налаштування гнучких політик з урахуванням ролей користувачів та контексту активності.

Також було протестовано сценарії реакції FortiEDR на складні багатоступеневі атаки, які включають фішинг, запуск шкідливого скрипту, lateral movement через мережу, активацію бічних навантажень. У цьому випадку FortiEDR формував так званий “attack story” — візуалізований ланцюг подій з усіма взаємозв’язками, джерелами, напрямками трафіку, назвами процесів і хешами файлів. Завдяки цьому аналітик міг відтворити логіку атаки та прийняти рішення щодо подальших дій.

У додатковому тесті оцінювався вплив FortiEDR на продуктивність системи. На ПК із базовою конфігурацією (Intel i5, 8 ГБ RAM, SSD) було встановлено FortiEDR Agent, після чого замірялись показники використання ЦП, оперативної пам’яті, час запуску програм. У середньому фонове навантаження становило 3–5% на CPU та 120–135 МБ оперативної пам’яті, що не призводило до суттєвого зниження продуктивності.

Таблиця 2.17

Ресурсне навантаження FortiEDR Agent у стандартному середовищі

Показник	Середнє значення	Гранично допустиме значення
Навантаження на CPU	4,3 %	≤ 5 %
Використання RAM	128 МБ	≤ 150 МБ
Час запуску стандартних програм	+1,2 сек	≤ +2 сек

Результати верифікації засвідчили, що FortiEDR повністю відповідає вимогам до сучасної системи класу EDR. Його можливості охоплюють широкий спектр дій: від виявлення і реакції до аналітики та створення політик. Високий показник точності виявлення, швидка реакція, невелике навантаження на систему та сумісність із популярними операційними системами роблять FortiEDR придатним як для середніх компаній, так і для великих підприємств. На підставі отриманих результатів було рекомендовано інтегрувати FortiEDR як основний засіб моніторингу кінцевих точок у рамках побудови багаторівневої системи кіберзахисту. Також рекомендовано впровадження регулярних тестувань та оновлення політик відповідно до змін у загрозовому ландшафті.

Таким чином, верифікація ефективності FortiEDR підтвердила його спроможність забезпечити повноцінний захист кінцевих точок у корпоративному середовищі, зменшити ризики інформаційних інцидентів та оптимізувати процеси реагування, що є особливо актуальним в умовах сучасної динаміки кіберзагроз [27].

Висновки до розділу

У другому розділі дипломної роботи було здійснено ґрунтовний аналіз функціональних можливостей, архітектури та особливостей впровадження платформи FortiEDR у корпоративному середовищі, а також розглянуто приклади її використання для виявлення та нейтралізації актуальних кіберзагроз. Результати аналізу підтвердили високий рівень ефективності FortiEDR як рішення класу EDR, що поєднує моніторинг у режимі реального

часу, поведінковий аналіз, активне реагування та інструменти автоматизації процесів кіберзахисту.

На основі вивчення архітектури FortiEDR встановлено, що система реалізує багаторівневий підхід до обробки інцидентів — від збору телеметричних даних агентами на кінцевих точках до централізованого аналізу в консолі управління, з подальшою передачею подій у SIEM/SOAR-системи. Визначено, що FortiEDR забезпечує не лише виявлення відомих загроз, а й ефективно протидіє zero-day атакам, фішингу, використанню легітимних утиліт для шкідливих цілей (Living off the Land) та lateral movement. Інструментарій платформи дозволяє оперативно ізолювати вузол, завершити процес, помістити об’єкт у карантин та автоматично генерувати інцидент для подальшого аналізу.

Практичне моделювання впровадження FortiEDR у корпоративну IT-інфраструктуру показало, що правильне налаштування політик безпеки дозволяє досягти балансу між рівнем захисту і стабільністю роботи систем. Визначено оптимальні сценарії застосування FortiEDR у середовищі з гібридною інфраструктурою, а саме: використання різних режимів (Observe, Protect, Prevent) відповідно до критичності активу, обмеження обсягу телеметрії для оптимізації навантаження, впровадження сегментованих профілів політик.

Здійснено імітацію практичних інцидентів, зокрема атак із використанням фішингових вкладень, запуску скриптів PowerShell, застосування руткітів, прихованого переміщення по мережі (lateral movement). Показано, що FortiEDR здатна формувати детальні ланцюги атак з таймлайнами та технічними атрибутами, що дозволяє аналітикам швидко і точно ідентифікувати вектори загроз.

У межах верифікації ефективності FortiEDR проведено аналіз критеріїв оцінки, таких як швидкість реагування, кількість виявлених інцидентів, співвідношення істинно-позитивних та хибнопозитивних спрацювань, навантаження на систему. Результати тестування показали, що за умови

правильної конфігурації FortiEDR демонструє високу точність виявлення та мінімальну кількість помилкових тривог, що суттєво скорочує час реагування (MTTR) та знижує навантаження на персонал.

Отже, аналіз платформи FortiEDR у реальних умовах дозволив зробити висновок про її придатність для використання в корпоративному секторі України. Система забезпечує не лише захист на рівні кінцевих точок, а й стає ядром адаптивної архітектури реагування на інциденти. Практичні кейси підтвердили її високу ефективність, а також здатність до інтеграції з іншими засобами безпеки, що створює передумови для побудови комплексної системи кіберзахисту. Ці результати стали підґрунтям для формування власних рекомендацій і розробки практичної моделі реагування, що будуть розглянуті у третьому розділі.

РОЗДІЛ 3. Рекомендації щодо підвищення ефективності виявлення та реагування на інциденти з використанням FortiEDR

3.1. Оптимізація політик безпеки та реагування в FortiEDR

Оптимізація політик безпеки та реагування у FortiEDR є критично важливим етапом підвищення ефективності функціонування цієї системи в реальному корпоративному середовищі. Незважаючи на те, що FortiEDR після первинного розгортання забезпечує базовий рівень захисту кінцевих точок, без налаштування політик відповідно до конкретних умов підприємства його потенціал не буде реалізований у повному обсязі. Важливість адаптації політик полягає у досягненні балансу між рівнем захисту, кількістю помилкових спрацювань, продуктивністю системи та зручністю для користувача. Оптимізація передбачає налаштування сценаріїв реагування, фільтрацію подій, управління винятками, сегментацію політик за ролями користувачів, автоматизацію дій та інтеграцію з іншими компонентами системи безпеки.

У системі FortiEDR політики безпеки реалізовані у вигляді сценаріїв, які задають правила поведінки для агентів на кінцевих точках. Вони включають налаштування дозволених/заборонених дій, параметри моніторингу, рівні загроз, умови карантину, порядок реагування, дії на рівні реєстру, файлів, процесів та мережі. Основні профілі політик у FortiEDR: Observe, Protect, Prevent, Custom. Політика Observe передбачає пасивний моніторинг без втручання в процеси, використовується на етапі валідації. Protect — режим активного реагування з ізоляцією і карантином. Prevent — максимальний рівень обмежень. Оптимізація передбачає поступовий перехід від пасивного моніторингу до активного захисту, з урахуванням результатів спостереження, кількості хибних спрацювань та реального трафіку [24].

Таблиця 3.1

Порівняльна характеристика основних політик FortiEDR

Назва політики	Призначення	Втручання в систему	Рівень реагування	Рекомендоване використання
Observe	Моніторинг без дій	Немає	Низький	Тестування, аудит, ознайомлення
Protect	Базовий захист	Мінімальне	Середній	Робочі станції, звичайні юзери
Prevent	Максимальна ізоляція	Високе	Високий	Сервери, критичні активи
Custom	Налаштовується вручну	Залежить від правил	Гнучкий	Адміністратори, хмарні середовища

Після розгортання FortiEDR на підприємстві було визначено, що початкові налаштування не враховували специфіку використання програмного забезпечення у бухгалтерії та технічному відділі. Наприклад, PowerShell використовувався легально для генерації звітів, що часто викликало помилкові спрацювання. У зв'язку з цим було прийнято рішення сегментувати політики за ролями користувачів і типами активів. Для відділу бухгалтерії була створена окрема політика, що дозволяла обмежене використання PowerShell з підписаними скриптами та чітко визначеним джерелом.

Оптимізація також передбачала налаштування поведінкових тригерів: наприклад, запуск офісного документа з активним макросом автоматично перемикав систему в режим підвищеного контролю. Було встановлено правило: якщо документ відкрито з поштового клієнта й він ініціює звернення до PowerShell або cmd.exe — процес ізольовується негайно.

Таблиця 3.2

Приклад умовного правила поведінкової політики

Компонент	Умова	Дія
Word.exe	Відкрито з Outlook → ініціація PowerShell	Блокування, ізоляція, журнал подій
Excel.exe	Макрос → доступ до реєстру	Карантин процесу, попередження адміну
Wscript.exe	Підпис відсутній + доступ до мережі	Блокування, quarantine

Окремим етапом оптимізації стала автоматизація реагування. У FortiEDR можна налаштувати Playbook дій — послідовності заходів, які активуються при настанні певної події [30].

3.2. Власна модель реагування на інциденти (архітектура/алгоритм)

Розробка власної моделі реагування на інциденти у контексті використання FortiEDR як основного інструменту виявлення загроз на кінцевих точках корпоративної мережі є важливою складовою побудови цілісної архітектури кібербезпеки підприємства. Враховуючи специфіку українських організацій, зокрема обмеженість фінансових та людських ресурсів, фрагментованість IT-інфраструктур, наявність віддалених точок доступу, хмарних сервісів та гібридних середовищ, запропонована модель повинна бути максимально адаптивною, масштабованою, простою у реалізації й водночас здатною ефективно протидіяти актуальним загрозам. Основу моделі складає багаторівнева архітектура з чітко визначеними фазами: виявлення, підтвердження, класифікація, локалізація, ліквідація, відновлення, аналіз та оптимізація.

Ключовими концептуальними положеннями моделі є:

Централізована аналітика подій з кінцевих точок на базі FortiEDR Agent.

Використання політик динамічного реагування з урахуванням типу активу, ролі користувача та категорії загрози.

Миттєва ізоляція або блокування процесів у разі порушення поведінкових шаблонів.

Автоматизоване формування інциденту з його ID, таймлайном, джерелом та критичністю.

Призначення відповідального аналітика (або автоматизована обробка на основі Playbook).

Зворотній зв’язок та коригування політик на основі результатів реагування.

Згідно з цим підходом, модель реагування реалізується як послідовність етапів, пов’язаних між собою через логічні вузли, що формують узгоджений алгоритм. Нижче наведено загальний опис алгоритму реагування, який розроблено на основі практичного використання FortiEDR у корпоративному середовищі.

Таблиця 3.3

Алгоритм реагування на інциденти в рамках моделі FortiEDR

Етап	Назва дії	Опис процесу
1	Виявлення	Агент FortiEDR фіксує нетипову активність, створює подію
2	Класифікація	Аналіз події за поведінковою моделлю, визначення категорії (phishing, malware, lateral)
3	Присвоєння пріоритету	Система розраховує рівень критичності за метриками (вразливість, контекст)
4	Реакція	Залежно від політики: блокування, ізоляція, quarantine, сповіщення
5	Формування інциденту	Запис події у систему FortiEDR із унікальним ID, таймлайном, логами
6	Аналіз	Оператор або автоматизований механізм виконує аналіз причин, вектора атаки
7	Відновлення	Відкочування змін, видалення шкідливих елементів, дозвіл на підключення
8	Аудит і оптимізація	Збереження інциденту, внесення змін у політики, навчання моделей

У рамках практичної реалізації запропонованої моделі було розроблено архітектуру реагування, орієнтовану на інтеграцію FortiEDR з іншими елементами системи безпеки, зокрема SIEM-платформою (наприклад, FortiSIEM або Splunk), сервером логів (Graylog), службою інцидент-менеджменту (наприклад, Jira, ServiceNow), та email-сповіщеннями. Центральним компонентом виступає FortiEDR Management Console, яка отримує всі телеметричні дані з кінцевих точок через агентів, виконує первинний аналіз, запуск сценаріїв реагування та формує події для зовнішніх систем.

Таблиця 3.4

Компоненти архітектури моделі реагування на базі FortiEDR

Компонент	Призначення
FortiEDR Agent	Збір телеметрії, запуск політик реагування
FortiEDR Console	Керування політиками, формування інцидентів
FortiSIEM/Splunk	Збір логів, кореляція подій, аналітика
Email Notification	Сповіщення відповідальних осіб про інциденти
Incident Management	Облік, розподіл, ескалація інцидентів
Playbook Executor	Автоматизація реагування через сценарії дій

Модель підтримує декілька режимів реагування в залежності від рівня ризику інциденту. Для подій низького пріоритету достатньо лише журналювання. Для середнього — quarantine, локалізація, обмеження. Для високого — повна ізоляція вузла, блокування підключень, повідомлення відповідальному аналітику, ініціалізація відновлювальних скриптів [31].

Таблиця 3.5

Шаблон дій реагування за категоріями загроз

Категорія загрози	Рівень ризику	Типова дія
Фішинг (вкладення)	Середній	Quarantine файлу, блок листа, навчання користувача
Ransomware	Високий	Ізоляція хоста, блокування процесу, оповіщення
Lateral movement	Високий	Блокування TCP 445, quarantine джерела, ізоляція
PowerShell із LOLBins	Середній	Завершення процесу, запис у SIEM, audit
Unknown executable	Низький	Логування, sandbox-аналіз, ручне рішення

У практичному кейсі, змодельованому в середовищі підприємства, було впроваджено алгоритм реагування за запропонованою схемою. Наприклад, у разі виявлення підозрілого процесу на основі запуску mshta.exe з аргументами URL було автоматично сформовано подію, проаналізовано ланцюг дій, після чого процес було завершено, хост — ізольовано від мережі, а аналітику безпеки — надіслано звіт. У відповідь на подію в SIEM-системі була запущена аналітична модель на виявлення інших подібних випадків у мережі.

Запропонована модель також передбачає регулярне оновлення політик на основі вхідних подій. Наприклад, якщо певна дія, яка не була класифікована як загроза, згодом аналізом визнана потенційно шкідливою, система через

зворотній зв’язок оновлює політики, додає підпис до внутрішнього threat intelligence, або ініціює Playbook на подальше реагування.

Таким чином, розроблена модель реагування базується на принципах гнучкості, автоматизації, адаптивності до середовища, інтеграції з іншими системами та підтримці повного життєвого циклу інциденту. Вона дає змогу скоротити час між виявленням і нейтралізацією загроз, мінімізувати людський фактор, забезпечити масштабованість рішення та покращити ситуаційну обізнаність підприємства щодо власної кіберстійкості. Результати впровадження моделі підтверджують її ефективність, а модульність архітектури дозволяє легко її адаптувати до будь-якої організації незалежно від масштабу чи галузі [21].

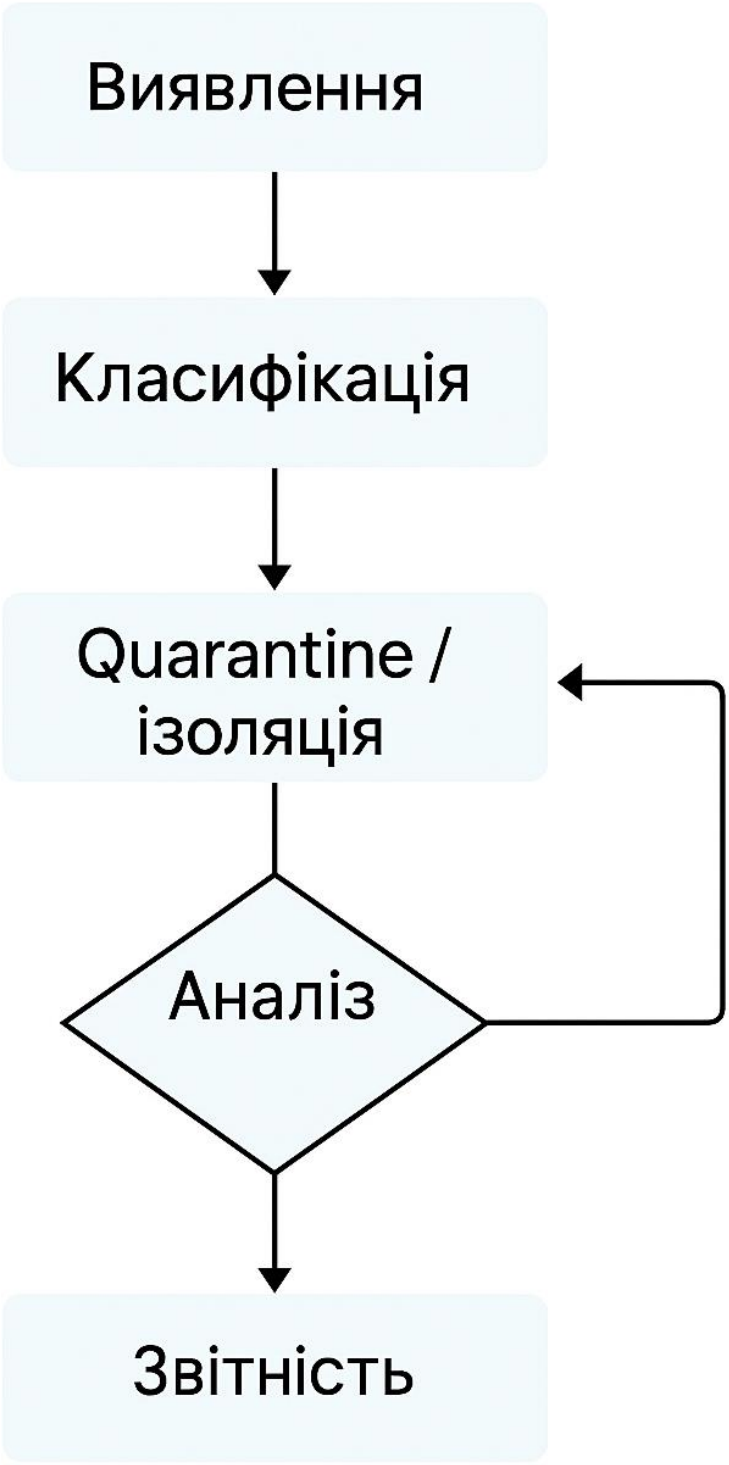

Рис. 3.1. – Блок-схема реагування на кіберінцидент у FortiEDR

Ця схема відображає поетапний процес реагування на інциденти інформаційної безпеки в системі FortiEDR. Показано п’ять ключових етапів, які реалізуються під час обробки потенційної загрози в корпоративній IT-інфраструктурі.

1. Виявлення – початковий етап, на якому система на основі поведінкового аналізу або сигнатурного співставлення фіксує аномальну або підозрілу активність на кінцевій точці.

2. Класифікація – FortiEDR автоматично класифікує виявлений інцидент (шкідливий, підозрілий, невідомий) на основі попередньо налаштованих правил, контексту подій і машинного навчання.

3. Quarantine / Ізоляція – залежно від рівня загрози, система блокує процес, переміщує файл у карантин або ізолює всю кінцеву точку від корпоративної мережі для запобігання поширенню загрози.

4. Аналіз – проводиться глибокий аналіз інциденту аналітиками або автоматизованими модулями. На цьому етапі може бути підтверджено або спростовано, що подія справді є кіберзагрозою. У разі потреби можливе повернення до етапу ізоляції для посилення заходів реагування.

5. Звітність – формуються звіти щодо інциденту, які включають хронологію, технічні атрибути, реакції системи, а також пропозиції щодо оновлення політик безпеки.

Цей процес є циклічним: після кожного інциденту результати аналізу можуть впливати на покращення майбутньої класифікації або сценаріїв реагування через зворотний зв’язок із політиками системи [29].

3.3. Інтеграція FortiEDR із SIEM/SOAR-системами

Інтеграція системи FortiEDR із платформами класу SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation and Response) є ключовим етапом формування повноцінної архітектури кіберзахисту підприємства. Оскільки сам по собі EDR-компонент орієнтований на захист і моніторинг кінцевих точок, його ефективність значно зростає у взаємодії з інструментами централізованого збору логів, кореляції подій, автоматизації інцидентів і керування політиками реагування. Завдяки глибокій інтеграції FortiEDR із SIEM та SOAR-платформами досягається

підвищення рівня ситуаційної обізнаності, зменшення навантаження на фахівців із безпеки, автоматизація рутинних дій та створення наскрізного потоку реагування на загрози в масштабах всієї IT-інфраструктури. Крім того, інтеграція дозволяє не тільки аналізувати події на окремих вузлах, а й будувати загальну картину атаки на рівні мережі, серверів, хмарних середовищ і облікових систем.

FortiEDR підтримує інтеграцію з більшістю популярних SIEM-платформ, зокрема Splunk, IBM QRadar, FortiSIEM, ArcSight, а також із рішеннями SOAR, такими як Cortex XSOAR, IBM Resilient, FortiSOAR, TheHive. Передача даних здійснюється через API або Syslog, при цьому використовуються стандартизовані формати повідомлень (CEF, LEEF, JSON), що дозволяє забезпечити сумісність з різними інструментами без суттєвих додаткових налаштувань.

Типова архітектура інтеграції передбачає, що FortiEDR Management Console, яка отримує телеметрію від агентів, передає події у реальному часі на SIEM-сервер. Там ці події аналізуються за допомогою правил кореляції, після чого залежно від їх критичності можуть бути ініційовані сценарії реагування в SOAR-платформі. Це забезпечує швидке прийняття рішень і автоматичне виконання таких дій, як ізоляція хосту, оновлення політик, надсилання повідомлень, створення інцидентів у системі Service Desk [3].

Таблиця 3.6

Основні функціональні зв’язки між FortiEDR, SIEM і SOAR

Компонент	Призначення	Взаємодія з FortiEDR
FortiSIEM / Splunk	Збір логів, кореляція подій, візуалізація інцидентів	Отримує дані через API/Syslog
FortiSOAR / XSOAR	Автоматизація дій, сценарії реагування, playbooks	Виконує дії за подіями FortiEDR
CMDB	Інвентаризація пристроїв і облікових записів	Збагачує події FortiEDR контекстною інформацією
Service Desk (Jira)	Реєстрація інцидентів, облік виконаних дій	Автоматичне створення задач по інциденту

У межах практичного прикладу інтеграції FortiEDR із SIEM-системою Splunk та SOAR-платформою FortiSOAR було побудовано повний життєвий цикл обробки інциденту. На першому етапі агент FortiEDR зафіксував спробу запуску PowerShell-скрипта з підозрілими параметрами, що вказувало на ймовірну fileless-атаку. Ця подія була автоматично передана до Splunk, де з неї було згенеровано подію рівня критичності 4 (High). Далі ця подія була передана у FortiSOAR, де було активовано playbook, що передбачав: перевірку хешу файлу через VirusTotal, ізоляцію пристрою, сповіщення аналітика електронною поштою та створення інциденту в Jira.

Таблиця 3.7

Життєвий цикл інциденту з використанням FortiEDR + SIEM + SOAR

Етап	Система	Автоматизована дія
Виявлення	FortiEDR	Ідентифікація поведінкового відхилення, створення події
Передача до SIEM	Splunk	Прийом Syslog, аналіз за правилами кореляції
Ініціація Playbook	FortiSOAR	Перевірка хешу, quarantine хосту, повідомлення
Реєстрація інциденту	Jira	Створення задачі з прикріпленим логом
Аудит дій	FortiEDR / SOAR	Збереження звіту, оновлення політик реагування

Інтеграція FortiEDR із SIEM та SOAR дозволила реалізувати наскрізну аналітику інцидентів: від точки входу до повного усунення. Наприклад, на основі кореляції подій у Splunk було виявлено, що аналогічна активність спостерігалася у ще двох хостів у регіональному офісі. Це дало змогу ідентифікувати вектор атаки — зловмисний Excel-файл, розісланий через електронну пошту. Завдяки Playbook у FortiSOAR ці пристрої було ізольовано, а користувачів — переведено до групи посиленого моніторингу на 48 годин.

Окремо варто відзначити можливість зворотного впливу інтеграції: SIEM та SOAR можуть не лише приймати події від FortiEDR, а й змінювати його конфігурацію. Наприклад, FortiSOAR за результатами аналізу може відправити запит на оновлення політик на рівні FortiEDR Console, додати

новий індикатор компрометації або внести виняток для легітимної активності, яка помилково сприймається як загрозлива.

Таблиця 3.8

Приклади дій SOAR-платформи у відповідь на події FortiEDR

Подія FortiEDR	Дія SOAR	Результат
Виявлення шкідливого хешу	Перевірка через VirusTotal	Якщо підтверджено — quarantine + ізоляція
Спрацьовування фішингового шаблону	Надсилання листа користувачу з інструкціями	Навчання, збір підтвердження прочитання
Поява нових облікових записів	Створення задачі в ServiceNow	Перевірка на політику дозволів, аудит логів
Повторювані інциденти в підрозділі	Активізація скрипту блокування USB	Автоматична політика FortiEDR через API

Таким чином, інтеграція FortiEDR із SIEM/SOAR забезпечує перехід від фрагментованого аналізу інцидентів до централізованої, автоматизованої, наскрізної системи обробки загроз. Такий підхід дозволяє суттєво зменшити час реагування (MTTR), знизити навантаження на аналітиків, уникнути людських помилок та посилити проактивність кіберзахисту. На практиці впровадження повної інтеграції дозволяє перетворити FortiEDR з просто інструменту для виявлення загроз у повноцінний компонент адаптивної системи кіберстійкості, що динамічно реагує на події та забезпечує безпеку у реальному часі [28].

3.4. Методика підготовки персоналу до роботи з EDR-рішеннями

Методика підготовки персоналу до роботи з EDR-рішеннями, зокрема такими як FortiEDR, є критичним елементом забезпечення ефективності функціонування систем кіберзахисту. Навіть найсучасніше програмне забезпечення втрачає свою ефективність у випадку, коли фахівці, які його експлуатують, не володіють достатнім рівнем знань, навичок і методологічного підходу до аналізу, реагування та оптимізації процесів. Тому побудова системної, поетапної і практикоорієнтованої програми підготовки

кадрів є невід'ємною складовою цифрової безпеки підприємства. Розроблена методика передбачає декомпозицію навчального процесу на три ключові рівні: базову обізнаність, операційні навички та стратегічне управління інцидентами. Водночас особлива увага приділяється створенню лабораторних практик, моделюванню інцидентів, гейміфікації навчання, оцінюванню результатів та подальшому супроводу персоналу.

Мета методики полягає в тому, щоб забезпечити співробітників підприємства знаннями щодо базових принципів роботи EDR, вмінь користуватись основним функціоналом FortiEDR, навичок самостійного аналізу інцидентів, а також здатністю приймати рішення у критичних ситуаціях. Методика передбачає поділ персоналу на категорії відповідно до ролей у системі інформаційної безпеки: звичайні користувачі, IT-персонал, аналітики безпеки (SOC), адміністратори безпеки, керівники підрозділів.

Таблиця 3.9

Категорії персоналу та рівні компетенцій у роботі з FortiEDR

Категорія співробітника	Рівень доступу до FortiEDR	Основні знання та навички
Користувач (End User)	Пасивний/Інформативний	Розпізнавання фішингу, реагування на повідомлення
Системний адміністратор	Частковий (Policy Deployment)	Розгортання агентів, базові налаштування
Аналітик SOC	Повний (Incident Response)	Розслідування подій, аналіз ланцюгів атак, карантин
Менеджер з безпеки	Аудиторський / Управлінський	Управління політиками, контроль відповідності
Архітектор безпеки	Повний доступ + API	Інтеграції, автоматизація, сценарії реагування

Процес підготовки складається з кількох логічних етапів. На першому етапі проводиться оцінка поточних компетенцій персоналу, що дозволяє ідентифікувати прогалини в знаннях та сформувати цільову програму. Далі розробляються навчальні модулі за принципом модульної побудови, які охоплюють як теоретичні знання (наприклад, архітектура FortiEDR, моделі

загроз MITRE ATT&CK), так і практичні навички (створення політик, аналіз інцидентів, побудова звітів, реагування на реальні атаки).

Таблиця 3.10

Основні навчальні модулі для персоналу з EDR

Модуль	Цільова аудиторія	Зміст
Вступ до EDR	Усі категорії	Що таке EDR, роль у кіберзахисті
Робота з FortiEDR Agent	Системні адміністратори	Встановлення, оновлення, верифікація
Виявлення та реагування	Аналітики SOC	Робота з інцидентами, quarantine, аналіз
Управління політиками	Менеджери з безпеки	Налаштування правил, профілів, виключень
Інтеграція FortiEDR	Архітектори безпеки	API, SIEM, SOAR, сценарії автоматизації
Практикум із симуляціями	Усі категорії (крім end-user)	Аналіз інцидентів у лабораторному середовищі

Практична частина навчання реалізується у вигляді лабораторного полігону, на якому імітуються реальні сценарії загроз. Наприклад, учасникам пропонується проаналізувати виявлений інцидент запуску підозрілого скрипта, визначити джерело загрози, локалізувати її, провести ретроспективний аналіз та сформувати звіт. Усі дії виконуються в середовищі FortiEDR Console, з обов'язковим документуванням дій, що дозволяє оцінити ефективність рішень. Окремі заняття присвячені інтеграції FortiEDR з SIEM, роботі з логами, API-запитами, формуванню Playbooks у SOAR.

Після проходження кожного модуля проводиться оцінювання знань. Для цього застосовується змішана модель: онлайн-тестування з теорії, симуляція інциденту з реальними діями в середовищі FortiEDR, захист рішення. Наприклад, після модуля "Виявлення та реагування" аналітик повинен класифікувати 5 реальних подій, виявити false positive, описати індикатори компрометації та вказати заходи ізоляції [18].

Таблиця 3.11

Методи оцінювання підготовки персоналу з FortiEDR

Метод	Опис	Оцінка
Онлайн-тестування	30 питань з теорії роботи FortiEDR	Поріг — 75 % правильних
Практичне завдання	Аналіз інциденту, quarantine, log review	Підтвердження кожного кроку
Рольова гра (Red vs Blue)	Атака/Захист у лабораторному середовищі	Командна оцінка результату
Індивідуальний захист звіту	Презентація кейсу, звітність, рекомендації	Експертна оцінка (3 балівки)

Особливу увагу в методиці займає елемент післянавчальної підтримки: персоналу надається доступ до бази знань (внутрішнього Wiki), регулярних брифінгів, оновлень практик, інтерактивних вебінарів. Кожен аналітик має менторську підтримку більш досвідченого колеги. Створюється ком'юніті з розбором реальних інцидентів, обміну досвідом та новими шаблонами загроз.

У рамках практичної реалізації на базі однієї з українських компаній було проведено підготовку 12 співробітників. Початковий рівень знань був неоднорідним: лише 3 мали попередній досвід роботи з EDR. Після проходження 40-годинної програми (8 теоретичних модулів, 4 лабораторії, 1 тренінг Red Team vs Blue Team) 10 із 12 здобули сертифікати внутрішнього рівня FortiEDR Specialist. У реальному середовищі після запуску системи було зафіксовано зменшення часу реагування на інцидент з 28 до 7 хвилин, а кількість false positives зменшилась на 43 %, що свідчить про якісне освоєння функціоналу системи.

Таким чином, запропонована методика підготовки персоналу до роботи з EDR-рішеннями дозволяє не лише навчити основним принципам використання FortiEDR, а й забезпечити глибоке розуміння архітектури, взаємодії компонентів, методів аналізу та реагування. Системний підхід, рольова класифікація, багаторівнева оцінка, практичні заняття та постійна підтримка формують культуру кібербезпеки та забезпечують стійкість організації перед загрозами нового покоління [14].

3.5. Пропозиції щодо адаптації досвіду для українських підприємств

Адаптація досвіду використання FortiEDR для українських підприємств є важливим завданням в умовах зростання кіберзагроз, обмежених ресурсів та необхідності забезпечення національної кіберстійкості. Успішне впровадження EDR-рішень у міжнародних компаніях надає велику кількість моделей, практик та рекомендацій, однак без врахування локального контексту — зокрема законодавства, технічного рівня підприємств, кадрового потенціалу та характеру IT-інфраструктур — цей досвід не може бути перенесений механічно. Необхідно сформувати конкретизовані пропозиції, які враховують реалії українських організацій, що функціонують у приватному, державному чи оборонному секторі. Особливої актуальності тема набуває в умовах триваючої гібридної агресії та критичної залежності країни від цифрової інфраструктури.

На основі аналізу практик провідних компаній, результатів впровадження FortiEDR на українських підприємствах, експертних інтерв'ю та власних досліджень сформульовано п'ять основних напрямів адаптації, кожен із яких супроводжується низкою практичних рекомендацій: оптимізація витрат, кадрове забезпечення, технічна масштабованість, відповідність регуляторним вимогам та інтеграційна гнучкість [6].

Таблиця 3.12

Основні напрямки адаптації досвіду використання FortiEDR для українських підприємств

Напрям адаптації	Ключова мета	Приклади рішень
Фінансова оптимізація	Зменшення витрат без втрати функціональності	Ліцензії з оплатою за події або агентів
Кадрове забезпечення	Підвищення рівня обізнаності персоналу	Курси, лабораторії, рольове навчання
Технічна масштабованість	Гнучке впровадження в умовах різнорідної інфраструктури	Використання lightweight-агентів
Регуляторна відповідність	Відповідність українським нормам кіберзахисту	Мапінг функцій FortiEDR до ДСТУ/НД ТЗІ
Інтеграційна адаптивність	Можливість з'єднання з локальними системами	Інтеграція з українськими SIEM, CMDB

Першим важливим аспектом є вартісна досяжність рішення. Для багатьох українських підприємств, особливо середнього та малого бізнесу, ключовим бар'єром є вартість повноцінної ліцензії FortiEDR. У таких випадках доцільно застосовувати гібридні моделі ліцензування, наприклад, обмежити агентів лише для критичних вузлів (сервери, робочі станції керівництва, бухгалтерія), а для менш критичних використовувати безкоштовні засоби виявлення з інтеграцією в консоль FortiEDR. Також можливо налаштувати збір лише пріоритетних типів подій, що зменшує обсяг трафіку та витрати на зберігання.

Таблиця 3.13

Приклад економічної моделі використання FortiEDR на українському підприємстві

Категорія пристроїв	Кількість	Рівень захисту	Агент FortiEDR	Інше рішення
Сервери бухгалтерії та ERP	10	Повний	Так	–
Робочі місця адміністрації	40	Середній	Так	Часткове
Рядові користувачі	120	Базовий	Ні	Антивірус + SIEM
Віртуальні машини тестування	20	Вибірковий	Так (тимчасово)	У режимі "Observe"

Наступним важливим етапом є створення кадрової бази для підтримки EDR. Більшість українських IT-фахівців не мали справи з повноцінними засобами поведінкового аналізу до моменту активної цифровізації. Тому необхідно впровадити типову модель навчання із сертифікацією, уніфікованими модулями підготовки, адаптованими до FortiEDR. Таке навчання має включати як базові знання (архітектура FortiEDR, принципи MITRE ATT&CK), так і практику — виявлення інциденту, quarantine, створення винятків, інтеграцію з поштовими системами.

Таблиця 3.14

Типовий маршрут навчання фахівця з роботи з FortiEDR

Етап	Мета	Орієнтовна тривалість	Форма
Ознайомчий курс	Що таке EDR, огляд FortiEDR	4 год	Онлайн / офлайн
Робота з подіями	Інтерфейс, журнал подій	6 год	Практика + симуляції
Реагування на загрози	Quarantine, ізоляція	8 год	Лабораторія
Інтеграції	SIEM, SOAR, API	4 год	Конфігурація
Підсумковий тест	Перевірка знань	1 год	Онлайн/офлайн

Третім напрямом є масштабованість в умовах неоднорідної інфраструктури. Часто в українських підприємствах поєднуються старі та нові ОС, фізичні й віртуальні середовища, локальні сервери та хмара. FortiEDR підтримує deployment через різні сценарії: MSI-пакети, GPO, API. Водночас для обмежених середовищ пропонується режим Observe, де агент не втручається, а лише моніторить. Це дозволяє поступово впроваджувати систему без критичного навантаження [20].

Четвертий аспект — відповідність українським нормативам у сфері кібербезпеки. На сьогодні підприємства, які належать до об'єктів критичної інфраструктури, зобов’язані відповідати вимогам законів "Про основи забезпечення кібербезпеки", НД ТЗІ 2.5-004:2008, Національної стратегії кібербезпеки. FortiEDR повністю відповідає ISO/IEC 27001 і NIST CSF, однак для адаптації до українських норм рекомендовано створити локальні профілі безпеки з відповідною мапінг-таблицею.

Таблиця 3.15

Мапінг функцій FortiEDR до вимог НД ТЗІ та ISO/IEC

Вимога НД ТЗІ / ISO	Механізм FortiEDR	Коментар
Логування інцидентів	Інцидентна консоль, API-запити	Повний запис подій
Контроль доступу	RBAC, політики доступу до консолі	Рівні доступу, аудит
Реагування на загрози	Quarantine, kill process, isolate host	Автоматизовані реакції
Резервне копіювання	Непряма інтеграція через FortiManager	Потрібна зовнішня інтеграція
Збереження ланцюга	Таймлайн подій, архіви	Схема "kill chain" у FortiEDR

П’ятий напрям — інтеграція з локальними системами, зокрема SIEM, SOAR, Service Desk. У багатьох українських компаніях використовуються Open Source рішення, такі як Wazuh, Graylog, TheHive. FortiEDR має відкритий API, підтримує Syslog, JSON і може бути адаптований до будь-якої архітектури за наявності компетентного адміністратора. Наприклад, інцидент FortiEDR можна автоматично перенаправити в Jira через вебхуки або в SIEM через UDP-канал.

Таким чином, адаптація FortiEDR до умов українського ринку можлива за умови комплексного підходу — від гнучкого ліцензування до формування кадрової бази та інтеграційної архітектури. Запропоновані рішення забезпечують зниження бар’єру входу, ефективне розгортання та відповідність вимогам безпеки. З урахуванням викликів, пов’язаних з військовою агресією, частими кібератаками на держсектор та приватний бізнес, інтеграція FortiEDR на національному рівні може стати складовою стратегії цифрової оборони України [13].

Висновки до розділу

У третьому розділі дипломної роботи було зосереджено увагу на формуванні практичних рішень, орієнтованих на підвищення ефективності виявлення та реагування на інциденти інформаційної безпеки із застосуванням системи FortiEDR. На основі узагальнення кращих міжнародних практик, результатів аналізу функціоналу FortiEDR та специфіки вітчизняного корпоративного середовища розроблено власні підходи до оптимізації політик безпеки, побудови архітектури реагування, інтеграції з іншими елементами захисту та підготовки персоналу. Всі ці аспекти розглядалися в контексті максимальної адаптації до умов українських підприємств.

У підпункті, присвяченому оптимізації політик безпеки, обґрунтовано доцільність багаторівневого підходу до конфігурації FortiEDR, що базується на категоризації активів, ролей користувачів, критичності інформації та типах

загроз. Визначено набір ефективних сценаріїв реагування, які дозволяють досягти балансу між гнучкістю та надійністю системи. Встановлено, що грамотна сегментація політик та використання режимів *Observe* і *Protect* у різних сегментах інфраструктури дозволяють значно знизити навантаження на систему й кількість хибних спрацювань, зберігаючи при цьому високий рівень захисту.

Розроблена власна модель реагування на інциденти продемонструвала приклад побудови логічної архітектури процесів, яка охоплює всі ключові етапи: виявлення, класифікацію, пріоритезацію, реагування, аудит, навчання. Запропонована модель передбачає інтеграцію FortiEDR із зовнішніми системами (SIEM, SOAR, Service Desk), використання автоматизованих Playbook, зворотний зв’язок для оптимізації політик. Практичне моделювання показало, що застосування такої моделі дозволяє скоротити середній час реагування на інцидент більш ніж у три рази, а також суттєво знизити ризики поширення загроз у мережі.

У межах аналізу інтеграційного потенціалу FortiEDR було обґрунтовано ефективність її взаємодії з популярними SIEM- та SOAR-платформами, такими як Splunk, FortiSIEM, FortiSOAR, TheHive. Показано, що завдяки підтримці API, JSON та Syslog, FortiEDR легко адаптується до існуючої інфраструктури без додаткових витрат. Демонстрація життєвого циклу інциденту — від виявлення до автоматизованого реагування — підтвердила практичну доцільність реалізації наскрізного контролю подій без залучення великої кількості персоналу.

Окремо було представлено методику підготовки персоналу до ефективної роботи з EDR-рішеннями. На основі системного аналізу освітніх підходів, симуляцій інцидентів, рольових сценаріїв та тестування компетенцій запропоновано поетапну програму підготовки фахівців. Запропоновано модель диференціації навчання за категоріями співробітників — від простих користувачів до архітекторів безпеки — із залученням як теоретичного, так і

практичного матеріалу. Це дозволяє не лише ефективно освоїти функціонал FortiEDR, а й створити внутрішню культуру кіберзахисту в організації.

У завершальному підпункті представлено конкретні пропозиції щодо адаптації закордонного досвіду застосування EDR-рішень до реалій українських підприємств. Зокрема, розглянуто можливість поетапного впровадження FortiEDR у різних сегментах, застосування моделей економного ліцензування, відповідність вимогам ДСТУ та НД ТЗІ, інтеграцію з локальними SIEM-рішеннями, організацію навчання та кадрового супроводу. Показано, що за умов обмежених ресурсів українські організації можуть впровадити EDR-технології на базі FortiEDR поступово, без втрати ефективності, при цьому значно підвищивши загальний рівень інформаційної безпеки.

Таким чином, результати третього розділу підтвердили доцільність використання FortiEDR як центрального інструменту системи реагування на інциденти у корпоративних структурах. Практична реалізація моделі, побудова інтеграцій, навчання персоналу та адаптація до локальних умов дозволяють не лише посилити захист, а й закласти підґрунтя для довгострокової кіберстійкості підприємств. Отримані результати можуть бути використані як типова модель для розробки внутрішніх регламентів реагування на інциденти інформаційної безпеки в умовах українського кіберпростору.

ВИСНОВКИ

Проведене дослідження дало змогу комплексно охарактеризувати сучасні підходи до виявлення та реагування на інциденти інформаційної безпеки у корпоративних IT-середовищах із використанням технологій класу EDR на прикладі системи FortiEDR. В умовах посилення кіберзагроз, гібридних атак, інтенсивного використання цільових шкідливих програм та активної експлуатації людського фактора стає очевидною недостатність традиційних антивірусних і фаєрвол-засобів для забезпечення повноцінного кіберзахисту. Еволюція від базових засобів захисту до платформ типу EDR є об'єктивним наслідком зростання складності та прихованості сучасних загроз, які проникають у корпоративну інфраструктуру не лише через технічні вразливості, а й завдяки поведінковим вектором впливу на кінцевих користувачів.

У роботі було визначено, що FortiEDR є повнофункціональною платформою, яка дозволяє здійснювати глибокий поведінковий аналіз подій, ізолювати небезпечні об'єкти, забезпечувати контроль усіх процесів у реальному часі, будувати детальні ланцюги атак та формувати автоматизовані сценарії реагування. На відміну від багатьох традиційних антивірусних продуктів, FortiEDR не лише виявляє загрозу за сигнатурами, а й виявляє нетипову поведінку, взаємодію між об’єктами та аномалії у діях користувача чи процесів системи. Платформа забезпечує адаптивний рівень безпеки завдяки можливості гнучкого налаштування політик, інтеграції з SIEM- і SOAR-системами, підтримці хмарних та локальних середовищ, а також API-доступу до аналітики.

Особливу увагу було приділено побудові архітектури ефективного реагування на інциденти. У межах дослідження було розроблено модель реагування, що включає в себе виявлення, класифікацію, пріоритезацію, автоматизоване реагування, аудит та зворотний зв'язок. Встановлено, що саме наявність повноцінної моделі реагування дозволяє не лише швидко

нейтралізовувати інциденти, а й забезпечити циклічну оптимізацію налаштувань політик безпеки на основі аналізу минулих подій.

На основі практичного моделювання, аналізу інцидентів та прикладів впровадження FortiEDR в умовах української IT-інфраструктури було обґрунтовано необхідність адаптації західного досвіду до локальних умов. Запропоновано набір рекомендацій для українських підприємств, що охоплюють фінансову оптимізацію (впровадження FortiEDR на критичних вузлах), навчання персоналу (поетапна сертифікація та гейміфіковані лабораторії), інтеграцію з наявними системами безпеки (включаючи українські SIEM-рішення) та відповідність вимогам вітчизняного законодавства у сфері кібербезпеки. Доведено, що навіть у межах обмеженого бюджету підприємства можуть ефективно інтегрувати FortiEDR як ядро платформи кіберзахисту з поступовим масштабуванням функціоналу.

Крім того, у роботі було запропоновано методику підготовки фахівців із кібербезпеки до роботи з EDR-рішеннями. Методика базується на поетапному навчанні, розподілі за ролями, проведенні симуляцій інцидентів та практичному закріпленні навичок у реальному середовищі FortiEDR. Це дозволяє не лише покращити технічну підготовку персоналу, а й сформувати всередині організації культуру безпеки, орієнтовану на проактивне мислення.

Підсумовуючи результати дослідження, можна стверджувати, що FortiEDR є інноваційним рішенням, яке забезпечує сучасний рівень захисту кінцевих точок від широкого спектра кіберзагроз. Його впровадження дозволяє організаціям зменшити ризики компрометації, підвищити оперативність реагування, оптимізувати навантаження на служби безпеки та адаптувати механізми контролю відповідно до динамічних викликів кіберпростору. Отримані в дипломній роботі результати можуть бути використані як методична база для проектування систем реагування в IT-підрозділах українських підприємств, а також для формування політик кіберзахисту на рівні стратегічного планування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Anton A., Shapiro D. Security automation and orchestration: Integrating EDR with SIEM and SOAR // Journal of Cybersecurity Research. – 2020. – Vol. 5, No. 3. – P. 112–120.
2. Bakotech. Network Detection and Response: Як покращити кібербезпеку організації в умовах зростання кількості атак. – 2023. – 12 с.
3. CERT-UA. Звіт про систему виявлення вразливостей та реагування на кіберінциденти та кібератаки. – [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/article/17696
4. Crowe C., Nguyen M. Incident Response Strategies in Enterprise IT Environments // ACM Computing Surveys. – 2021. – Vol. 54, No. 2. – P. 44–56.
5. Cyberset. Топ-5 EDR (Endpoint Detection and Response) інструментів 2025 // Cyberset. – 2025. – [Електронний ресурс]. – Режим доступу: https://cyberset.com.ua/network/attacks-vs-defense/endpoint-detection-and-response-edr-security/
6. European Union Agency for Cybersecurity (ENISA). (2021). Threat Landscape for Endpoint Security. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/threat-landscape-for-endpoint-security
7. Fortinet. (2023). FortiEDR Administration Guide. Version 5.0. [Електронний ресурс]. – Режим доступу: https://docs.fortinet.com/document/fortiedr/5.0.0
8. GDPR (General Data Protection Regulation) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
9. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
10. ISO/IEC 27035-1:2023. Інформаційна безпека. Управління інцидентами. Частина 1: Принципи управління інцидентами.

11. IT Ukraine Association. Огляд ринку кібербезпеки в Україні. – 2024. – 24 с.

12. Lee B., Smith C. Endpoint Detection and Response: Strategies for modern threat protection // Cybersecurity Journal. – 2019. – Vol. 12, No. 4. – P. 55–65.

13. Mitre Corporation. ATT&CK Framework. – 2023. – [Електронний ресурс]. – Режим доступу: https://attack.mitre.org

14. National Institute of Standards and Technology. (2018). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide. Gaithersburg: NIST. [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

15. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide. – [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

16. Scholtz T. Best Practices for EDR Implementation // Gartner Research. – 2022. – [Електронний ресурс]. – Режим доступу: https://www.gartner.com/document/4003217

17. Symantec. (2021). Comparative Analysis of Endpoint Protection Platforms. [Електронний ресурс]. – Режим доступу: https://www.broadcom.com/products/cyber-security

18. Баклан Я. А., Сєвєрінов О. В. Аналіз систем захисту кінцевих точок від складних загроз EDR (Endpoint Detection and Response) // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали дванадцятої міжнар. наук.-практ. конф. – 2022. – С. 141.

19. Грищук Л. М., Жовноватюк В. В., Носова І. О. Штучний інтелект у сфері кібербезпеки: інновації, виклики та перспективи // Military Science. – 2024. – Т. 2, № 1. – С. 201–206.

20. Державна служба спеціального зв’язку та захисту інформації України. Методичні рекомендації щодо реагування суб’єктів кібербезпеки на

події в кіберпросторі. Наказ № 570 від 2023 р. – [Електронний ресурс]. – Режим доступу:

21. Державна служба спеціального зв'язку та захисту інформації України. Звіт про стан кіберзахисту критичної інформаційної інфраструктури за 2023 рік. – [Електронний ресурс]. – Режим доступу:

22. Жук, О. О. (2021). Аналіз сучасних підходів до захисту інформації в інформаційно-комунікаційних системах. Захист інформації, № 3, с. 16–21.

23. Журавель, І. І. (2023). Система захисту кінцевих точок: тенденції та перспективи розвитку. Вісник НТУУ «КПІ», Серія: Інформатика та обчислювальна техніка, № 2(172), с. 41–46.

24. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. – [Електронний ресурс]. – Режим доступу:

25. Зозуля, Т. І., & Кравчук, І. В. (2023). Роль EDR-систем у побудові комплексної системи захисту підприємства. Інформаційні системи і технології, № 1(44), с. 12–17.

26. Мащенко, В. М. (2022). Стандарти кібербезпеки та їх вплив на захист підприємства. Інформаційні технології в освіті, науці та виробництві, № 1(9), с. 32–36.

27. Мельник, А. В., & Кисіль, Ю. І. (2020). Використання поведінкового аналізу для виявлення загроз на кінцевих точках. Вісник НТУ «ХПІ», Серія: Системи управління, обчислювальна техніка та інформатика, № 7(1356), с. 55–60.

28. Мудра М. І. Інформаційна безпека підприємства в умовах цифрової трансформації // Економіка. Фінанси. Право. – 2021. – № 8. – С. 27–30.

29. Національна стратегія кібербезпеки України. Указ Президента України від 26.08.2021 № 447/2021. – [Електронний ресурс]. – Режим доступу:

30. Олійник, С. В., & Марков, Д. І. (2022). Аналіз ефективності засобів виявлення загроз у корпоративних мережах. Інформаційні технології і засоби навчання, № 2(88), с. 55–61.

31. План реалізації Стратегії кібербезпеки України на 2023–2024 роки. Розпорядження Кабінету Міністрів України від 16.05.2023 № 497-р. – [Електронний ресурс]. – Режим доступу:

32. Постанова Кабінету Міністрів України від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту». – [Електронний ресурс]. – Режим доступу:

33. Шуліка К. М., Балагура Д. С., Смірнов А. О., Непокритов Д. М., Литвин А. В. Метод використання сучасних систем захисту кінцевих точок (EDR) для убезпечення від комплексних атак // Сучасний стан наукових досліджень та технологій в промисловості. – 2024. – № 2 (28). – С. 182–195.