КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.808
УДК 004.89

Примаченко Діана Володимирівна
асистент
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0003-2386-7440
primachenkodiana08@gmail.com

Святська Надія Андріївна
студентка
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0000-8132-9403
svyatskan@gmail.com

Голобородько Сергій Олександрович
старший викладач
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0006-9892-3031
s.holoborodko@duikt.edu.ua

Недодай Михайло Геннадійович
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0000-0876-9971
c13h21n3o10@gmail.com

Дьячук Олександр Станіславович
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0006-5585-6393
realjewua@gmail.com

EDR ТА XDR ЯК ОСНОВНІ ТЕХНОЛОГІЇ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

Анотація. У статті аналізується роль захисту кінцевих точок (Endpoint Security) як основного елементу сучасних IT-інфраструктур, що відіграє ключову роль у протидії кіберзагрозам на початковому етапі атак. Розглядаються традиційні інструменти, такі як EPP (Endpoint Protection Platform), які базуються на сигнатурному аналізі та блокуванні відомих загроз. Детальний огляд EDR (Endpoint Detection and Response) висвітлює його переваги: безперервний моніторинг дій на кінцевих пристроях у реальному часі, використання машинного навчання для ідентифікації відхилень від норми, а також поведінкову аналітику для виявлення підозрілих активностей. EDR забезпечує не лише детектування, а й автоматизовані механізми реагування: блокування підозрілих дій, ізоляцію пристроїв від мережі, видалення шкідливого коду. XDR (Extended Detection and Response) представлено як еволюційний розвиток EDR, де аналіз даних відбувається на рівні всієї інфраструктури. Технологія агрегує інформацію з кінцевих пристроїв, мережевих сенсорів, хмарних сервісів, електронної пошти та SIEM-систем, що забезпечує комплексний огляд загроз. XDR автоматизує кореляцію подій, виявляє складні атаки, які охоплюють різні сегменти мережі, та прискорює реакцію через централізоване управління (наприклад, одночасне блокування загрози в різних середовищах). Порівняння EDR та XDR демонструє, що останній усуває розрізненість інструментів, забезпечує єдиний інтерфейс для моніторингу та зменшує операційне навантаження на команди безпеки. Як приклади реалізації технологій описані: FortiManager — інструмент для централізованого управління політиками безпеки, налаштування фаєрволів, моніторингу подій у різних сегментах мережі та координації роботи EDR-рішень; Symantec Endpoint Security Complete — платформа, яка поєднує EDR, антивірусний захист, контроль додатків, шифрування даних і захист від експлойтів, забезпечуючи багаторівневий захист для корпоративних пристроїв.

Ключові слова: захист кінцевих точок; кібербезпека; засоби захисту; мережева безпека; технології захисту кінцевих точок; XDR; EDR; Fortinet; Symantec, кібератака

ВСТУП

Кібербезпека стає все більш актуальною у світі, який надто залежить від технологій та високотехнологічних рішень. Захист кінцевих точок (англ. Endpoint Security) є ключовим завданням у цьому контексті, оскільки саме це є місцем, де інформація зустрічається з потенційними загрозами. У цій статті ми розглянемо важливість захисту кінцевих точок та основні заходи, які можуть бути прийняті для забезпечення надійності цього аспекту кібербезпеки.

Кінцеві пристрої, такі як настільні комп'ютери, ноутбуки, сервери, маршрутизатори та мобільні пристрої, можуть бути вразливими до зловмисних кібератак і порушень. Кінцеві пристрої залишаються основними цілями для зловмисників і, отже, є вразливими точками входу в мережу. Ці пристрої становлять серйозну проблему, оскільки вони, як правило, знаходяться під контролем і використовуються співробітниками, забезпечуючи віддалений зв'язок з мережею і підключення до неї. Безпека кінцевих точок і відповідне навчання співробітників є переднім краєм багаторівневої стратегії глибокого захисту від кібератак [1].

Постановка проблеми. Вибір ефективного захисту кінцевих точок є надзвичайно важливим у сучасному контексті кібербезпеки з ряду об'єктивних та стратегічних причин. Насамперед, кінцеві точки часто є основним місцем атак для зловмисників, оскільки вони представляють собою велику поверхню для потенційних загроз. Професійний захист кінцевих точок забезпечує ефективний контроль над доступом, а також реагує на потенційно небезпечну активність.

Аналіз останніх досліджень і публікацій. Багато вчених та дослідників присвятили свою роботу вивченню питань кібербезпеки, зокрема захисту кінцевих точок, серед яких: Брюс Шнайер [2], Крістофер Крідер [3], Ріхард Кларк [4] та інші. Авторами були розроблені рекомендації щодо використання сучасних технологій захисту, таких як антивірусні програми, механізми виявлення загроз та реагування на їх, інструменти шифрування тощо, а також аналізували та досліджували цей напрямок, пропонуючи нові підходи та рішення для ефективного захисту кінцевих точок у сучасному інформаційному середовищі.

Мета статті. Дослідження має на меті розгляд та розкриття важливості захисту кінцевих точок у сфері кібербезпеки. Дослідження спрямоване на дослідження технології XDR, EDR у захисті кінцевих точок, які можуть виникнути на кінцевих точках, таких як комп'ютери та інші пристрої, що з'єднані з мережею. Окрім того, воно ставить за мету розглянути основні заходи та стратегії, які можуть бути використані для забезпечення надійності та безпеки цих кінцевих точок.

Дослідження розглядає важливість захисту кінцевих точок через їхню ключову роль у виявленні та захисті від кіберзагроз. Зокрема, дослідження може досліджувати питання, пов'язані з першим контактом із загрозами, витоками конфіденційної інформації, та впливом вразливостей на безпеку всієї мережі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Захист кінцевих точок виявляється критичним аспектом цифрової безпеки підприємства, оскільки саме ці пристрої є першим контактом із потенційними

кіберзагрозами. Виходячи за межі традиційного підходу до захисту мережі, сучасні загрози вимагають високофункціональних стратегій, спрямованих саме на кінцеві точки.

Однією з визначальних проблем є витік конфіденційної інформації через вразливості в кінцевих точках. Нападники активно використовують цей вектор, висліджуючи можливості для несанкціонованого доступу та витоку важливих даних. Тому ефективний захист кінцевих точок забезпечується не тільки через виявлення і блокування загроз, але і шляхом запобігання можливим витокам, що можуть серйозно пошкодити довіру та надійність інформаційних систем [5].

EDR (Endpoint Detection and Response) є ключовим компонентом сучасних стратегій кібербезпеки, спрямованим на виявлення та відповідь на загрози в області кінцевих точок, таких як комп'ютери, сервери та мобільні пристрої. Системи EDR володіють здатністю аналізувати активність на кожній кінцевій точці в реальному часі, виявляти аномальні патерни та потенційні загрози, а також забезпечувати відповідь на інциденти. Рішення виявляє загрози у середовищі, досліджуючи весь життєвий цикл загрози та надаючи інформацію про все. Дослідження використовує технології, такі як аналіз журналів, машинне навчання та поведінкова аналітика для розпізнавання загрозливих дій, що можуть свідчити про атаку або порушення безпеки. Стримуючи загрозу в кінцевій точці, EDR допомагає усунути загрозу до того, як вона зможе поширитися.

Рис. 1. Схема роботи EDR [6]

EDR зосереджується насамперед на виявленні просунутих загроз, тобто тих, які розроблені, щоб обійти передові засоби захисту і успішно проникнути в середовище. EPP (Endpoint Protection Platform) зосереджується виключно на запобіганні загрозам на периметрі. За допомогою EPP важко, якщо взагалі можливо, заблокувати 100% загроз. Комплексне рішення для захисту кінцевих точок використовує можливості як EPP, так і EDR.

Більш складні загрози, які оминають захист периметра, можуть спричинити хаос у мережі. Програми-вимагачі шифрують конфіденційні дані до отримання фінансового викупу. Рішення EDR допоможе швидко знайти, локалізувати та усунути загрози, щоб забезпечити безпеку даних на кінцевих точках у середовищі [7].

XDR (Extended Detection and Response) є еволюційним кроком у сфері кібербезпеки, спрямованим на покращення виявлення і реагування на загрози. XDR відрізняється від традиційних рішень захисту кінцевих точок (EDR) та інших систем безпеки тим, що охоплює аналіз багатофакторних подій на різних рівнях інфраструктури. Інструмент об'єднує дані з різних джерел, таких як кінцеві точки, мережеві пристрої, хмарні сервіси тощо, для глибокого розуміння інцидентів безпеки. XDR використовує аналітику, машинне навчання та інші технології, щоб ідентифікувати та відповідати на загрози в реальному часі.

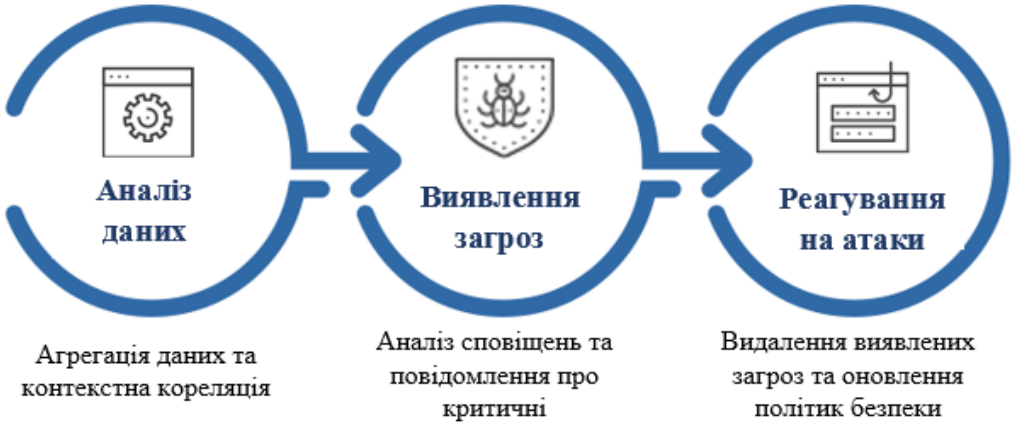

Рис. 2. Схема роботи XDR [8]

XDR пропонує виявлення та реагування на інциденти, пов'язані з безпекою, через кілька рівнів інформаційно-технологічного середовища. Замість того, щоб просто повідомляти про потенційні загрози, XDR може інтегруватися з іншими системами безпеки та виконувати автоматизовані заходи для забезпечення захисту, такі як блокування підозрілих процесів, ізоляція компрометованих кінцевих точок або блокування конкретних мережевих з'єднань. Продукт збирає інформацію, а потім автоматично з'єднує дані з кінцевих точок, електронної пошти, хмарних робочих навантажень, серверів, а також мереж, щоб виявити приховані загрози і дозволити експертам з безпеки вивчити їх і швидко відреагувати на них. Це допомагає скоротити час реакції на інциденти та зменшити вплив загроз на організацію, роблячи XDR потужним інструментом для сучасного кіберзахисту.

Розширене виявлення і реагування (XDR) є альтернативою традиційним реактивним методам, які забезпечують видимість атак на кожному рівні окремо за допомогою таких інструментів, як виявлення і реагування на кінцевих точках (EDR), аналіз мережевого трафіку (NTA) або управління інформацією та подіями безпеки (SIEM). Видимість ізольованих інцидентів, що відбуваються на різних рівнях, надає цінну інформацію, хоча і вимагає ручного розслідування, а також криміналістичної експертизи, щоб зібрати воєдино інформацію про реальну атаку. XDR уникає цієї ручної роботи, автоматично збираючи дані і створюючи звіт про атаку, що дозволяє миттєво реагувати [9].

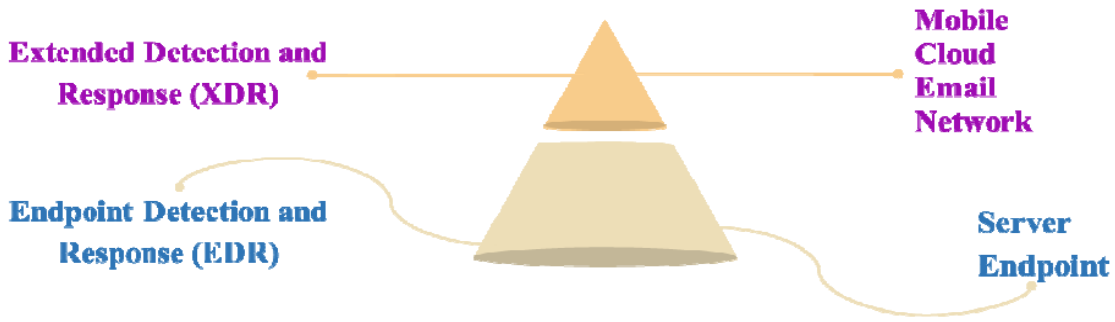

Рис. 3. Детальна схема усунення обмежень XDR і EDR [10]

Рішення EDR та XDR покликані замінити застарілі реактивні підходи до кібербезпеки. Як наслідок, EDR та XDR рішення схожі в декількох аспектах, таких як

– Превентивний підхід: традиційні рішення безпеки часто зосереджені на виявленні та усуненні поточних загроз. EDR та XDR можуть запобігти інцидентам безпеки шляхом збору детальних даних та застосування аналізу даних і розвідки загроз для виявлення загроз до того, як вони виникнуть.
– Швидке реагування на загрози: EDR та XDR підтримують автоматизоване виявлення загроз та реагування на них. Це дозволяє організації мінімізувати витрати, вплив і збитки, спричинені кібератакою, шляхом запобігання або швидкого усунення її наслідків.
– Підтримка функції розвідки загроз: функція забезпечує проактивний захист, дозволяючи аналітикам виявляти й усувати потенційні проблеми безпеки до того, як ними скористається зловмисник. EDR і XDR забезпечують глибоку видимість і легкий доступ до даних, що допомагає в пошуку загроз.

Незважаючи на свою схожість, EDR та XDR застосовують різні підходи до кібербезпеки. Деякі з основних відмінностей між EDR та XDR охоплюють:

– Ціль: EDR зосереджується на захисті кінцевої точки, забезпечуючи поглиблену видимість і запобігання загрозам для конкретного пристрою. XDR розглядає проблему ширше, інтегруючи безпеку кінцевих точок, хмарних обчислень, електронної пошти та інших рішень.
– Інтеграція рішень: рішення EDR можуть забезпечити найкращий у своєму класі захист кінцевих точок, і організація може вручну інтегрувати їх з безліччю точкових рішень. XDR розроблено для забезпечення інтегрованої видимості та управління загрозами в рамках одного рішення, що значно спрощує архітектуру безпеки організації [11].

Рішення щодо впровадження EDR або XDR залежить від конкретних потреб та ресурсів організації у сфері безпеки. Однак є деякі фактори, які можуть зробити XDR кращим ніж EDR рішенням для деяких організацій.

Однією з головних переваг XDR над EDR є комплексний підхід до кібербезпеки. XDR інтегрує дані з різних джерел, щоб забезпечити більш цілісне уявлення про стан безпеки організації. Це дозволяє краще реагувати на кінцеві точки та інші загрози, які можуть охоплювати кілька середовищ або векторів атак. На відміну від цього, EDR забезпечує захист лише окремих кінцевих точок в мережі і може не виявляти загрози, що походять з інших джерел.

Ще однією перевагою XDR є його здатність зменшити складність операцій з забезпечення безпеки. Надаючи уніфіковане рішення для виявлення загроз і реагування

на них у різних середовищах, XDR може спростити операції з безпеки і зменшити потребу в багатоточкових рішеннях. Це може допомогти зменшити витрати і потреби в ресурсах для операцій з кібербезпеки.

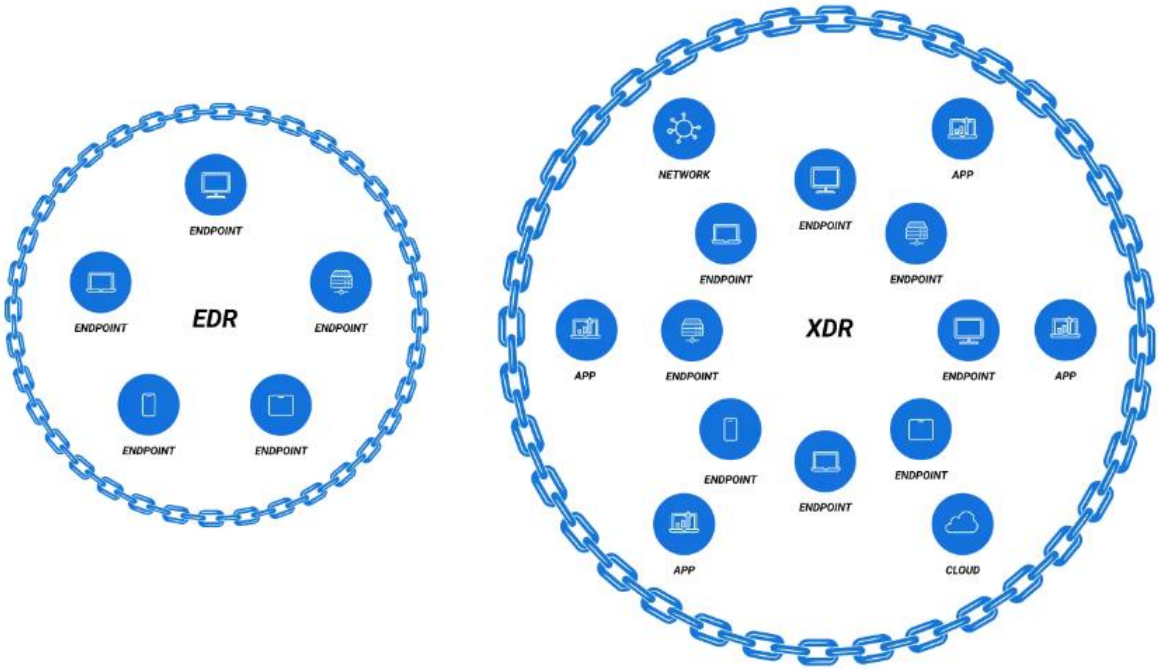

Рис. 4. Порівняння EDR і XDR [12]

Оцінюючи рішення для кінцевих точок, організації повинні враховувати свої конкретні потреби в безпеці та ресурси. Фактори, які слід враховувати, охоплюють:

- Розмір і складність мережі організації;
- Тип і обсяг конфіденційних даних, які необхідно захистити;
- Рівень ризику, пов'язаний з галуззю або географічним розташуванням організації;
- Бюджет і ресурси, доступні для операцій з кібербезпеки. [13]

Здатність забезпечити безпеку мережі також залежить від стійкості кінцевих точок. Віруси та зловмисні програми, які проникають на кінцеві точки, можуть стрімко розповсюджуватися по всій мережі, збільшуючи обсяг можливих атак. У цьому контексті важливим є використання антивірусного програмного забезпечення та захисту, які ефективно виявляють та усувають шкідливі програми, забезпечуючи надійний щит у боротьбі з кіберзагрозами.

Щоб досягти повного захисту, необхідно поєднувати технічні заходи зі стратегіями освіти персоналу. Спільне навчання користувачів про правила кібербезпеки та навички виявлення соціально-інженерних атак стає не менш важливим елементом системи захисту, адже багато загроз починаються саме з невірного поводження користувачів [14].

Однією з відомих сучасних технологій для захисту кінцевих точок є FortiManager. Це продукт американської компанії Fortinet, яка спеціалізується на розробці інтегрованих рішень для мережевої безпеки. FortiManager є центральним елементом в їхньому портфелі та використовується для управління та моніторингу Fortinet Security

Fabric. FortiManager надає інтерфейс для централізованого управління конфігураціями безпеки для всіх пристроїв Fortinet у мережі. Завдяки цьому продукту можна ефективно керувати великою кількістю пристроїв, що значно спрощує адміністрування великих мереж. Також він дозволяє централізовано керувати політикою безпеки на всіх пристроях Fortinet, забезпечуючи уніфікованість і спрощення адміністрування. Крім цього FortiManager забезпечує можливості моніторингу та створення звітів щодо активності в мережі, допомагаючи адміністраторам відстежувати й аналізувати події в реальному часі. FortiManager інтегрується з іншими продуктами Fortinet, такими як FortiGate (універсальні брандмауери), FortiAnalyzer (система аналізу та звітності) та інші, створюючи єдину безпечну інфраструктуру [15].

Ще одним відомим комплексним рішенням спрямованим на захист кінцевих точок у корпоративних мережах є Symantec Endpoint Security Complete від компанії Symantec. Цей продукт поєднує в собі різноманітні функції та технології для надійного захисту комп'ютерів та інших пристроїв у корпоративному середовищі. Symantec Endpoint Security Complete розроблено для задоволення потреб сучасних корпорацій щодо забезпечення високого рівня захисту та ефективне управління безпековими політиками. Рішення дозволяє виявляти і блокувати віруси, трояни, шкідливі програми та інші кіберзагрози. Також Symantec Endpoint Security Complete здійснює управління політикою безпеки для мобільних пристроїв, що дозволяє включати їх у загальну інфраструктуру захисту [16].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Кінцеві точки є не лише місцем загроз, але й вразливими об'єктами, де може відбутися витік конфіденційної інформації. Захист від цих загроз вимагає комплексного підходу, починаючи від встановлення сучасного антивірусного програмного забезпечення та завершуючи централізованим управлінням політикою безпеки.

Дослідження засвідчило важливість регулярних оновлень та патчів для усунення вразливостей, які можуть використовуватися зловмисниками. Врахування аспекту навчання персоналу та підвищення кібербезпекової грамотності користувачів є не менш важливим для підтримання безпеки системи в цілому.

Оскільки ландшафт кібербезпеки продовжує розвиватися, очікується, що XDR ставатиме все більш важливим компонентом загальних стратегій безпеки організацій, а нові технології, такі як штучний інтелект, машинне навчання та автоматизація, сприятимуть подальшим інноваціям у цій галузі. Оскільки кінцеві точки є популярним вектором атак з метою отримання доступу до мережі та чутливих активів, рішення EDR залишатимуться важливою частиною ефективних рішень XDR.

Symantec Endpoint Security Complete та FortiManager — це приклади інтегрованих рішень, що дозволяють керувати та моніторити безпеку кінцевих точок у корпоративних мережах. Їхні функції включають антивірусний захист, фаєрволи, управління політикою безпеки та багато іншого, забезпечуючи повноцінний захист на рівні кінцевих точок.

Отже, підтверджено необхідність централізованого та комплексного підходу до захисту кінцевих точок у сфері кібербезпеки, що має забезпечити ефективний захист від сучасних кіберзагроз та стати невід'ємною частиною загальної стратегії кібербезпеки. Тому, подолання цих викликів вимагає постійної уваги до нових технологій та стратегій у галузі кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hussain, A., Mark, W., & Toins, A. (2021). Endpoint Security: On the Frontline of Cyber Risk. *Community Banking Connection*, *(3).* https://www.communitybankingconnections.org/articles/2021/i3/endpoint-security-on-the-frontline-of-cyber-risk
2. Click Here to Kill Everybody. (n. d.). *Schneier on Security*. https://www.schneier.com/books/click-here/
3. A Framework for Cybersecurity Gap Analysis in Higher Education. (n. d.). *AIS eLibrary*. https://aisel.aisnet.org/sais2019/6/?utm_source=chatgpt.com
4. Richard Clarke's Cyberwar: File Under Fiction. (n. d.). *WIRED*. https://www.wired.com/2010/04/cyberwar-richard-clarke/?utm_source=chatgpt.com
5. Ostapov S.E., Yevseiev S. P., & Korol O. H. (2013). *Information security technologies*. HNEU. https://repository.hneu.edu.ua/handle/123456789/22547
6. Chiradeep BasuMallick. (2022). What Is Endpoint Detection and Response? Definition, Importance, Key Components, and Best Practices. *Spiceworks*. https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-edr/
7. What Is Endpoint Detection and Response (EDR). (n. d.). *Cisco*. https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html
8. What is XDR Explained? An overview of Extended Detection and Response Technology. (n. d.). *OpenEDR*. https://www.openedr.com/blog/xdr-explained/
9. Shaji George, A., Hovan George, A.s, Baskar, Dr T, & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions -Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. *IJARSCT,* 8(1), 493–501. https://doi.org/10.5281/zenodo.7028219
10. Makenzie Buenning (2024). EDR vs XDR: What's the Difference? *NinjaOne*. https://www.ninjaone.com/it-hub/endpoint-management/edr-vs-xdr-whats-the-difference/
11. XDR vs. EDR: Similarities, Differences, and How to Choose. (n. d.). *Cynet*. https://www.cynet.com/xdr-security/xdr-vs-edr/
12. Honcharova, L.L., Voznenko, A.D., Stasiuk, O.I., & Koval, Yu. O. (2013). Fundamentals of information security in telecommunication and computer networks. *State Economic and Technological University of Transport*. https://studfile.net/preview/9649827/
13. Central Network Management. (n. d.). *Fortinet*. https://www.fortinet.com/products/management/fortimanager
14. Symantec Endpoint Security Complete. (n. d.). *Broadcom*. https://www.broadcom.com/products/cybersecurity/endpoint/end-user/complete
15. Mykhailyshyn, D. A. (2022). Methods of detecting intrusions into computer networks. *Cybersecurity and computer-integrated technologies*, 68–69.
16. From EDR to XDR and Beyond: The Evolution of Endpoint Security. (n. d.). *Cisco*. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m05/from-edr-to-xdr-and-beyond-the-evolution-of-endpoint-security.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Diana Prymachenko
Asistant
State University of Information and Communication Technologies
ORCID ID: 0009-0003-2386-7440
primachenkodiana08@gmail.com

Nadiia Sviatska
Student
State University of Information and Communication Technologies
ORCID ID: 0009-0000-8132-9403
svyatskan@gmail.com

Sergii Goloborodko
Senior Lecturer
State University of Information and Communication Technologies
ORCID ID: 0009-0006-9892-3031
s.holoborodko@duikt.edu.ua

Mykhailo Nedodai
Graduate Student
State University of Information and Communication Technologies
ORCID ID: 0009-0000-0876-9971
c13h21n3o10@gmail.com

Oleksandr Diachuk
Graduate Student
State University of Information and Communication Technologies
ORCID ID: 0009-0006-5585-6393
realjewua@gmail.com

EDR AND XDR AS THE MAIN ENDPOINT SECURITY TECHNOLOGIES

Abstract. The article analyzes the role of Endpoint Security as a key element of modern IT infrastructures, which plays a key role in countering cyber threats at the initial stage of attacks. Traditional tools, such as EPP (Endpoint Protection Platform), which are based on signature analysis and blocking known threats, are considered. A detailed review of EDR (Endpoint Detection and Response) highlights its advantages: continuous real-time monitoring of endpoint activities, the use of machine learning to identify anomalies, and behavioral analytics to detect suspicious activity. EDR provides not only detection, but also automated response mechanisms: blocking suspicious activities, isolating devices from the network, and removing malicious code. XDR (Extended Detection and Response) is presented as an evolutionary development of EDR, where data analysis takes place at the level of the entire infrastructure. The technology aggregates information from endpoints, network sensors, cloud services, email, and SIEM systems to provide a comprehensive view of threats. XDR automates the correlation of events, detects complex attacks that span different network segments, and accelerates response through centralized management (e.g., simultaneously blocking threats in different environments). A comparison of EDR and XDR demonstrates that the latter eliminates the fragmentation of tools, provides a single interface for monitoring, and reduces the operational burden on security teams. Examples of technology implementation are described below: FortiManager, a tool for centralized management of security policies, configuration of firewalls, monitoring events in different network segments, and coordination of EDR solutions; Symantec Endpoint Security Complete, a platform that combines EDR, antivirus protection, application control, data encryption, and protection against exploits, providing multi-level protection for corporate devices.

Keywords: endpoint protection; cybersecurity; security tools; network security; endpoint protection technologies; XDR; EDR; Fortinet; Symantec; cyberattack.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Hussain, A., Mark, W., & Toins, A. (2021). Endpoint Security: On the Frontline of Cyber Risk. *Community Banking Connection*, *(3)*. https://www.communitybankingconnections.org/articles/2021/i3/endpoint-security-on-the-frontline-of-cyber-risk
2. Click Here to Kill Everybody. (n. d.). *Schneier on Security*. https://www.schneier.com/books/click-here/
3. A Framework for Cybersecurity Gap Analysis in Higher Education. (n. d.). *AIS eLibrary*. https://aisel.aisnet.org/sais2019/6/?utm_source=chatgpt.com
4. Richard Clarke's Cyberwar: File Under Fiction. (n. d.). *WIRED*. https://www.wired.com/2010/04/cyberwar-richard-clarke/?utm_source=chatgpt.com
5. Ostapov S.E., Yevseiev S. P., & Korol O. H. (2013). *Information security technologies*. HNEU. https://repository.hneu.edu.ua/handle/123456789/22547
6. Chiradeep BasuMallick. (2022). What Is Endpoint Detection and Response? Definition, Importance, Key Components, and Best Practices. *Spiceworks*. https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-edr/
7. What Is Endpoint Detection and Response (EDR). (n. d.). *Cisco*. https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html
8. What is XDR Explained? An overview of Extended Detection and Response Technology. (n. d.). *OpenEDR*. https://www.openedr.com/blog/xdr-explained/
9. Shaji George, A., Hovan George, A.s, Baskar, Dr T, & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions -Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. *IJARSCT*, 8(1), 493–501. https://doi.org/10.5281/zenodo.7028219
10. Makenzie Buenning (2024). EDR vs XDR: What's the Difference? *NinjaOne*. https://www.ninjaone.com/it-hub/endpoint-management/edr-vs-xdr-whats-the-difference/
11. XDR vs. EDR: Similarities, Differences, and How to Choose. (n. d.). *Cynet*. https://www.cynet.com/xdr-security/xdr-vs-edr/
12. Honcharova, L.L., Voznenko, A.D., Stasiuk, O.I., & Koval, Yu. O. (2013). Fundamentals of information security in telecommunication and computer networks. *State Economic and Technological University of Transport*. https://studfile.net/preview/9649827/
13. Central Network Management. (n. d.). *Fortinet*. https://www.fortinet.com/products/management/fortimanager
14. Symantec Endpoint Security Complete. (n. d.). *Broadcom*. https://www.broadcom.com/products/cybersecurity/endpoint/end-user/complete
15. Mykhailyshyn, D. A. (2022). Methods of detecting intrusions into computer networks. *Cybersecurity and computer-integrated technologies*, 68–69.
16. From EDR to XDR and Beyond: The Evolution of Endpoint Security. (n. d.). *Cisco*. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m05/from-edr-to-xdr-and-beyond-the-evolution-of-endpoint-security.html