КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2(22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.5467
УДК 004.89

Легомінова Світлана Володимирівна
доктор економічних наук, професор, завідувач кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Гайдур Галина Іванівна
доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпеки
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID 0000-0003-0591-3290
gaydurg@gmail.com

АНАЛІЗ СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ОРГАНІЗАЦІЙ ТА ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ ПЛАТФОРМИ ПРОТИДІЇ ЇМ

Анотація. Враховуючи процес ускладнення геополітичного та геоекономічного ландшафтного простору, розвитку інформаційних технологій та формування нових викликів безпеці, що пов'язані з появою нових кіберзагроз, виникає необхідність постійного моніторингу та прогнозування їх з метою запобігання наслідків в вигляді пошкодження та витоку цінної та конфіденційної інформації. Авторами проаналізовано нові прогнозовані загрози кібербезпеці організаціям, особлива увага приділена захисту кінцевих точок. Виявлено загрози у сфері розвитку штучного інтелекту (підпільна розробка шкідливих великих мовних моделей (LLM); оновлення «Script Kiddies»; голосове шахрайство для соціальної інженерії, яке створене штучним інтелектом); зміни тенденцій у поведінці суб'єктів загрози (атаки на ланцюги поставок проти рішень керованої передачі файлів, загрози зловмисного програмного забезпечення, які стають полімовними); як нових виникаючих загроз та методів атак (зростаюче суперництво QR кодів; прихованих атак на периферійні пристрої; впровадження Python в Excel, що створює потенційно новий вектор для атак; драйвери LOL, які змінюють алгоритми дій). Результируючим виявленню майбутніх загроз акцентовано на необхідності стратегічного планування впровадження нових технологій та платформ: як-от функції виявлення та реагування на кінцеві точки (EDR), також використання EDR як частину багатоінструментальної архітектури розширеного виявлення та реагування (XDR). Доведено, що дослідження Gartner мають колосальний вплив на покращення можливостей організацій з виявлення загроз, надаючи цінну інформацію про сильні та слабкі сторони кожного постачальника послуг кібербезпеки щодо інформації по виявленню нових загроз, шляхом зосередження уваги організацій на можливості виявлення прогалин в існуючій інфраструктурі безпеки та прийнятті обґрунтованих рішень щодо інвестування в додаткові рішення чи послуги, які ефективно усувають ці прогалини. Проаналізовано сфери діяльності світових компаній-лідерів, знайдено їх зв'язок з українськими компаніями та запропоновано подальше співробітництво для ефективного захисту національного кіберпростору.

Ключові слова: загрози; кібербезпека; кінцеві точки; квадрант Gartner; стратегічне планування.

ВСТУП

Сфера кібербезпеки отримує все більш вимогливі виклики до відбиття загроз кіберпростору, що спричинені змінами подій у геополітичному та геоекономічному ландшафтному просторі. Одночасно набувають розвитку нові загрози, а також з'являються нові актори та гравці у всьому світі, що продукують нові способи використання або застосування старих тактик і підходів, відбувається комплементарне

співробітництво на інтегрованих платформах, яке мотивовано досягненням єдиної мети в політичній або економічній площині. Тому перманентний моніторинг кіберзагроз є реальним викликом сьогодення.

Рушієм інноваційного розвитку кіберзагроз є вирішення геостратегічних амбіцій світових рівнів, де використовуються дезінформація, шпигунство, розбалансування процесів, що викликає загрози в сферах цивільної життєдіяльності та правовому полі.

Особливого занепокоєння викликає швидка еволюція програм-вимагачів, які ускладнюються за структурою та функціями, стають більш масштабними, що обумовлено об'єднанням зусиль зацікавлених суб'єктів їх продукування, які застосовують платформи для обговорення через приховані форуми. Тому ідентифікація загроз ускладнюється, а інструменти безпеки мають бути більш унікальними.

Постановка проблеми. Проблематика захисту кіберпростору набуває актуальності в відповідності з бурхливим розвитком інформаційних технологій та інтегруванням інформаційних платформ різних сфер активності, а також з одночасною зацікавленістю сторонніх осіб порушити периметр захисту пулів цінної та конфіденційної інформації, керуючись мотивацією політичного або економічного змісту. Це спонукає компанії у сфері кібербезпеки знаходити нові способи за засоби, продукувати нові технології, щоб протистояти сучасним кібервикликам.

Аналіз останніх досліджень і публікацій. Умовою успішного функціонування інформаційних систем організацій являється ефективний захист від кібератак зловмисників, тому організаціям необхідно проводити постійний моніторинг інноваційних рішень на світовому на національному рівні у сфері кібербезпеки, щоб мати об'єктивну оцінку поточного рівня інформаційної безпеки. Проблематиці даної сфери приділяють увагу низка дослідницьких організацій, компанії світового рівня, науковці. Існує велика кількість публікацій з рекомендаціями та пропозиціями впровадження технологій захисту, особливу увагу заслуговують дослідження й пропозицій, які вирішуються за допомогою Endpoint Detection and Response (EDR) [15]. Але проблематика захисту інформаційних систем потребує більш системного вивчення передумов формування загроз та комплексних шляхів вивчення інформаційного контенту для продукування рішень. Авторами запропоновано дослідження, яке дозволило структурувати напрями очікуваних загроз й аналіз можливостей та здатностей компаній протидіяти кіберзагрозам та кібератакам.

Мета статті. Розкрити основні загрози кібербезпеки на найближчій час. Провести аналіз діяльності компаній-лідерів світу за рейтинговими оцінками, сформувати бачення на транслювання впливу цих компаній на ринок компаній з кібербезпеки України, що надасть змогу виявити проблемні місця та зорієнтуватися в релевантному напрямі розвитку їх співпраці.

МЕТОДИКА ДОСЛІДЖЕННЯ

Цифровізація проникає у всі сфери нашого життя: політику, економіку, медицину, освіту, тому проблематика управління якістю цих процесів, а також захист їх кіберпростору не втрачає своєї актуальності, а навпаки набирає обертів. В межах нашого дослідження було використано декілька наукових підходів, які дозволили описати ключові аспекти формування системного бачення загроз інформаційної безпеки з метою вчасного знаходження релевантних інструментів захисту кіберпростору організації.

Методологічними засадами статті слугував аналіз щорічних та щомісячних моніторингових досліджень рейтингових агентств та провідних комерційних компаній

надання послуг у сфері кібербезпеки, а також авторське компаративне дослідження, яке дозволило виділити основні компанії-лідери на ринку кібербезпеки.

Отже, методологічна база дозволила підтвердити практично теоретичні припущення щодо особливостей засобів та методів захисту периметру організації та забезпечення необхідного рівня кібербезпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Експерти з кібербезпеки та дослідники загроз із команди Trellix Advanced Research Center зібрали свої прогнози щодо тенденцій, тактик і загроз, про які організаціям слід пам'ятати напередодні 2024 року [1]:

Загроза штучного інтелекту:

- Підпільна розробка шкідливих великих мовних моделей (LLM);
- Воскресіння «Script Kiddies»;
- Голосове шахрайство для соціальної інженерії, створене Штучним Інтелектом (ШІ).

Зміна тенденцій у поведінці суб'єктів загрози:

- Атаки на ланцюги поставок проти рішень керованої передачі файлів;
- Загрози зловмисного програмного забезпечення стають «поліглотом»;

Виникаючі загрози та методи атак:

- Викриття тихого сплеску інсайдерських загроз;
- Зростаюча битва за (QR) коди;
- Прихований напад на периферійні пристрої;
- Python в Excel створює потенційно новий вектор для атак;
- Драйвери LOL змінюють правила гри.

Однією з розробок сфери штучного інтелекту являються великі мовні моделі (LLM), які генерують текст, демонструючи надзвичайний технологічний потенціал як для позитивних застосувань, так й для зловмисного використання. Як-от GPT-4, Claude і PaLM2 представляють потужний та ефективний інструмент, який усуває потребу у великому досвіді, часі та ресурсах, але може використовуватись за різними спрямуваннями.

Як загрозу можна визначити можливість створення масштабних фішингових кампаній з використанням FraudGPT і WormGPT.

«Script Kiddies» з'явився з появою в вільному доступі безкоштовного програмного забезпечення, що спровокувало велику кількість зацікавлених осіб до активного застосування вже існуючих автоматизованих інструментів, сценаріїв до здійснення кібератак. ChatGPT, Bard або Perplexity AI, мають механізми безпеки, які запобігають написанню шкідливого коду [3], але існують інструменти, які можуть бути використані злочинцями. Доступ до цих можливостей може спонукати до написання шкідливих кодів, створення глибоких фейкових відео, допомогти скористатись можливостями соціальної інженерії.

Генерування штучним інтелектом голосових повідомлень [4] має створювати значні ризики в практиці психологічного маніпулювання свідомістю об'єктів впливу на площині соціальної інженерії (як-от здійснення фінансових операцій на користь іншої особи).

Рішення для керованої передачі файлів (MFT), призначені для безпечного обміну конфіденційними даними між об'єктами, за своєю суттю містять скарбницю конфіденційної інформації. Це варіюється від інтелектуальної власності, даних клієнтів, фінансових записів і багато іншого. Рішення MFT відіграють вирішальну роль у сучасних бізнес-операціях, і

організації значною мірою покладаються на них для полегшення безперебійного обміну даними як всередині, так і ззовні. Будь-який збій або компрометація цих систем може призвести до значного простою в роботі, пошкодженню репутації та виникненню фінансових втрат [5]. Тому, як дуже приваблива ціль розглядається розробниками програм-вимагачів, що слід враховувати як мотивовану загрозу.

Складність систем MFT та їх інтеграція у внутрішню бізнес-мережу часто створює слабкі місця в безпеці та вразливості. Так, група CL0P використовує рішення Go-anywhere MFT і злам MOVEit, перетворивши один успішний експлойт на серйозний глобальний злом у ланцюжку постачання програмного забезпечення [5]. Націлюють свою діяльність групи CL0P на великі компанії у фінансовій, виробничій та медійної сферах.

Програмне забезпечення-вимагач зазвичай поширюється через шкідливі вкладення електронної пошти, шкідливі веб-сайти та шкідливі посилання. Оператори програм-вимагачів CL0P також використовують відомі вразливості, зокрема Accellion FTA та «ZeroLogon».

Прикладами компаній, які постраждали від програми-вимагача CL0P, є енергетичний гігант Shell, фірма з кібербезпеки Qualys, гігант супермаркетів Kroger і численні університети по всьому світу, такі як Університет Колорадо, Університет Маямі, Стенфордська медицина, Університет Меріленда в Балтіморі (UMB), і Каліфорнійський університет. Сервери всіх цих компаній Accellion FTA були зламані групою програм-вимагачів CL0P, що призвело до втрати конфіденційної інформації та порушення їхньої роботи. За даними Mandiant у середині грудня 2020 року UNC2546 використовував чотири вразливості нульового дня в пристроїв передачі файлів Accellion (FTA). Чотири вразливості, усі з яких зараз виправлено, це: CVE-2021-27101, CVE-2021-27102 , CVE-2021-27103 і CVE-2021-27104 [7].

CL0P також має деякі унікальні особливості, які роблять його особливо небезпечним. Наприклад, він здатний поширюватися через мережу, що означає вірогідність заразити кілька комп’ютерів одночасно. Програми-вимагачі CL0P часто використовують цифрові підписи, щоб уникнути певних заходів безпеки кінцевих точок. Крім того, він здатний видаляти точки відновлення системи Windows, що ще більше ускладнює процес відновлення [7].

Отже, організаціям рекомендується ретельно обирати їх рішення для керованої передачі файлів, запровадити рішення DLP і зашифрувати конфіденційні дані, щоб захистити себе [5].

Розробки шкідливого програмного забезпечення починають активно використовувати мови Golang, Nim і Rust, що дозволяє швидко та продуктивно створювати складне шкідливе програмне забезпечення, що враховуючі відносну новизну цих мов, відображається на відсутності комплексних інструментів аналізу для цих мов, можливостей існуючих інструментів безпеки не вистачає.

Одним з інструментів фішингових кампаній на сьогодні слугують QR-коди, які часто використовуються в силу об’єктивних причин необхідності здійснення безконтактних платежів, або іншої активності, яка з’явилась під впливом пандемії COVID-19. Загроза фішингу, орієнтованого на QR-код, буде зростати, що вимагає від користувачів обережності під час сканування кодів, особливо з невідомих або підозрілих джерел.

Ландшафт загроз починає зосереджуватись на сфері периферійних пристроїв, а саме: брандмауєрах, маршрутизаторах, VPN, комутаторах, мультиплексорах та шлюзах, які не здатні виявляти вторгнення. Шлюзи в наш цифровий світ за задумом є першою та останньою лінією захисту. Це робить їх і ціллю, і сліпою зоною, враховуючі різноманіття архітектур периферійних пристроїв [8]. Тому нова реальність — недостатньо вивчені вразливості в наших шлюзах, маршрутизаторах і VPN, що створює необхідність розробки нових інструментів кіберзахисту.

Існування вразливих драйверів становлять значну загрозу, вони використовуються для виведення з ладу рішень безпеки на самих ранніх стадіях атаки. Під час таких атак зловмисники скидають на пристрої жертв драйвери, з маркуванням сертифікованого, що здатні працювати з привілеями ядра, успішна експлуатація дозволяє зловмисникам досягти ескалації привілеїв на рівні ядра, що надає їм найвищий рівень доступу та контролю над системними ресурсами атакуємого об'єкта. Прикладом таких атак являється проєкт ZeroMemoryEx Blackout, інструмент The Terminator від Spyboy та інструмент AuKill — це приклади використання вразливих драйверів для обходу засобів контролю безпеки та виконання шкідливого коду. Існують певні функції та ініціативи для захисту від цієї атаки, такі як Vulnerable Driver Blocklist від Microsoft та проект LOL Drivers. Однак, це не змінює того факту, що ці атаки легко і просто виконуються, з підвищеною ймовірністю успішного зараження і більшою доступністю вразливих драйверів [10].

Акцентування на захисті кінцевих точок формування релевантних платформ захисту кінцевих точок (EPP), досягається розгортанням агентів або датчиків для захисту керованих кінцевих точок, включаючи настільні ПК, портативні ПК, сервери та мобільні пристрої. EPP призначені для запобігання ряду відомих і невідомих зловмисних атак. Крім того, вони надають можливість розслідувати та виправляти будь-які інциденти, які уникають контролю захисту.

Компанії для нівелювання атак зловмисників або їх купірування знаходяться у постійному пошукі ефективних рішень для боротьби у кіберпросторі. Враховуючи, що виявлення кінцевих точок і реагування (EDR) інтегровано в EPP і розвивається в розширене виявлення та реагування (XDR), увага має бути зосереджена на інтеграцію з операціями безпеки.

В межах припущення стратегічного планування визначаються певні напрями впровадження.

До кінця 2025 року 80% організацій типу C отримають функцію виявлення та реагування на кінцеві точки (EDR) як послугу керованого виявлення та реагування (MDR).

До кінця 2025 року понад 50% організацій типу B консолідують EDR у портфоліо пріоритетних постачальників інвестицій у безпеку для більш ефективних операцій безпеки.

До кінця 2026 року 80% організацій типу A використовуватимуть EDR як частину багатоінструментальної архітектури розширеного виявлення та реагування (XDR) [11].

Американська дослідницька та консалтингова компанія Gartner, яка щорічно формує дослідницькі звіти рейтингової оцінки сегментів ринку інформаційних технологій у форматах «магічний квадрант», використовує методику, яка основі на експертних оцінок передбачає будову двох лінійних шкал: повнота бачення (англ. completeness of vision) та здатність реалізації (ability to execute). Ці два критерії графічно формують чотири квадранти площини, які називаються:

- «лідери» (leaders) — постачальники з позитивними оцінками як «повноти бачення», так і «здатності реалізації»;
- «претенденти» (challengers) — постачальники з позитивними оцінками тільки за «здатністю реалізації»;

– «провидці» (visionaries) — постачальники з позитивними оцінками тільки по «повноті бачення»;
– «Нішеві гравці» (niche players) — постачальники з негативними оцінками за обома критеріями.

Gartner називає «магічним квадрантом» (за алюзією на магічний квадрат) звіт з аналізом будь-якого сегмента ринку, який включає зображення з розподілом постачальників за зазначеними чвертями; щорічно компанія випускає кілька десятків магічних квадрантів на регулярній основі. Постачальники іноді відзначають навіть сам факт потрапляння до будь-якої магічний квадрант окремим прес-релізом як визнання ринкових досягнень, навіть якщо компанія згадана лише у квадранті «нішевих гравців» [12].

За результатами проведеного дослідження Gartner за 2022 рік магічний квадрант має вигляд (рис.1).

За результатами досліджень Gartner у 2022 році в квадранті «Лідери» зафіксовані компанії: Microsoft, CrowdStrike, SentinelOne, Cybereason, Trend Micro, Sophos; у квадранті «Провидці» — ESET; у квадранті «Претенденти» — компанії: Cisco, Palo Alto Networks, Broadcom (Symantec), VMware, Fortinet. Отже, представники квадранта «Лідерів» формують тренди технологій захисту кінцевих точок та їх розповсюдження. Представники квадранта «Претенденти» здатні активно впроваджувати технології.

Магічний квадрант Gartner XDR (розширене виявлення та реагування) — це комплексна оцінка постачальників у галузі кібербезпеки. Він оцінює їхні можливості у виявленні, дослідженні та реагуванні на загрози в багатьох джерелах даних, включаючи кінцеві точки, мережі, програми та хмарні середовища. Квадрант поділяє постачальників на чотири категорії: Лідери, Претенденти, Провидці та Нішеві гравці. Це графічне представлення допомагає організаціям швидко визначити найкращих виконавців на ринку [14].

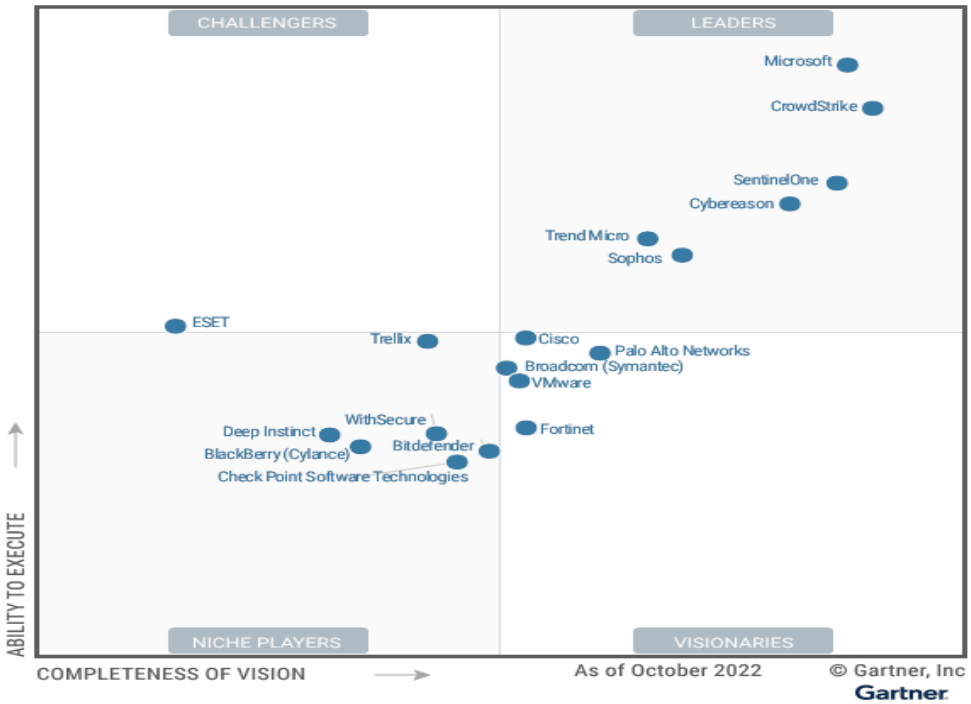

Рис. 1. Магічний квадрант Gartner для платформ захисту кінцевих точок 2022 [15]

Дослідження Gartner мають колосальний вплив на покращення можливостей організацій з виявлення загроз, надаючи цінну інформацію про сильні та слабкі сторони кожного постачальника послуг кібербезпеки щодо інформації по виявленню нових загроз. Таким чином, вони зосереджують увагу організацій на можливості виявити прогалини в існуючій інфраструктурі безпеки та прийняти обґрунтовані рішення щодо інвестування в додаткові рішення чи послуги, які ефективно усувають ці прогалини.

В області реагування на інциденти вивчення систематизованого досвіду дозволяє підвищити ефективність за рахунок розробки надійного плану реагування на інциденти для мінімізації збитків і часу відновлення.

Оцінка постачальників магічним квадрантом Gartner здійснюється й за критерієм їх здатності швидко й ефективно розслідувати загрози та реагувати на них.

Постачальники-лідери мають доступ до потужних інструментів і технологій, які оптимізують процеси реагування на інциденти. Рішення їх часто інтегруються з існуючою інфраструктурою безпеки, дозволяючи групам безпеки співвідносити сповіщення з багатьох джерел, автоматизувати дії реагування та скорочувати час, потрібний для виявлення та усунення загроз [14].

Створення стратегічних планів безпеки для організацій відбувається в відповідності до розуміння мінливого ландшафту загроз та оцінюючи довгострокове бачення та стратегію постачальників, організації можуть відповідним чином узгодити свої ініціативи щодо безпеки. В основі стратегічних планів полягають інноваційні підходи або проривні технології, які можуть суттєво вплинути на стан безпеки організації.

Gartner змінив підхід організацій до стратегій кібербезпеки. Надаючи цінну інформацію про можливості постачальників щодо виявлення загроз, ефективності реагування на інциденти та довгострокової стратегії, це дає можливість організаціям приймати обґрунтовані рішення при виборі рішень для кібербезпеки. Оскільки ландшафт загроз продовжує швидко розвиватися, використання таких ресурсів, як XDR Magic Quadrant від Gartner, стає все більш важливим для того, щоб випередити кіберсупротивників і захистити конфіденційні дані [14].

Компанії потребують передових рішень для захисту кінцевих точок від атак і злому. Хоча EDR став стандартом, XDR став наступним еволюційним кроком. UES, DaaS, ASCA, EASM, BAS, EM, ITDR, EAI та AMTD — це передові технології, які надають нові погляди та підходи до XDR [13].

Hype Cycle від Gartner ілюструє найактуальніші інновації в просторі безпеки кінцевих точок, щоб допомогти лідерам безпеки в плануванні впровадження та впровадження нових технологій. Інновації в галузі безпеки кінцевих точок зосереджені на швидшому автоматизованому виявленні та запобіганні загрозам, а також на усуненні загроз, що забезпечує інтегроване розширене виявлення та реагування (XDR) для кореляції точок даних і телеметрії з таких рішень, як кінцева точка, мережа, Інтернет, електронна пошта та ідентифікація. Методи забезпечення легкого, безпечного, віддаленого доступу залишаються затребуваними, керуючи робочим столом як послугою (DaaS) та ізоляцією кінцевої точки та браузера для посиленого контролю та безпеки. Актуальним залишається активне впровадження мережі з нульовою довірою [13].

У таблиці 1 представлено світові компанії-лідери у сфері кібербезпеки кінцевих точок, а також їх взаємозв’язок з українськими компаніями, які є партнерами або використовують запропоновані технології захисту кінцевих точок.

Таблиця 1

Світові компанії-лідери у сфері кібербезпеки кінцевих точок

Світова компанія	Місце у квадранті Гартнера		Загрози, на яких спеціалізується компанія	Компанія-партнер в Україні
	2021 [18]	**2022** [15]		
Microsoft [19], [20]	Leaders	Leaders	• захист від вірусів, троянців, шпигунського ПЗ та інших форм шкідливого програмного забезпечення; • захист від атак на основі вразливостей у програмному забезпеченні; • заходи для захисту від атак типу DDoS; • системи аутентифікації та авторизації для захисту від несанкціонованого доступу; • шифрування даних для забезпечення конфіденційності та цілісності; • управління доступом до даних та захист від витоку інформації; • захист від вірусів, спаму та інших загроз електронної пошти; • захист даних, що зберігаються та обробляються в хмарних сервісах Microsoft Azure; • моніторинг та виявлення аномальних активностей, а також реагування на інциденти безпеки; • надання користувачам оновлень та патчів для усунення вразливостей у програмному забезпеченні.	**ELKO** https://partner.microsoft.com/ru-ua/solutions/genuine-partner-oem-cds
CrowdStrike [21]	Leaders	leaders	• Zero-Day Exploits • Advanced Persistent Threats • Insider Threats • Cyberattacks	**INTELLIGENT IT DISTRIBUTION** https://iitd.com.ua/en/crowdstrike/
SentinelOne [22]	Leaders	leaders	• виявлення та блокування вірусів, троянських коней, черв'яків та інших видів шкідливих програм; • захист від атак ransomware, які зашифровують файли користувача та вимагають викуп; • використовує технології машинного навчання для виявлення нових атак, які ще не були відомі або документовані; • безпека комп'ютерів та інших кінцевих точок, які можуть бути точкою входу для атак; • допомога в ідентифікації, відслідковуванні та відновленні після кіберінцидентів; • моніторинг та реагування на загрози миттєво для забезпечення ефективного захисту.	**BAKOTECH**
Cybereason [23]	Visionaries	leaders	• malware attacks • malicious code • ransomware activities	Немає на ринку України
Trend Micro [24]	Leaders	leaders	• виявлення та блокування вірусів, троянів, черв'яків та інших шкідливих програм; • проактивне виявлення та блокування вірусів-викрадачів, які шифрують дані та вимагають викуп;	**SEETON ELKO IT Dialog CBIT IT** https://www.trendmicro.com/ru_ru/partners/find-a-partner.html

			• виявлення та блокування фішингових атак, шкідливих посилань у електронних листах та на веб-сайтах; • управління доступом до програм та пристроїв, що допомагає уникнути неповноважного використання ресурсів; • захист обчислювальних ресурсів у хмарних середовищах від різноманітних кіберзагроз; • захист підключених до Інтернету речей від можливих кіберзагроз; • моніторинг та аналіз кіберзагроз для вчасного виявлення та реагування на нові загрози; • заходи безпеки для ефективного захисту критичних систем та інфраструктури від кібератак.	
Sophos [25]	Leaders	leaders	• Generic miner • Generic adware • Remote-access Trojan • Browser (search) hijacking	**SMART NETWORK DISTRIBUTION** https://partners.sophos.com/english/directory/search?f0=Technical+Accreditations&f0v0=Endpoint+and+Server+Partner&country=Ukraine
McAfee [26]	Leaders	-	• Smishing for malware • SMS spy • Malicious code • Fake cryptocurrency mining service	**CBIT IT** https://elioplus.com/europe/ukraine/channel-partners/mcafee
Cisco [27]	visionaries	visionaries	• захист мережевих інфраструктур від кіберзагроз; • розробка інфраструктури мережі; • розробка рішень для хмарних обчислень та хмарних сервісів; • активно працює у сфері Інтернету речей, розробляючи технології для збору, обробки та аналізу даних від підключених пристроїв; • розробка інструментів для аналізу великих обсягів даних (Big Data) та надання відповідних рішень для обробки та інтерпретації цих даних; • постачає рішення для покращення комунікацій та співпраці в організаціях.	**IT Dialog** **IT SPECIALIST** **SEETON** https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/pf/index.jsp#/
Palo Alto Networks [28]	-	visionaries	• експлуатація вразливостей у мережевому обладнанні та пристроях; • атаки на рівні мережі, такі як DDoS, атаки на перехоплення трафіку, вторгнення в систему та інші; • захист конфіденційних даних від втрати, витоку чи несанкціонованого доступу; • захист хмарних інфраструктур; • захист від шкідливих програм, антивіруси, захист електронної пошти і інші методи захисту від загроз, які можуть виникнути через користувачів; • захист від загроз, пов'язаних з підключеними пристроями Інтернету речей (IoT); • контроль і моніторинг доступу до ресурсів та інфраструктури;	**WISE IT** **ESKA** **SEETON** https://locator.paloaltonetworks.com/

			• використання аналізу поведінки для виявлення нестандартних або підозрілих активностей.	
Broadcom (Symantec) [29]	visionaries	vision aries	• антивірусні програми; • засоби виявлення і запобігання загрозам; • інструменти безпеки для кінцевих точок • Code Red • Nimda • Bugbear	**WISE IT** https://wiseit.com.ua/en/partners/
VMware [30]	visionaries	vision aries	• забезпечення безпеки віртуальних інфраструктур, підвищення стійкості до кібератак, виявлення та усунення загроз; • забезпечення високого рівня доступності, надійності та відновлення послуг у віртуальних середовища; • забезпечення конфіденційності, цілісності та доступності даних, які обробляються та зберігаються в віртуальних областях; • забезпечення конфіденційності, цілісності та доступності даних, які обробляються та зберігаються в віртуальних областях; • захист віртуальних машин, мереж та інших елементів віртуалізованого середовища; • забезпечення ефективного та безпечного управління доступом до віртуальних ресурсів; • забезпечення безпеки та продуктивності віртуальних робочих столів.	**SEETON** **WISE IT** **INTELLIGENT IT DISTRIBUTION** **IT SPECIALIST** https://partnerlocator.vmware.com/#sort=relevancy&f:@sfaccountcountryc=[UKRAINE]
Fortinet [31], [32]	niche players	vision aries	• розробляє і виробляє брандмауери, які забезпечують захист мережі від несанкціонованого доступу та шкідливих атак; • виявлення та блокування вірусів, троянських програм, шкідливих файлів та інших загроз; • розробка VPN-рішень, які забезпечують безпечний та шифрований зв'язок для віддалених працівників та філіалів; • засоби контролю за витоком конфіденційної інформації та забезпечення її безпеки; • захист від атак на веб-застосунки, включаючи захист від SQL-ін'єкцій, кросс-сайтового скриптингу та інших атак на веб-застосунки; • виявлення та захист від ускладнених загроз, таких як цільовані атаки та атаки з використанням невідомих уразливостей; • захист хмарних інфраструктур та сервісів.	**IT SPECIALIST** **WISE IT** https://partnerportal.fortinet.com/directory/search?l=Ukraine

Джерело: сформовано авторами на основі [15], [18] – [32].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, проаналізовані загрози майбутнього періоду дали змогу зрозуміти, що новий підхід для забезпечення ефективного захисту кіберпростору організації передбачає більш системного бачення на загрози та вимагає застосування інноваційних технологій та інтегрованих платформ співпраці між компаніями-лідерами в розрізі глобальних

розробок та ліцензійному використанні. Перспективи подальших досліджень будуть зосереджені на більш детальному вивченні особливостей майбутніх загроз та пошуки інструментів забезпечення ефективного інформаційного захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Trellix 2024 Threat Predictions*.(2023). https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
2. Tripathi, S. *Underground Development of Malicious LLMs*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
3. Ajeeth, S. *The Resurrection of Script Kiddies*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
4. Pena, R. *AI-generated Voice Scams for Social Engineering*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
5. Fokker, J. *Supply Chain Attacks Against Managed File Transfers Solutions*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
6. Provecho, E. *Malware Threats are Becoming Polyglot*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
7. *CLOP*. SentinelOne. https://www.sentinelone.com/anthology/clop/
8. Phuc, P. *The Stealthy Assault on Edge Devices*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
9. Kersten, M. *Python in Excel Creates a Potential New Vector for Attacks*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
10. Chandra, A. *LOL Drivers Are Becoming a Game Changer*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
11. Firstbrook, P.,& Silva, C. *Magic Quadrant for Endpoint Protection Platforms*. https://assets.sentinelone.com/eval/gartner-mq-22?xs=486596
12. *Gartner Magic Quadrant*. https://webcitation.org/691VWPAM8?url=http://www.workengine.com/Company/SitePages/Market%20Recognition.aspx
13. *Hype Cycle for Endpoint Security*. (2023). Gartner Research. https://www.gartner.com/en/documents/4589999
14. *The Impact of Gartner's XDR Magic Quadrant on Cybersecurity Strategies*. (2023). Ask. https://www.ask.com/news/impact-gartner-s-xdr-magic-quadrant-cybersecurity-strategies?utm_content=params%3Aad%3DdirN%26qo%3DserpIndex%26o%3D740004%26ag%3Dfw10&ueid=D7A48E0A-AB46-4B4A-858B-EA9CFA50E92E
15. *Magic Quadrant for Endpoint Protection Platforms*. (2022). Gartner. https://www.gartner.com/doc/reprints?id=1-2AJ91JO6&ct=220707&st=sb&culture=ru-ru&country=ru
16. Штонда, Р., Черниш, Ю., Мальцева, І., Чайка, Є., & Поліщук С. (2023). Практичні підходи до кіберзахисту мобільних пристроїв за допомогою рішення endpoint detection and response. *Кібербезпека: освіта, наука, техніка, 1(21)*, 17–29.
17. *Endpoint Protection Platforms. Reviuwes and Ratings.* Gartner. https://www.gartner.com/reviews/market/endpoint-protection-platforms
18. *Gartner named Microsoft a Leader in the 2021 Endpoint Protection Platforms (EPP) Magic Quadrant*. (2021). https://www.microsoft.com/en-us/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/
19. *Microsoft Digital Defense Report*. (2021). https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
20. *Microsoft Digital Defense Report 2022 Executive Summary*. (2022). https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bcRe?culture=uk-ua&country=ua
21. *2023 Global threat report.* (2023) https://iitd.com.ua/wp-content/uploads/2023/03/crowdstrike2023globalthreatreport.pdf
22. *Annual Report and Form 10K*. (2022). https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_S_2022.pdf
23. *Cybereason*. (2023). https://research.contrary.com/reports/cybereason
24. *Rethinking Tactics 2022 Annual Cybersecurity Report.* (2022). https://documents.trendmicro.com/assets/rpt/rpt-rethinking-tactics-annual-cybersecurity-roundup-2022.pdf
25. *Maturing criminal marketplaces present new challenges to defenders. Sophos 2023 Threat Report*. (2023). https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf

26. *The McAfee Consumer Mobile Threat Report*. (2022). https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2022.pdf
27. *2022 Annual Report Reimagining the future of connectivity*. (2022). https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf
28. *Annual Report & Proxy Statement.* (2022). https://investors.paloaltonetworks.com/static-files/137ede42-9e7b-4eac-9a6d-197f697bd96d
29. *The Threat Landscape in 2021*. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-2021
30. *VMware IT Performance Annual Report 2022.* https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-company-it-performance-annual-report-2022.pdf
31. *Global Threat Landscape Report*. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf
32. *Key Findings from the 2H 2022 FortiGuard Labs Threat Report.* URL: https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Svitlana Lehominova
Doctor of Sciences, professor, head of the department of information and cyber security management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID 0000-0002-4433-5123
shiarasvitlana77@gmail.com

Halyna Haidur
Doctor of Sciences, professor, head of the department of information and cyber security
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID 0000-0003-0591-3290
gaydurg@gmail.com

ANALYSIS OF CURRENT THREATS TO THE INFORMATION SECURITY OF ORGANIZATIONSAND THE FORMATION OF THE INFORMATION PLATFORM AGAINST THEM

Abstract. Taking into account the process of complication of the geopolitical and geoeconomic landscape space, the development of information technologies and the formation of new security challenges associated with the emergence of new cyber threats, there is a need for constant monitoring and forecasting of them in order to prevent consequences in the form of damage and leakage of valuable and confidential information. The authors analyzed the new predictable cyber security threats to organizations, with special attention paid to the protection of endpoints. Threats identified in the field of artificial intelligence development (underground development of malicious Large Language Models (LLM); "Script Kiddies" update; voice fraud for social engineering, which is created by artificial intelligence); changing trends in the behavior of threat actors (attacks on supply chains against managed file transfer solutions, malware threats that are becoming multilingual); as new emerging threats and attack methods (growing QR code rivalry; stealth attacks on peripheral devices; Python implementation in Excel creating a potentially new vector for attacks; LOL drivers changing action algorithms). The resulting detection of future threats emphasizes the need for strategic planning for the adoption of new technologies and platforms: such as Endpoint Detection and Response (EDR) capabilities, as well as the use of EDR as part of a multi-instrumented enhanced detection and response (XDR) architecture. Gartner's research has been proven to have a tremendous impact on improving organizations' threat detection capabilities by providing valuable insight into the strengths and weaknesses of each cybersecurity service provider with respect to emerging threat intelligence, by focusing organizations' attention on opportunities to identify gaps in their existing security infrastructure and adopt sound decisions to invest in additional solutions or services that effectively address these gaps. The spheres of activity of the world's leading companies were analyzed, their connection with Ukrainian companies was found, and further cooperation was proposed for the effective protection of national cyberspace.

Keywords: threats; cyber security; endpoints; Gartner quadrant; strategic planning.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Trellix 2024 Threat Predictions*. (2023). https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
2. Tripathi, S. *Underground Development of Malicious LLMs*. https://www.trellix.com/about/newsroom/stories/ research/trellix-2024-threat-predictions/
3. Ajeeth, S. *The Resurrection of Script Kiddies*. https://www.trellix.com/about/newsroom/stories /research/trellix-2024-threat-predictions/
4. Pena, R. *AI-generated Voice Scams for Social Engineering*. https://www.trellix.com/about/newsroom/stories /research/trellix-2024-threat-predictions/
5. Fokker, J. *Supply Chain Attacks Against Managed File Transfers Solutions*. https://www.trellix.com/ about/newsroom/stories/research/trellix-2024-threat-predictions/
6. Provecho, E. *Malware Threats are Becoming Polyglot*. https://www.trellix.com/about/newsroom/stories/ research/trellix-2024-threat-predictions/
7. *CLOP*. SentinelOne. https://www.sentinelone.com/anthology/clop/

8. Phuc, P. *The Stealthy Assault on Edge Devices*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
9. Kersten, M. *Python in Excel Creates a Potential New Vector for Attacks*. https://www.trellix.com/about/newsroom/stories/research/trellix-2024-threat-predictions/
10. Chandra, A. *LOL Drivers Are Becoming a Game Changer*. https://www.trellix.com/about/newsroom/stories/ research/trellix-2024-threat-predictions/
11. Firstbrook, P.,& Silva, C. *Magic Quadrant for Endpoint Protection Platforms*. https://assets.sentinelone.com/ eval/gartner-mq-22?xs=486596
12. *Gartner Magic Quadrant*. https://webcitation.org/691VWPAM8?url=http://www.workengine.com/Company/SitePages/Market%20Recognition.aspx
13. *Hype Cycle for Endpoint Security.* (2023). Gartner Research. https://www.gartner.com/en/documents/4589999
14. *The Impact of Gartner's XDR Magic Quadrant on Cybersecurity Strategies*. (2023). Ask. https://www.ask.com/news/impact-gartner-s-xdr-magic-quadrant-cybersecurity-strategies?utm_content=params%3Aad%3DdirN%26qo%3DserpIndex%26o%3D740004%26ag%3Dfw10&ueid=D7A48E0A-AB46-4B4A-858B-EA9CFA50E92E
15. *Magic Quadrant for Endpoint Protection Platforms*. (2022). Gartner. https://www.gartner.com/doc/reprints?id=1-2AJ91JO6&ct=220707&st=sb&culture=ru-ru&country=ru
16. Shtonda, R., Chernysh, Y., Maltseva, I., Chaika, E., & Polishchuk S. (2023). Practical approaches to cyber protection of mobile devices using the endpoint detection and response solution. *Cyber security: education, science, technology, 1(21),* 17–29.
17. *Endpoint Protection Platforms. Reviuwes and Ratings*. Gartner. https://www.gartner.com/reviews/market/endpoint-protection-platforms
18. *Gartner named Microsoft a Leader in the 2021 Endpoint Protection Platforms (EPP) Magic Quadrant*. (2021). https://www.microsoft.com/en-us/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/
19. *Microsoft Digital Defense Report*. (2021). https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
20. *Microsoft Digital Defense Report 2022 Executive Summary*. (2022). https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bcRe?culture=uk-ua&country=ua
21. *2023 Global threat report*. (2023) https://iitd.com.ua/wp-content/uploads/2023/03/crowdstrike2023globalthreatreport.pdf
22. *Annual Report and Form 10K*. (2022). https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_S_2022.pdf
23. *Cybereason*. (2023). https://research.contrary.com/reports/cybereason
24. *Rethinking Tactics 2022 Annual Cybersecurity Report.* (2022). https://documents.trendmicro.com/assets/rpt/rpt-rethinking-tactics-annual-cybersecurity-roundup-2022.pdf
25. *Maturing criminal marketplaces present new challenges to defenders. Sophos 2023 Threat Report*. (2023). https://assets.sophos.com/X24WTUEQ/at/b5n9ntjqmbkb8fg5rn25g4fc/sophos-2023-threat-report.pdf
26. *The McAfee Consumer Mobile Threat Report*. (2022). https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-mobile-threat-report-feb-2022.pdf
27. *2022 Annual Report Reimagining the future of connectivity*. (2022). https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2022.pdf
28. *Annual Report & Proxy Statement.* (2022). https://investors.paloaltonetworks.com/static-files/137ede42-9e7b-4eac-9a6d-197f697bd96d
29. *The Threat Landscape in 2021*. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-2021
30. *VMware IT Performance Annual Report 2022.* https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-company-it-performance-annual-report-2022.pdf
31. *Global Threat Landscape Report*. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf
32. *Key Findings from the 2H 2022 FortiGuard Labs Threat Report.* https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings-2h-2022