УДК 004.056 DOI https://doi.org/10.35546/kntu2078-4481.2025.2.2.29

К. С. МОСКВІН
магістрант кафедри безпеки інформаційних та комунікаційних систем
Харківський національний університет радіоелектроніки
ORCID: 0009-0006-5323-1488

О. В. СЄВЄРІНОВ
кандидат технічних наук, доцент,
професор кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-6327-6405

З. М. СИДОРЕНКО
асистент кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0002-0104-6807

Д. С. БАЛАГУРА
кандидат технічних наук,
доцент кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0009-0006-9839-3317

А. В. ЛИТВИН
старший викладач кафедри радіоелектронних систем пунктів управління
Харківський національний університет повітряних сил
імені Івана Кожедуба
ORCID: 0000-0003-1962-6356

ДОСЛІДЖЕННЯ ВПЛИВУ ІНТЕГРАЦІЇ ЗАСОБІВ КІБЕРЗАХИСТУ НА ЗАХИЩЕНІСТЬ ІТ-ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ

У статті розглянуто актуальну проблему забезпечення кібербезпеки в умовах зростаючої кількості складних і багатовекторних атак на корпоративні ІТ-інфраструктури. Обґрунтовано необхідність переходу від ізольованого застосування засобів захисту до комплексного інтегрованого підходу, що передбачає взаємодію між NGFW, EDR, SIEM, PAM, IAM та MDM. Зазначено, що значна частина порушень безпеки спричинена недостатньою координацією між компонентами кіберзахисту, що унеможливлює виявлення складних атак на ранніх етапах.

На основі аналізу сучасних досліджень і статистичних даних досліджено типові вразливості ІТ-систем, ключові вектори атак, а також недоліки у поточній практиці управління безпекою. Запропоновано архітектурну модель багаторівневого захисту, яка дозволяє створити єдине інформаційне середовище для кореляції даних про загрози, управління доступом та забезпечення реагування в реальному часі. Увагу зосереджено на практичному впливі впровадження інтегрованих систем на підвищення рівня захищеності, зменшення часу виявлення загроз та підвищення ефективності реагування на інциденти. Також акцентовано на покращенні продуктивності ІТ-відділів завдяки автоматизації рутинних процесів та централізованому управлінню безпекою.

У роботі запропоновано рекомендації щодо впровадження інтегрованої моделі кіберзахисту з урахуванням поточних потреб організацій та вимог стандартів, таких як ISO/IEC 27001, NIST Cybersecurity Framework. Результати дослідження є корисними для ІТ-менеджерів, фахівців із кібербезпеки та керівництва організацій, що прагнуть зміцнити інформаційну безпеку своєї інфраструктури. Окремо виділено вплив технологічної інтеграції на зменшення людського фактору у реагуванні на інциденти та формування безпечного цифрового середовища.

Ключові слова: *кібербезпека, ІТ-інфраструктура, інтеграція засобів захисту, багаторівневий захист, NGFW, EDR, SIEM, PAM, IAM, MDM, управління доступом, реагування на загрози.*

K. S. MOSKVIN
Master's Student at the Department of Information Technologies Security
Kharkiv National University of Radio Electronics
ORCID: 0009-0006-5323-1488

O. V. SIEVIERINOV
Candidate of Technical Sciences, Associate Professor,
Professor at the Department of Information Technologies Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-6327-6405

Z. M. SYDORENKO
Assistant at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0002-0104-6807

D. S. BALAGURA
Candidate of Technical Sciences,
Associate Professor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0009-0006-9839-3317

A. V. LYTVYN
Senior Instructor at the Department of Radioelectronic Systems of Control Points
Ivan Kozhedub Kharkiv National Air Force University
ORCID: 0000-0003-1962-6356

RESEARCH ON THE IMPACT OF CYBERSECURITY TOOLS INTEGRATION ON THE SECURITY OF AN ORGANIZATION'S IT INFRASTRUCTURE

The article addresses the pressing issue of ensuring cybersecurity in the context of increasing numbers of complex and multi-vector attacks on corporate IT infrastructures. It substantiates the need to transition from isolated security tools to a comprehensive, integrated approach that ensures the interaction between NGFW, EDR, SIEM, PAM, IAM, and MDM. It is noted that a significant portion of security breaches is caused by insufficient coordination between cybersecurity components, which hinders the early detection of complex attacks.

Based on the analysis of current research and statistical data, typical vulnerabilities of IT systems, key attack vectors, and weaknesses in current security management practices are examined. An architectural model of multi-layered protection is proposed, enabling the creation of a unified information environment for correlating threat data, managing access, and providing real-time incident response. Special attention is given to the practical impact of integrated systems on enhancing infrastructure protection, reducing threat detection time, and improving incident response efficiency. The article also emphasizes the improvement in IT department productivity through the automation of routine tasks and centralized security management.

Recommendations are proposed for implementing an integrated cybersecurity model that takes into account the current needs of organizations and the requirements of standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. The results of the study are valuable for IT managers, cybersecurity professionals, and organizational leadership seeking to strengthen their information security. The impact of technological integration on reducing human factor involvement in incident response and establishing a secure digital environment is separately highlighted.

Key words: *cybersecurity, IT infrastructure, security tools integration, multilayered protection, NGFW, EDR, SIEM, PAM, IAM, MDM, access management, incident response.*

Постановка проблеми

У сучасних умовах цифрової трансформації бізнесу та державного управління інформаційні технології стають основою функціонування більшості процесів. Разом із цим зростає складність IT-інфраструктур, кількість взаємозалежних систем, сервісів та облікових записів, що, у свою чергу, збільшує площу потенційних атак і вразливих точок. Усе частіше організації стають жертвами багаторівневих та багатовекторних кібератак, які використовують як технічні уразливості, так і людський фактор.

Основна проблема полягає в тому, що більшість організацій досі використовують фрагментовані, слабо інтегровані рішення для захисту: міжмережеві екрани, антивіруси, засоби контролю доступу, системи моніторингу тощо. Вони часто функціонують автономно, без належного обміну даними, кореляції подій і централізованого реагування. Такий підхід унеможливлює оперативне виявлення складних атак, знижує ефективність інцидент-менеджменту та не дозволяє будувати повноцінну систему кіберзахисту, яка відповідає сучасним викликам.

Крім того, в умовах гібридної інфраструктури (поєднання локальних і хмарних ресурсів, використання особистих пристроїв працівників, мобільних доступів тощо) питання управління доступом, контролю кінцевих точок та шифрування даних стає критично важливим. Однак ізольоване впровадження рішень IAM, PAM, MDM або EDR не забезпечує очікуваного рівня захищеності без їхньої взаємодії через єдину платформу управління та аналітики.

Ще одним проблемним аспектом є відсутність належної автоматизації процесів реагування, аналізу загроз і оновлення політик безпеки. В умовах обмежених людських ресурсів і великого обсягу подій безпеки саме автоматизація стає ключовим фактором підвищення ефективності захисту. Водночас, рівень впровадження таких засобів, як SIEM, SOAR або поведінковий аналіз, залишається низьким у більшості організацій.

Таким чином, проблема полягає не лише в наявності кіберзагроз, а в неузгодженості, неефективності та недостатній зрілості більшості реалізованих систем захисту. Це обґрунтовує необхідність дослідження впливу комплексної інтеграції засобів кібербезпеки на підвищення захищеності IT-інфраструктури, а також розробки архітектурних підходів, що дозволяють досягати високої стійкості до загроз при мінімізації витрат і людського фактору.

Аналіз останніх досліджень і публікацій

Актуальність інтегрованих підходів до кіберзахисту підтверджується значною кількістю сучасних наукових досліджень. У роботі K. Scarfone та P. Mell [1], опублікованій у рамках ініціативи NIST, детально аналізуються можливості систем виявлення та запобігання вторгненням (IDPS) і підкреслюється важливість їх інтеграції з іншими компонентами безпеки для досягнення високої ефективності. Автори наголошують на необхідності використання уніфікованої політики реагування та централізованого збору журналів подій як основи для побудови захищених систем.

У статті A. Yaseen [2] зроблено акцент на автоматизованому управлінні інфраструктурою для підвищення рівня кіберзахисту. Дослідження демонструє, що автоматизація процесів моніторингу, виявлення загроз та управління конфігураціями істотно знижує ризики, пов’язані з людським фактором. Автор обґрунтовує ефективність поєднання інструментів SIEM, IAM та MDM у межах єдиного підходу до керування безпекою.

Робота Y. Kilani та E. Abu-Shanab [3] досліджує вплив кібербезпеки на внутрішні організаційні процеси. Автори встановлюють, що високий рівень технологічної інтеграції рішень кіберзахисту позитивно корелює з підвищенням ефективності управління, зниженням затримок у прийнятті рішень та покращенням якості обслуговування. Таким чином, кібербезпека розглядається не лише як технічна необхідність, а як стратегічний фактор розвитку організацій.

Доповненням до зазначених досліджень є робота A. Vázquez-Ingelmo [4], де розглядається вплив SIEM на швидкість реагування на інциденти при використанні з EDR та IAM у межах автоматизованих сценаріїв реагування.

Таким чином, наукова спільнота підтверджує, що ефективне підвищення рівня захищеності IT-інфраструктури можливе лише за умови взаємодії між усіма компонентами системи безпеки. Поєднання автоматизації, централізованого моніторингу та управління доступом формує основу для створення надійного, адаптивного та масштабованого захисного середовища.

Формулювання мети дослідження

Мета дослідження зосереджена на розробці концепції багаторівневої інтегрованої архітектури кіберзахисту для організаційних IT-інфраструктур. В умовах зростання складності загроз та технологічного навантаження, ефективна інтеграція засобів безпеки (NGFW, EDR, SIEM, IAM, PAM, MDM) стає ключовим чинником забезпечення стійкості до атак. Актуальність теми обумовлена необхідністю швидкого реагування, централізованого моніторингу та мінімізації людського фактору в інцидент-менеджменті.

Дослідження передбачає аналіз існуючих архітектур безпеки, вивчення практик інтеграції різнорідних компонентів захисту, а також виявлення бар’єрів, що заважають побудові єдиного середовища управління. Основна мета полягає в тому, щоб обґрунтувати модель ефективної взаємодії між компонентами кіберзахисту, яка забезпечить зменшення часу реагування, підвищення точності детекції та покращення загальної інформаційної безпеки організації.

Очікувані результати включають методичні рекомендації щодо впровадження інтегрованої архітектури, приклади оптимальних конфігурацій і механізмів взаємодії, що зможуть підвищити безпеку як комерційних, так і критичних державних IT-систем.

Викладення основного матеріалу дослідження

Сучасний розвиток інформаційних технологій супроводжується стрімким збільшенням кількості кіберзагроз, які становлять небезпеку для корпоративних середовищ. За статистикою [5]:

– 24 мільярди скомпрометованих облікових даних пропонуються для продажу у неконтрольованих сегментах Інтернет;

– 97 % підприємств покладаються на застарілу або гібридну інфраструктуру IAM (управління ідентифікацією та доступом);

– 82 % порушень даних і атак програм-вимагачів включають або базуються на скомпрометованих облікових даних користувачів;

– більш ніж 80 % порушень безпеки пов’язані з викраденням або компрометацією автентифікаційних даних.

Кіберзлочинці використовують різноманітні вектори атак, включаючи скомпрометовані облікові записи, несанкціонований доступ до систем, зловживання мобільними пристроями, а також недостатній рівень захисту мережі. Інтеграція ефективних засобів кіберзахисту є ключовим фактором у забезпеченні безпеки IT-інфраструктури та збереженні її продуктивності.

За статистикою, понад 60 % кібератак здійснюється через скомпрометовані облікові записи, що підкреслює важливість рішень для управління доступом, таких як PAM (управління привілейованим доступом) та IAM (управління ідентифікацією та доступом). У статті розглянуто вплив інтеграції різних рішень, таких як NGFW (фаєрволи нового покоління), EDR (виявлення та реагування на загрози для кінцевих пристроїв), SIEM (системи управління інформацією та подіями безпеки), PAM, IAM та MDM (управління мобільними пристроями), на захищеність IT-інфраструктури.

Вразливості корпоративних систем

Вразливості корпоративних систем залишаються однією з основних причин успішних кібератак. Це свідчить про постійне зростання кількості уразливих місць, які можуть бути використані зловмисниками для атак на корпоративні середовища. Вразливості можуть виникати як у програмному забезпеченні, так і в апаратних компонентах системи, створюючи можливості для зловмисників отримати доступ до конфіденційної інформації або порушити роботу корпоративної мережі.

Одним із основних факторів, що сприяють появі нових вразливостей, є постійна складність і розвиток програмного забезпечення, а також прискорений цикл розробки продуктів. Часто виробники прагнуть швидко випустити нові функції, і це може призвести до виникнення недоліків у безпеці. Важливим аспектом для забезпечення кібербезпеки є своєчасне виявлення та виправлення таких вразливостей, що досягається шляхом регулярних оновлень та патчів безпеки.

До основних типів вразливостей належать [6]:

– застаріле або невиправлене програмне забезпечення;
– слабкі паролі;
– відсутність контролю доступу;
– недостатнє навчання співробітників;
– недостатньо захищені мережеві інтерфейси.

Врахування вразливостей дозволяє компаніям ефективніше захищати свої інформаційні ресурси та знижувати ризик успішних атак. Аналіз вразливостей має бути невід'ємною частиною процесу управління ризиками, а заходи щодо їх усунення повинні здійснюватися на постійній основі.

Ключовими векторами атак є:

– скомпрометовані облікові записи;
– небезпечні кінцеві пристрої;
– недостатній рівень захисту мережевого периметру;
– несанкціонований доступ.

Для забезпечення ефективного захисту корпоративної мережі організації необхідно врахувати такі аспекти:

– перед впровадженням будь-яких рішень слід провести аудит безпеки для визначення слабких місць, пріоритизації загроз та оцінки поточного стану безпеки;

– засоби захисту слід впроваджувати поетапно. Спершу організація має забезпечити захист периметра мережі через NGFW, потім встановити EDR для кінцевих пристроїв, інтегрувати IAM та PAM для управління доступом і завершити впровадження SIEM для моніторингу подій;

– усі рішення повинні бути інтегровані в єдину екосистему. Наприклад, дані з NGFW мають надходити в SIEM для аналізу, а інформація про підозрілу активність передаватись до EDR для ізоляції заражених пристроїв;

– забезпечення кібербезпеки неможливе без навчання співробітників.

Архітектура системи захисту IT-інфраструктури

Багатошарова система захисту є ключовим елементом ефективної стратегії кібербезпеки, оскільки забезпечує захист на різних рівнях корпоративної інфраструктури. Такий підхід дозволяє значно знизити ризик успішного проникнення зловмисників, оскільки кожен шар захисту створює додаткову перешкоду для атакуючих.

Багатошарова система захисту включає такі компоненти, як мережевий захист (міжмережеві екрани, IDS/IPS), захист кінцевих точок (антивірусне програмне забезпечення, EDR), управління ідентифікацією та доступом (IAM), а також системи шифрування даних. Кожен із цих елементів доповнює інші, забезпечуючи комплексний підхід до захисту корпоративних ресурсів. Перелік рішень кібербезпеки для побудови багатошарової системи захисту наведений на рисунку 1.

Як видно з рисунку 1 загальна структура архітектури захисту складається з умовних 4 рівнів, кожен з яких обробляє ризики відповідно до завдань та можливостей. Кожен рівень покладається на велику кількість інструментів, які можуть працювати як окремо, так і у співпраці один з одним. Ми зосередимось на найбільш важливих з них [7].

Архітектура системи захисту IT-інфраструктури складається з певного набору компонентів, який де-факто використовується у більшості найбільш захищених IT-інфраструктур. Ця архітектура дозволяє створити багаторівневий захист, забезпечуючи ефективну взаємодію між усіма компонентами. До цих компонентів відносяться:

– використання NGFW для аналізу трафіку, блокування загроз та забезпечення сегментації мережі;
– використання EDR для моніторингу, виявлення та автоматичного реагування на загрози кінцевих пристроїв;

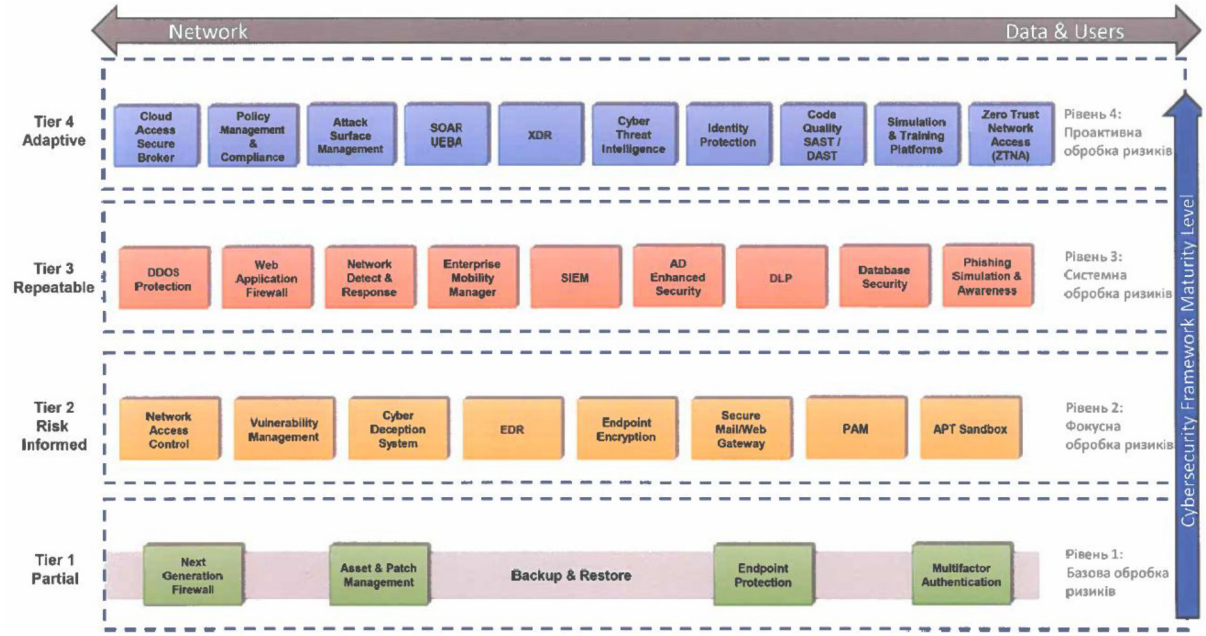

Рис. 1. Перелік рішень багатошарової системи захисту

– використання IAM для багатофакторної автентифікації та PAM для управління привілейованими обліковими записами при централізованому управлінні доступом;
– використання SIEM для аналізу подій у реальному часі та виявлення складних атак;
– використання MDM для управління політиками доступу та шифрування даних на мобільних пристроях.

Ця архітектура дозволяє створити багаторівневий захист, забезпечуючи ефективну взаємодію між усіма компонентами.

Розглянемо, які переваги надає використання кожного компоненту, що були розглянуті вище, з точки зору підвищення захищеності інфраструктури в цілому.

Вплив інтеграції NGFW

Фаєрволи нового покоління NGFW є критично важливим елементом сучасної кібербезпеки [8, 9], який забезпечує багаторівневий захист інфраструктури (рис. 2). Вони здатні глибоко аналізувати трафік у реальному часі, блокуючи потенційні загрози ще до того, як вони зможуть завдати шкоди.

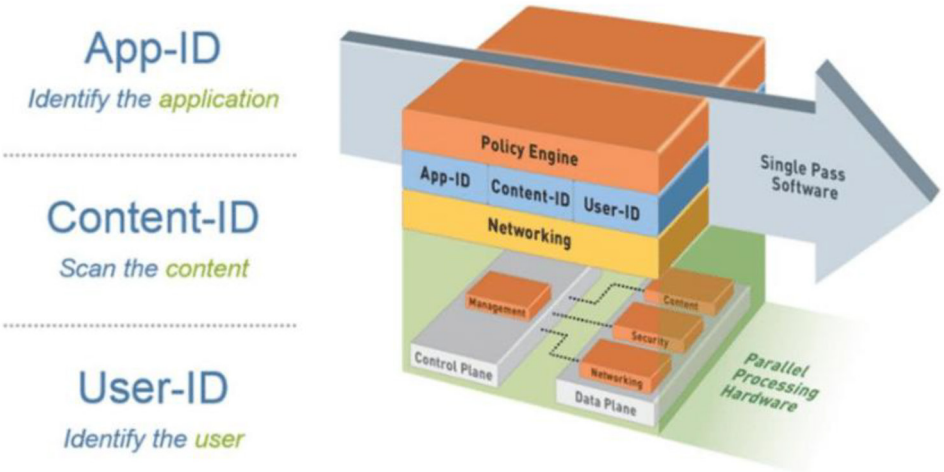

Рис. 2. Next-Generation Firewall

Одним із важливих аспектів NGFW є інтеграція з системами виявлення та запобігання вторгнень (IPS). NGFW враховує контекст мережевого з'єднання, такий як користувач, додаток, місцезнаходження та інші параметри, при прийнятті рішення про блокування або допуск трафіку. Розширений аналіз дозволяє не лише блокувати відомі загрози, але й ідентифікувати нові, використовуючи поведінкові моделі та методи машинного навчання. Також

це дозволяє розуміти, які дії є допустимими в конкретному контексті і зменшує ризик некоректного визначення стосовно атак чи нормальної поведінки користувача або системи.

Інтеграція NGFW з іншими системами моніторингу дає змогу обмінюватися даними між різними рішеннями, виявляючи складні багатовекторні атаки. Завдяки цьому організації можуть своєчасно реагувати на загрози, запобігати масштабним інцидентам і координувати заходи безпеки на всіх рівнях. Крім того, NGFW забезпечує контроль додатків, блокуючи небезпечні чи небажані програми, які можуть бути використані зловмисниками для експлойтів або викрадення інформації. Це дозволяє уникнути проникнення небезпечних програм у корпоративну мережу, зменшуючи ризик втрати даних або компрометації системи.

Роль EDR у захисті кінцевих пристроїв

Рішення EDR забезпечують моніторинг, виявлення та реагування на загрози для кінцевих пристроїв [10–12]. EDR пропонують декілька ключових функцій, які дозволяють суттєво підвищити рівень безпеки в організації (рис. 3).

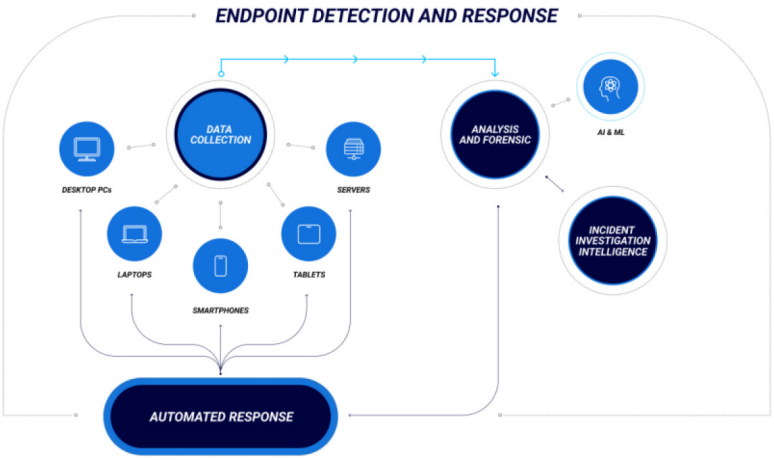

Рис. 3. Система типу EDR

EDR здійснює детальний моніторинг поведінки користувачів та процесів на кінцевих пристроях. Це включає аналіз відхилень від нормальної активності, таких як незвичні запити до ресурсів, підозріла активність програм чи виконання невідомих скриптів, що дозволяє отримувати повну інформацію про всі дії, які виконуються на пристроях, включаючи запуск додатків, зміну файлів, підключення до мережі та інші ключові події. Завдяки такому підходу система може виявляти потенційні загрози ще на етапі їх зародження, що дозволяє уникнути серйозних наслідків.

Автоматичне реагування є важливою перевагою EDR. У разі виявлення загрози система може миттєво ізолювати заражений пристрій від мережі, зупинити виконання шкідливого програмного забезпечення та видалити його з системи. Це мінімізує ризик поширення атаки на інші частини інфраструктури та скорочує час простою, викликаного інцидентом. Окрім автоматизації, EDR надає командам з кібербезпеки потужні інструменти для розслідування інцидентів.

Додатковою перевагою EDR є його інтеграція з іншими системами кібербезпеки, такими як SIEM, SOAR та рішення для управління ідентифікацією. Завдяки цьому EDR стає частиною комплексної стратегії захисту, що охоплює всі рівні інфраструктури організації.

Ще однією важливою функцією є здатність EDR працювати з хмарними середовищами, забезпечуючи однаковий рівень захисту як для локальних пристроїв, так і для ресурсів у хмарі. Це особливо важливо в умовах сучасної гібридної інфраструктури, коли співробітники можуть працювати з різних пристроїв і з різних місць.

Загалом EDR дозволяє організаціям не лише захищати свої кінцеві точки, але й підвищувати загальну стійкість до кіберзагроз.

Важливість PAM та IAM

Управління привілейованим доступом (PAM) є ключовим інструментом для захисту критичних систем та облікових записів [13]. Воно дозволяє створити і впровадити механізми контрольованого і безпечного доступу до найбільш чутливих ресурсів організації.

Однією з основних функціональних можливостей PAM є централізоване управління обліковими записами з підвищеними правами. Це забезпечує єдиний підхід до зберігання, створення, ротації та моніторингу привілейованих облікових записів. PAM дозволяє автоматично змінювати паролі або ключі доступу відповідно до політик безпеки, що значно знижує ризик їх компрометації.

PAM-рішення також забезпечують детальний аудит та моніторинг активності користувачів, які використовують привілейовані облікові записи [14]. Додатковою перевагою PAM є можливість розмежування прав доступу за принципом найменших привілеїв (Least Privilege). Це означає, що користувачі отримують лише ті права доступу, які необхідні для виконання їхніх завдань. Такий підхід мінімізує ризик помилкових дій або зловмисного використання привілейованих облікових записів.

PAM також пропонує можливості ізоляції та захисту сесій, що використовуються для підключення до критичних систем. Це забезпечує додатковий рівень контролю над доступом до серверів, баз даних, мережевого обладнання та інших ресурсів. Наприклад, сесії можуть бути автоматично перервані у разі виявлення підозрілої активності.

Інтеграція PAM із системами багатофакторної автентифікації (MFA) підвищує рівень захисту привілейованих облікових записів. Завдяки цьому навіть у разі компрометації пароля зловмисник не зможе отримати доступ до критичних систем без додаткової перевірки, наприклад, через одноразовий код або біометричні дані.

Крім того, PAM автоматизує процес ротації паролів привілейованих облікових записів. Ця функція забезпечує регулярне оновлення облікових даних, унеможливлюючи їх компрометацію через тривале використання. Такий підхід також знижує залежність від людського фактору в управлінні доступом.

Ще однією перевагою PAM є здатність інтегруватися з іншими системами безпеки, такими як SIEM, IAM та EDR. Це дозволяє створити комплексний підхід до захисту інфраструктури, забезпечуючи обмін інформацією про інциденти та спрощуючи реагування на загрози.

Використання PAM дозволяє організаціям підвищити безпеку своїх облікових записів, знизити ризики внутрішніх і зовнішніх загроз та забезпечити відповідність сучасним стандартам і регуляторним вимогам у сфері кібербезпеки.

Системи управління ідентифікацією та доступом (IAM) в свою чергу відіграють ключову роль у забезпеченні безпеки корпоративного середовища [15] (рис. 4). Вони забезпечують ефективне управління доступом до ресурсів організації через управління цифровими ідентичностями користувачів і контролю доступу до ресурсів у межах організації, що знижують ризик несанкціонованих дій. Крім того, сучасні IAM рішення підтримують використання єдиного входу (Single Sign-On, SSO), що дозволяє користувачам отримувати доступ до всіх необхідних ресурсів за допомогою однієї аутентифікації, підвищуючи зручність та безпеку.

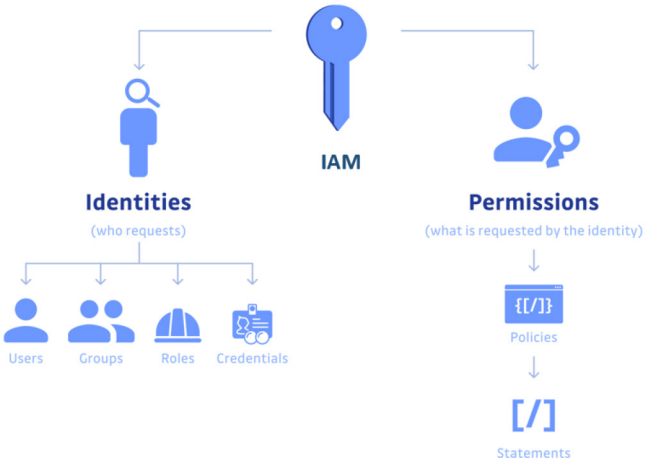

Рис. 4. Система типу IAM

Функція єдиної точки входу (SSO) дозволяє користувачам використовувати один набір облікових даних для доступу до всіх корпоративних систем. Це не лише спрощує процес автентифікації, але й знижує ризик компрометації через зменшення кількості паролів, які потрібно запам'ятовувати чи зберігати.

Інтеграція MDM

Рішення для управління мобільними пристроями (MDM) дозволяють організаціям забезпечувати безпечний та контрольований доступ до корпоративних ресурсів через мобільні платформи. Вони надають широкі можливості щодо централізованого керування мобільними пристроями (рис. 5), підвищуючи рівень безпеки та захищаючи дані компанії.

Однією з ключових функцій MDM є управління політиками безпеки. Це дозволяє встановлювати чіткі правила, які обмежують доступ до корпоративних ресурсів для пристроїв, що не відповідають встановленим вимогам безпеки.

MDM також забезпечує автоматичне шифрування корпоративних даних, що зберігаються на мобільних пристроях. Це запобігає витоку конфіденційної інформації у разі втрати або компрометації пристрою. Крім того, такі

Рис. 5. Функціональні можливості MDM

рішення дозволяють адмініструвати процеси доступу до корпоративних додатків, забезпечуючи безпеку даних навіть у випадках використання особистих пристроїв співробітниками.

У разі втрати або крадіжки пристрою адміністратори можуть оперативно видалити всі корпоративні дані з пристрою, мінімізуючи ризики витоку інформації. Це дозволяє організації забезпечувати високий рівень безпеки навіть у непередбачуваних ситуаціях.

Роль SIEM у забезпеченні комплексного захисту

Системи управління інформацією та подіями безпеки (SIEM) є центральним елементом інтеграції багаторівневих рішень кіберзахисту. Вони об'єднують дані з різних джерел, таких як NGFW, EDR, MDM, та забезпечують їхню кореляцію для виявлення загроз.

SIEM аналізує журнали подій і системні дані в реальному часі, ідентифікуючи аномальні патерни, які можуть вказувати на спроби атаки. Це дозволяє організаціям оперативно реагувати на загрози, запобігаючи їхньому поширенню.

Однією з ключових переваг SIEM є автоматизована аналітика, яка допомагає виявляти складні багатовекторні атаки. Крім того, SIEM забезпечує функціонал для створення звітів, необхідних для дотримання нормативних вимог. Це робить систему незамінним інструментом не лише для безпеки, але й для управління відповідністю.

Інтеграція SIEM із загальною екосистемою кіберзахисту значно підвищує ефективність реагування на інциденти, мінімізуючи збитки від атак та забезпечуючи цілісність корпоративної мережі.

Захищеність та продуктивність IT-інфраструктури

Інтеграція засобів кіберзахисту не лише значно підвищує рівень захищеності IT-інфраструктури, але й сприяє підвищенню її продуктивності. Це досягається завдяки оптимізації процесів, зниженню простоїв і раціональному використанню ресурсів. Основними напрямами впливу є:

– оптимізація процесів безпеки завдяки автоматизації рутинних завдань, таких як моніторинг, оновлення систем безпеки та аналіз загроз, ресурси організації спрямовуються на більш стратегічні ініціативи. Це дозволяє знизити ризики людських помилок та підвищити ефективність реагування на інциденти. Крім того, автоматизація зменшує навантаження на команди IT, дозволяючи їм зосередитися на вдосконаленні інфраструктури;

– швидке виявлення та мінімізація впливу атак засобами кіберзахисту. Це значно скорочує потенційний збиток і знижує ризик поширення атак на інші частини інфраструктури. Одночасно це дозволяє уникнути значних простоїв, забезпечуючи безперервність бізнес-процесів;

– надійно захищена IT-інфраструктура демонструє партнерам і клієнтам високий рівень відповідальності за безпеку даних, що сприяє зміцненню репутації організації та формуванню довгострокових бізнес-відносин. Крім того, прозорість і ефективність безпеки підвищують довіру співробітників, які працюють у захищеному цифровому середовищі.

Завдяки цим аспектам організації отримують не лише підвищений рівень безпеки, але й створюють основу для подальшого розвитку та ефективного функціонування в умовах зростаючих кіберзагроз.

Висновки

Проведене дослідження, присвячене розробці багаторівневої інтегрованої архітектури кібербезпеки, підтвердило доцільність комплексного підходу до побудови системи захисту IT-інфраструктури. Аналіз сучасних

вразливостей показав, що традиційні ізольовані рішення вже не забезпечують належного рівня стійкості до складних багатовекторних атак, особливо в умовах зростання обсягів даних, децентралізації та розвитку гібридних середовищ.

Запропонована архітектура охоплює чотири рівні кіберзахисту – периметр, кінцеві точки, контроль доступу та централізовану аналітику – і забезпечує ефективну взаємодію між такими системами як NGFW, EDR, PAM, IAM, SIEM та MDM. Її реалізація дозволяє формувати цілісний ландшафт безпеки, що здатен адаптуватися до нових загроз, зменшує навантаження на аналітиків SOC та скорочує час реагування на інциденти.

Інтеграція рішень забезпечує обмін подіями безпеки між компонентами, дає змогу автоматизувати виявлення загроз і оперативне прийняття рішень у реальному часі. Такий підхід дозволяє не лише своєчасно виявляти атаки, але й блокувати їх ще до нанесення шкоди.

Практична цінність запропонованої архітектури полягає у її масштабованості, відповідності вимогам сучасних стандартів безпеки (NIST, ISO/IEC 27001) та можливості поетапного впровадження в умовах обмежених ресурсів. Дослідження також демонструє, що побудова інтегрованої системи безпеки є ключовим фактором у підвищенні цифрової стійкості організацій.

Отже, впровадження багаторівневої архітектури з інтегрованими інструментами кібербезпеки є ефективним рішенням для захисту корпоративного середовища від складних та еволюційних кіберзагроз.

Список використаної літератури

1. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Gaithersburg, MD: National Institute of Standards and Technology, 2007. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-94/final

2. Yaseen A. Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures. ResearchGate. 2024. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/378594258

3. Kilani Y., Cyber-security effect on organizational internal process: mediating role of technological infrastructure. Problems and Perspectives in Management. № 18(1). 2020. pp 449-460 [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/340490846

4. Vázquez-Ingelmo A., García-Holgado A., García-Peñalvo F. J. A SIEM-based Framework for Automated Cybersecurity Incident Response. Lecture Notes in Computer Science. V. 13327. 2022. P. 370–385. DOI: https://doi.org/10.1007/978-3-031-09243-8_29

5. Network Infrastructure Security 2023: National Security Agency Cybersecurity Technical Report, 2023. [Електронний ресурс]. Режим доступу: https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_ NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

6. Open Web Application Security Project (OWASP). OWASP Top Ten. [Електронний ресурс]. Режим доступу: https://owasp.org/www-project-top-ten/

7. ISO/IEC 27001:2022. Information Security Management Systems. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/27001

8. Check Point Software Technologies. Next-Generation Firewall. [Електронний ресурс]. Режим доступу: https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/

9. National Institute of Standards and Technology (NIST). Cybersecurity Framework. [Електронний ресурс]. Режим доступу: https://www.nist.gov/cyberframework

10. Gartner Peer Insights. Reviews for Endpoint Protection Platforms. [Електронний ресурс]. Режим доступу: https://www.gartner.com/reviews/market/endpoint-protection-platforms.

11. Шуліка, К., Балагура, Д. і Сидоренко, З. Аналіз методів обходу сучасних систем захисту кінцевих точок EDR, Радіотехніка, № 2(217), 2024, с. 64–68. DOI: https://doi.org/10.30837/rt.2024.2.217.05.

12. Шуліка, К., Балагура, Д., Смірнов, А., Непокритов, Д., Литвин, А. Метод використання сучасних систем захисту кінцевих точок (EDR) для убезпечення від комплексних атак. СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ, № 2(28), 2024, с. 182–195. https://doi.org/10.30837/2522-9818.2024.2.182

13. Wallix Bastion. Privileged Access Management. [Електронний ресурс]. Режим доступу: Https://www.wallix.com/products/privileged-access-management/.

14. Delinea PAM Solution. Securing Privileged Accounts. [Електронний ресурс]. Режим доступу: https://delinea.com/what-is/privileged-access-management-pam.

15. Silverfort IAM Solution. Adaptive Authentication and Access Control. [Електронний ресурс]. Режим доступу: https://www.silverfort.com/

References

1. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Gaithersburg, MD: National Institute of Standards and Technology, 2007. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-94/final

2. Yaseen A. Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures. ResearchGate. 2024. Retrieved from: https://www.researchgate.net/publication/378594258

3. Kilani Y., (2020) Cyber-security effect on organizational internal process: mediating role of technological infrastructure. Problems and Perspectives in Management. no.18(1). pp 449–460.

4. Vázquez-Ingelmo A., García-Holgado A., García-Peñalvo F. J. A SIEM-based Framework for Automated Cybersecurity Incident Response. Lecture Notes in Computer Science. V. 13327. 2022. P. 370–385. Retrieved from: https://doi.org/10.1007/978-3-031-09243-8_29

5. Network Infrastructure Security 2023: National Security Agency Cybersecurity Technical Report, 2023. 40 c.; Retrieved from: https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_ NETWORK_ INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

6. Open Web Application Security Project (OWASP). OWASP Top Ten. Retrieved from: https://owasp.org/www-project-top-ten/

7. ISO/IEC 27001:2022. Information Security Management Systems. Retrieved from: https://www.iso.org/standard/27001

8. Check Point Software Technologies. Next-Generation Firewall. Retrieved from: https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/

9. National Institute of Standards and Technology (NIST). Cybersecurity Framework. Retrieved from: https://www.nist.gov/cyberframework

10. Gartner Peer Insights. Reviews for Endpoint Protection Platforms. Retrieved from: https://www.gartner.com/reviews/market/endpoint-protection-platforms.

11. Shulika, K., Balagura, D., Sydorenko, Z. (2024). Analiz metodiv obhodu suchasnyh cyctem zahystu kincevyh tochok EDR [Analysis of methods for bypassing modern EDR endpoint protection systems.] Radiotekhnika, no.2(217), pp 64–68.

12. Shulika, K., Balagura, D., Smirnov, A., Nepokrytov, D., & Lytvyn, A. (2024). Metod vykorystannya suchasnyh system zahystu kincevyh tochok (EDR) dlya ubezpechennya vid kompleksnyh atak [A method of using modern endpoint detection and response (EDR) systems to protect against complex attacks.] INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES, no. 2(28), pp. 182–195.

13. Wallix Bastion. Privileged Access Management. Retrieved from: Https://www.wallix.com/products/privileged-access-management/.

14. Delinea PAM Solution. Securing Privileged Accounts. Retrieved from: https://delinea.com/what-is/privileged-access-management-pam.

15. Silverfort IAM Solution. Adaptive Authentication and Access Control. Retrieved from: https://www.silverfort.com/