https://orcid.org/0000-0002-5080-1856
https://orcid.org/0000-0003-3604-2256
https://orcid.org/0009-0003-8844-1213

УДК 004.056.5

Ю.М. ЛИСЕЦЬКИЙ[*], С.І. БОБРОВ[*], О.І. ДАНЧЕНКО[**]

КОРПОРАТИВНА СИСТЕМА ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

[*]ДП «ЕС ЕНД ТІ УКРАЇНА», м. Київ, Україна
[**]Державна служба спеціального зв'язку та захисту інформації, м. Київ, Україна

Анотація. *У статті проаналізовано сучасні технології і системи кіберзахисту, такі як міжмережевий екран наступного покоління, мікросегментація, системи керування доступом до мережі, віддалений доступ із нульовою довірою, системи захисту від розподілених атак типу «відмова в обслуговуванні», системи захисту від атак на портали, брокери безпечного доступу до хмар, системи захисту від шкідливого програмного забезпечення, система захисту від атак через електронну пошту, система керування мобільними пристроями, система керування обліковими записами та авторизацією користувачів, система керування привілейованим доступом, системи захисту фізичного доступу, системи захисту від витоку інформації, система багатофакторної автентифікації та авторизації, системи захисту баз даних, система аналізу вразливостей, система імітації атак, система кіберпасток, система збору, кореляції, аналізу журналів та дій, система автоматизації дій під час розслідування чи реакції на інцидент. Вибір необхідних систем кіберзахисту для побудови корпоративної системи інформаційної та кібербезпеки визначається з урахуванням корпоративного IT-ландшафту. Критично важливими компонентами цієї системи є рішення щодо захисту мережі типу NGFW, захист робочих станцій і серверів від шкідливого програмного забезпечення на базі EDR/XDR, захист системи електронної пошти. Рекомендованими компонентами також є система управління доступом до мережі та віддаленим доступом із нульовою довірою, захист від витоків інформації, комплекс систем автентифікації та авторизації. Для організацій із середньою чи високою складністю IT-ландшафту системи кластера аналітики кібербезпеки є критично важливими, особливо системи збору й кореляції подій та система аналізу вразливостей. Враховуючи вищевикладене, запропоновано архітектуру корпоративної системи інформаційної та кібербезпеки, яка дозволить забезпечити ешелоновану систему ефективного захисту від кіберзагроз.*

Ключові слова: *інформаційна безпека, кібербезпека, технології, системи, архітектура, компоненти, корпоративна інформаційна система.*

Abstract. *The article analyses modern cybersecurity technologies and systems such as next-generation firewalls, micro-segmentation, network access control systems, zero-trust remote access, systems protecting against distributed denial-of-service attacks, systems protecting against portal attacks, secure access brokers to the cloud, malware protection systems, email attack protection system, mobile device management systems, user account and authorization management systems, privileged access management systems, physical access protection systems, data leak protection systems, multi-factor authentication and authorization systems, database protection systems, vulnerability analysis systems, attack simulation systems, cyber decoy systems, log and action collection, correlation, and analysis systems, as well as automation systems for actions during an investigation or incident response. The choice of necessary cybersecurity systems for designing a corporate information and cybersecurity system is determined, considering the corporate IT landscape. Critically important components of this system include network protection solutions such as NGFW, workstation and server protection against malicious software based on EDR/XDR, and email system protection. Highly recommended components also include network access management systems and remote access with zero trust, information leakage protection,*

ISSN 1028-9763. Математичні машини і системи. 2024. № 3-4

and a complex system of authentication and authorization. For organizations with medium or high complexity of IT landscapes, cybersecurity analytics cluster systems are critically important, especially event collection and correlation systems and vulnerability analysis systems. Considering the above, a corporate architecture of information and cybersecurity is proposed, which will ensure a layered system of effective protection against cyber threats.
Keywords: *information security, cybersecurity, technologies, systems, architecture, components, corporate information system.*

DOI: 10.34121/1028-9763-2024-3-4-37-49

1. Вступ

Стрімкий розвиток процесів цифровізації став джерелом не лише нових можливостей, але й ризиків та загроз насамперед інформаційній та кібербезпеці держави. Поряд із традиційними загрозами, такими як втручання сторонніх осіб у корпоративні інформаційні системи (КІС) і мережі, порушення цілісності баз даних (БД) тощо, створюються ряд додаткових загроз інформаційним ресурсам і технологіям, методи діагностики і протидії якім поки що відпрацьовані не в повній мірі [1]. Передусім це загрози, пов'язані з кібератаками, розкриттям персональних даних, впливом шпигунських програм і вірусів, фішингом, загрозами, пов'язаними з оновленням комп'ютерів, тощо [2, 3]. Тому завдання вдосконалення, підвищення надійності та ефективності корпоративних систем інформаційної та кібербезпеки (КСІК) є досить актуальним.

Мета статті — проаналізувати сучасні технології і системи кіберзахисту та запропонувати архітектуру побудови ешелонованої системи ефективного кіберзахисту КІС.

2. Компоненти КСІК

Раніше вважалося, що наявність міжмережевого екрана (ММЕ) вирішує майже 90 % проблем, пов'язаних із можливими атаками на КІС, і для базового рівня захисту достатньо МСЕ наступного покоління на периметрі та антивірусів, встановлених на робочих станціях та серверах. Але поряд із зростанням цінності вмісту КІС, збільшення залежності від даних та їх доступності зростає і попит на розвиток технологій, методів та засобів кібератак. Сьогодні арсенал засобів та способів отримання чи знищення інформації в КІС величезний і оновлюється щодня. Крім класичних засобів, що дозволяють продіагностувати віддалену систему та виявити її можливі слабкі місця, а також здійснити мережеву атаку в лоб через мережевий шлюз або за допомогою шкідливого програмного забезпечення (ПЗ), з'явилися комплексні атаки, які здійснюються через кілька векторів атак, не викликаючи підозр у вищеописаних систем кіберзахисту; різні варіанти прихованих шкідливих програм, у тому числі безфайлове шкідливе ПЗ, яке проникає через поштові системи та вебсесії, що маскуються у зображеннях, та ін.

Тому сучасна КСІК повинна включати компоненти, що виконують різні функції і доповнюють один одного, зокрема, захист мережевого рівня, захист робочих станцій та серверів, захист даних, що зберігаються та обробляються в КІС, аналітичні системи кібербезпеки.

До систем захисту мережевого рівня відносять міжмережеві екрани наступного покоління (Next Generation Firewall — NGFW), мікросегментацію, у тому числі у віртуальній інфраструктурі, системи керування доступом до мережі (Network access control — NAC), віддалений доступ з нульовою довірою (Zero Trust Network Access — ZTNA), системи захисту від розподілених атак типу «відмова в обслуговуванні» (Distributed Denial-of-Service Attack — DDoS), системи захисту від атак на портали (Web Application Firewall — WAF), брокери безпечного доступу до хмар (Cloud Access Security Broker — CASB).

До систем захисту робочих станцій та серверів відносять системи захисту від шкідливого ПЗ, у тому числі від невідомого раніше, систему захисту від атак через електронну

пошту, систему керування мобільними пристроями (Enterprise Mobility Management/Mobile Device Management — EMM/MDM), систему управління ідентифікацією та авторизацією користувачів і обліковими записами (Identity and Access Management — IAM), систему керування привілейованим доступом, системи захисту фізичного доступу.

До систем захисту даних відносять системи захисту від витоку інформації (Data Leak Protection — DLP), систему багатофакторної автентифікації та авторизації (MultiFactor Authentication — MFA), систему резервного копіювання та відновлення і системи архівації, системи захисту БД.

До аналітичних систем кібербезпеки відносять систему аналізу вразливостей, систему імітації атак, систему кіберпасток, систему збору, кореляції та аналізу журналів і дій (Security Information and Event Management — SIEM), систему автоматизації дій під час розслідування чи реакції на інцидент.

Окремо хотілося б відзначити, що часто ставлять рівність між кібербезпекою та інформаційною безпекою. Це не зовсім коректно. Інформаційна безпека займається забезпеченням безпеки даних, а саме: забезпечення доступності авторизованим користувачам, захист від неавторизованого доступу, захист від знищення, захист від спотворення тощо, в результаті будь-яких дій (кіберінциденту або виходу з ладу обладнання, або програмного збою, або відключення живлення, або руйнування каналів зв'язку та ін.). Кібербезпека у свою чергу захищає IT-інфраструктуру та дані від кібератак.

Надалі буде розглянуто системи кібербезпеки, в які не входять системи резервного копіювання та архівації інформації. Під словом безпека будемо мати на увазі саме кібербезпеку.

3. Корпоративні системи кібербезпеки

Міжмережевий екран наступного покоління (NGFW). Як випливає з назви, це пристрій для перевірки і фільтрації трафіка, але на відміну від своїх попередників, аналіз трафіка виконується на всіх рівнях моделі OSI (Open Systems Interconnection model) аж до сьомого (Application layer), крім безпосередньо функцій міжмережевого екрана (ММЕ) є також функціонал системи захисту від вторгнень (Intrusion Protection Systems — IPS) та БД відомих шкідливих активностей і ресурсів, що оновлюється.

Отже, ММЕ наступного покоління аналізує та фільтрує трафік, використовуючи інформацію про IP-адреси, порти та ін. аж до додатку, якому належить кожен інформаційний потік [4]. Рішення приймається інтелектуальним двигуном системи на підставі актуальної бази знань.

Такі пристрої встановлюють не тільки на периметрі мережі, де вони виконують функцію шлюзів безпеки (Secure Web Gateway — SWG), а й у середині КІС для контролю трафіка між сегментами та між вузлами КІС. NGFW може бути як апаратним, так і віртуальним, зокрема, працювати на рівні гіпервізора системи віртуалізації контролю трафіка безпосередньо між віртуальними машинами. Необхідність установки NGFW у середині мережі та в середині вузлів аж до рівня віртуальних машин викликана необхідністю гранульовано розділяти та контролювати трафік для детекції шкідливої активності на ранньому етапі та запобігання розповсюдженню її по мережі. Таке ж завдання вирішує і мікросегментація.

Мікросегментація. Мережева технологія, яка дозволяє розділити КІС на мінімально можливі логічні мережі, що передають окремі робочі навантаження, і не змішувати трафік, а також контролювання переміщення трафіка між цими логічними мережами називається мікросегментацією. Чим менше сегменти, тим вища швидкість реакції атак і менше швидкість її поширення по IT-інфраструктурі КІС. З іншого боку, рівні моделі OSI можна використовувати, зокрема, і віртуальної локальної мережі (Virtual Local Area Network — VLAN), але як із механізмів, тому що технологія мікросегментації динамічно налаштову-

ється та функціонує на другому та третьому рівнях моделі OSI, а у віртуальному середовищі на рівні гіпервізора та віртуальних комутаторів.

Системи керування доступом до мережі (Network access control systems — NAC). Крім завдання поділу та фільтрації трафіка в КІС, стоїть ще завдання визначення та поділу користувачів, які намагаються підключитися до КІС на рівні мережі. Це завдання вирішується за допомогою протоколу IEEE 802.1x. При цьому система контролю та управління доступом до мережі повинна визначати як «хто» підключається до мережі за його ідентифікаторами, так і «що» підключається, тобто, який пристрій [5]. Визначення пристрою (тобто його профілювання) виконується не тільки на базі MAC-адреси його мережевого адаптера, але також і за рахунок інших параметрів, так як підстановка «коректного» MAC-адреси стала вже повсякденною практикою і без детального аналізу робоча станція зловмисника може стати камерою або сканером із доступом до серверного сегмента.

Після відповіді на питання «хто?» і «що?» система приймає рішення: «що робити?», а саме, чи надавати доступ і, якщо надавати, то куди і з якими правами. Природно, що можливість профілювати пристрій, визначати, яке ПЗ встановлено, його версія та налаштування виходять повніше за наявності встановленого на цій робочій станції клієнтського ПЗ системи NAC, яка в разі корпоративних робочих станцій/ноутбуків встановлюється разом з іншим ПЗ.

Віддалений доступ із нульовою довірою (ZTNA). Різке зростання кількості працівників, які працюють віддалено і потребують підключення до інформаційних ресурсів КІС, призвело до двох результатів: класичний периметр організації ще більше розмився, і зросла роль інших засобів безпеки; важливість системи безпечного, зручного та функціонального віддаленого доступу до ресурсів КІС різко зросла [5].

Класична організація віддаленого доступу з допомогою IPSec VPN часто незручна і вимагає великої кількості додаткових систем безпеки наближення до рівня контролю співробітників у середині периметра, так як у класичному вигляді надто складно контролювати ПЗ, встановлене на віддаленому персональному комп'ютері (ПК), його захист від інтернету та ін.

Впровадження технології/рішення ZTNA дозволяє організовувати безпечне підключення до ресурсу або додатка КІС за рахунок автоматичної побудови шифрованого тунелю або тунелів до ресурсу, або додатка, контролю наявності, версії та функціональності програмного забезпечення, або налаштувань на віддаленій робочій станції.

Найчастіше рішення реалізовано на проміжному шлюзі, який проводить аутентифікацію/авторизацію та перевірку робочої станції та користувача, а також визначає можливість підключення до тих чи інших ресурсів. Ефективні рішення даного класу мають можливість періодично, в рамках сесії, контролювати виконання умов допуску до ресурсів та змінювати авторизацію у разі, якщо умови перестали виконуватись — процедура Change of Authorization (CoA).

Дане рішення функціонально дуже схоже на розглянуте раніше у системі управління доступом до NAC, але контролює віддалений доступ до ресурсів КІС і працює на інших протоколах та інших технічних реалізаціях.

Системи захисту від розподілених атак типу «відмова в обслуговуванні» (DDoS). Однією з найпоширеніших атак у даний час є атака типу відмова в обслуговуванні. В даний час, в основному, зустрічається розподілена версія атаки, яка здійснюється з тисяч IP-адрес. Суть атаки у спробі перевищити пропускну здатність каналу, продуктивність шлюзу, продуктивність IT-систем (серверів, систем зберігання даних тощо) за рахунок генерування, зазвичай з багатьох джерел, великої кількості трафіка у вигляді хибних запитів, сміттєвих даних або спеціальних пакетів, що змушують витрачати на їх обробку надмірну продуктивність. Для розуміння можливостей таких атак можна сказати, що в 2023 р. на

Google була здійснена атака обсягом 298 млн запитів у секунду, що більше, ніж кількість запитів до Вікіпедії за весь вересень 2023 р.

Незважаючи на те, що автори таких атак бувають дуже винахідливими в способах обходу захисту, більшість атак досить прості, їх дешево організувати і вони просто генерують велику кількість сміттєвих даних у спробі переповнити канал даних, процесор шлюзу або MME. Якщо КІС для успішного функціонування необхідний доступ до зовнішніх ресурсів в інтернет/хмарі або навпаки доступ зовнішніх користувачів до ресурсів КІС, а також, якщо об'єднання вузлів КІС відбувається за допомогою шифрованих тунелів в інтернет, то DDoS-атаки можуть бути згубними для роботи КІС і для функціонування підприємства в цілому [6].

Крім цього, DDoS-атаки можуть перевантажувати деякі елементи захисту, що ряд виробників може призводити до пропуска трафіка без контролю перевантаженого пристрою. Можливий також пропуск командою безпеки підозрілих подій внаслідок перемикання уваги на відображення атаки DDoS.

Враховуючи це, захист від DDoS-атак є дуже актуальним завданням і вирішується як на рівні хмарних центрів очищення, так і на рівні сервісів операторів та локальних пристроїв захисту на периметрі КІС.

Системи захисту від атак на портали (WAF). Для забезпечення доступу зовнішніх користувачів до внутрішніх ресурсів КІС необхідно не тільки забезпечити захист від DDoS, але й забезпечити захист самого frontend порталу (по суті вебдодатку) від специфічних атак на вебінфраструктуру. Проблематикою захисту від таких атак займається проєкт забезпечення безпеки вебзастосунків (Open Worldwide Application Security Project — OWASP), відомий публікацією поточного переліку 10 найбільш актуальних способів атаки на вебдодатки (OWASP Top 10). Захист від атак на вебдодаток виконує Web Application Firewall, який встановлюється в інфраструктуру КІС після системи захисту від DDoS, мережевого шлюзу, але перед вебдодатком, що захищається.

Брокери безпечного доступу до хмар (CASB). Коли йдеться про інфраструктуру КІС, зазвичай приділяють увагу ресурсам у середині периметра мережі, але не завжди звертають увагу на ресурси, розташовані у «хмарі», сподіваючись, що їх захистить оператор хмарної інфраструктури, що не було правильним, особливо з урахуванням кількості й швидкості зростання даних та систем, розташованих у «хмарах», а також відсутності зобов'язань операторів захищати дані користувачів від кібератак будь-якого типу (до речі про збереження «хмарних» даних теж повинен піклуватися та копіювати їх власник, а не оператор, за рідкісним виключенням придбання сервісу резервування). Існує цілий клас систем захисту ресурсів у «хмарах». Найбільш відомий із них брокер безпечного доступу, який контролює права користувача для підключення до мережевих ресурсів, виходячи з його автентифікації та поведінкового аналізу, перевіряє безпеку додатка для користувача, забезпечує виявлення хмарних додатків КІС, їх моніторинг та управління на своєму рівні [7]. Для захисту від несанкціонованого доступу система може заблокувати користувача або запропонувати йому пройти ще одну перевірку (використовувати ще один фактор аутентифікації), якщо на підставі впроваджених алгоритмів вважатиме, що його поведінка є аномальною або шкідливою.

Ще однією функціональністю рішення є захист даних від загрози знищення або спотворення, так і від витоку даних (функціональність DLP). Отже, CASB, з одного боку, захищає корпоративні додатки та дані у «хмарі» від неавторизованого доступу та впливу на інформацію, а також від викрадення інформації, а з іншого боку, від шкідливого впливу на робочі станції користувачів, а через них і на всю інфраструктуру КІС у разі компрометації хмарних програм та сервісів.

Системи захисту від шкідливого ПЗ (Malware protection). Антивірусне ПЗ з'явилося дуже давно (майже 40 років тому) і з того часу еволюціонувало разом із еволюцією шкід-

ливого ПЗ. Важливість цієї системи кібербезпеки у складі комплексу безпеки КІС неможливо переоцінити. Це останній рубіж оборони, якщо всі попередні рубежі не впоралися і атака досягла своєї мети – обчислювального пристрою з даними. Система боротьби зі шкідливим ПЗ, у тому числі з невідомим раніше на обчислювальних пристроях, зараз представлена двома типами рішень: Endpoint Detection & Response (EDR) та eXtended Detection & Response (XDR).

Обидві системи забезпечують виявлення відомого шкідливого ПЗ із великою ймовірністю та використовують інтелектуальні методи аналізу поведінки, передбачення та перевірки у пісочниці досліджуваного ПЗ для виявлення невідомого раніше шкідливого коду. Крім цього, такі системи виконують дії, спрямовані на запобігання шкідливим діям та боротьбу зі шкідливим ПЗ. Перевагою сучасних систем є централізація управління детекцією та реакцією для того, щоб інформація про вірус, виявлений на одній робочій станції, повідомлялась на агент антивірусного ПЗ на інших робочих станціях для своєчасного виявлення та знищення шкідливого ПЗ, коли і якщо він потрапить на цю робочу станцію.

Відмінність EDR від XDR полягає в тому, що XDR для виявлення атаки використовує інформацію, одержувану не тільки від робочої станції, а й від мережевих пристроїв, систем кіберзахисту та відповідних баз знань. Необхідно відзначити, що єдиного формалізованого опису, переліку функцій і характеристик XDR зараз немає і кожен виробник вкладає в цю абревіатуру свої бачення і погляд.

Система захисту від атак через електронну пошту (Email protection). Вважається, що зараз електронна пошта є найпоширенішим вектором атак, тобто в більшості випадків брамою кібератаки на КІС стає шкідливе посилання або файл, відкритий користувачем в електронному листі. Тому системи захисту електронної пошти від кібератак є одним із найважливіших компонентів кіберзахисту.

Система захисту електронної пошти полягає у перевірці кожного листа на наявність вбудованих потенційно шкідливих експлойтів та їх блокування; блокування листів, отриманих із скомпрометованих або шкідливих доменів; видалення/блокування посилань на шкідливі або підозрілі сайти; видалення з листа шкідливих файлів та файлів налаштованого типу/розширення; передачі до карантину/пісочниці підозрілих вкладень або вкладень із певними ознаками; попередженні про підозрілий формат, структуру або список адресатів.

Цей функціонал побудований на передбачених правилах обробки з можливістю їх кастомізувати та доповнювати командою безпеки КІС з використанням оновлюваних баз знань шкідливих та підозрілих доменів, адрес, структур листа та хешей вкладень. Можливість перевіряти виконувані та офісні файли в пісочниці для виявлення потенційно шкідливої поведінки також є потужним інструментом захисту поряд з інтелектуальним двигуном самого інструментарію.

Ще одним рівнем захисту електронної пошти, можливо, найголовнішим, є навчання всіх користувачів основам кібербезпеки при роботі з електронною поштою (часто називають кібергігієна) і періодичне тестування їх поведінки.

Система керування мобільними пристроями (EMM/MDM). Захист мобільних пристроїв, які мають доступ до корпоративних даних від злому або несанкціонованого доступу до інформації, з урахуванням різних способів використання, архітектури та ОС, потребує окремих підходів та окремого рішення.

На мобільний пристрій встановлюється клієнтське ПЗ системи EMM/MDM, яке створює шифровану область пам'яті, куди записуються корпоративні програми та дані, доступ до яких здійснюється відповідно до корпоративної політики, встановлюється шифрований тунель у корпоративну мережу, за яким відбувається обмін даними та працюють усі корпоративні програми.

Система EMM/MDM відстежує актуальність версії ОС мобільного пристрою та антивірусного програмного забезпечення й контролює налаштування безпеки мобільного

пристрою. У разі втрати/крадіжки мобільного пристрою розшифрувати корпоративні дані на мобільному пристрої буде дуже важко, майже неможливо. Крім того, адміністратор генерує команду на видалення всіх даних корпоративної області та права доступу в корпоративну мережу з пристрою та бази користувачів КІС.

Система керування обліковими записами та авторизацією користувачів (Identity & Access Management — IAM). Однією з можливостей отримати неавторизований доступ до ІТ-ресурсів КІС є відсутність контролю за життєвим циклом облікових записів та за фактом і історією призначення чи позбавлення прав доступу конкретного співробітника до конкретної системи з конкретними правами. Якщо кількість співробітників обчислюється десятками і немає високої плинності кадрів, то, в теорії, акуратний адміністратор або співробітник відділу кібербезпеки може вести такий журнал, наприклад, в офісному додатку. Але, якщо кількість співробітників/облікових записів обчислюється сотнями і тисячами та/або висока плинність кадрів, то без спеціальної системи управління обліковими записами та доступом (IAM) дуже велика ймовірність наявності неврахованих та непотрібних прав на доступ до систем та/або активних облікових записів звільнених або співробітників, які перейшли на іншу посаду.

Принцип роботи IAM полягає в тому, що ІТ-системи при спробі користувача до них підключитися для підтвердження прав користувача на роботу з ними, звертаються до IAM, яка зберігає в собі всі права користувача для роботи з усіма ІТ-системами компанії, історію їх змін і хто дозволив зміни. Створення облікового запису зі стандартними правами для конкретного підрозділу та посади, зміна прав при переведенні співробітника до іншого підрозділу, а також видалення облікового запису відбуваються автоматично на підставі запису у ПЗ відділу кадрів. Для цього система IAM глибоко інтегрується з системою обліку персоналу (відділ кадрів), із системою управління підприємством (Enterprise Resource Planning — ERP) та корпоративними ІТ-системами.

Система керування привілейованим доступом (Privileged access management — PAM). З погляду маніпулювання даними та ІТ-системами і навіть при видаленні слідів впливу, системний адміністратор є неконтрольованим тому, що має максимум привілеїв для роботи з системою. Вирішення цієї проблеми покладено на систему, яка може контролювати дії адміністратора та тримати його активність під наглядом команди кібербезпеки та його керівництва.

Особливість системи PAM полягає в тому, що її адмініструє команда безпеки і системні адміністратори не мають доступу до її файлів, налаштувань та журналу подій, тобто не можуть впливати на неї. Системи цього класу побудовані як проксі-шлюзи для доступу до адміністрування будь-якої ІТ-системи. Адміністратори мають права на доступ до системи PAM, але не мають доступу до цільових систем. Після підключення до PAM вони запитують доступ до цільових ІТ-систем та отримують його після узгодження відповідно до налаштованих правил та ланцюжка авторизації (офіцер безпеки, керівник, запити на уточнення мети тощо).

Під час сесії всі дії адміністратора контролюються й зберігаються у кількох форматах аж до відео з метою використання у подальшому розслідуванні. При цьому можливе негайне реагування (припинення сесії, повідомлення тощо) на задані команди або дії, наприклад, спроба введення команди на видалення бази даних або руйнування кластера, що призведе до блокування сесії та запиту на команду безпеки й керівника.

Системи захисту фізичного доступу (Physical Access Control — PAC). Особливість комплексних систем безпеки полягає в тому, що, з одного боку, кібернетична інфраструктура захищається системами контролю фізичного доступу від неавторизованого доступу до ІТ-обладнання для його фізичного руйнування або для підключення до локальної консолі систем, яка вважається захищеною та надає набагато більше прав на маніпуляцію з системами, ніж через віддалений доступ. А з іншого боку, кіберзахист не дозволяє зловми-

снику отримати доступ до систем фізичного захисту (контроль фізичного доступу або відеоспостереження) та внести на них зміни для отримання неправомірної авторизації на фізичний доступ до приміщень КІС.

До систем захисту фізичного доступу відносять різні системи сигналізації на території та у приміщеннях; системи контролю та управління фізичним доступом, заснованим на різних способах авторизації та їх комбінаціях (ключ-токен, біометрія (відбиток пальця, малюнок вен, сітківка та ін., пароль/код); системи відеоспостереження з функціями відеоаналітики, розпізнавання та пошуку; ситуаційні центри з функцій аналітики комплексних подій та реакції на них.

Системи захисту від витоку інформації (DLP). Витік даних можливий не тільки внаслідок кібератак та отримання зловмисниками неавторизованого доступу до даних, а й внаслідок навмисного чи випадкового поширення чутливих даних співробітниками організації. Боротися з цією проблемою покликана система DLP. DLP може мати мережевий та хостовий модулі, які борються з витоками даних на відповідних елементах інфраструктури. Робота системи DLP ґрунтується на класифікації інформації/даних/файлів. Способи класифікації можуть бути побудовані на базі міток у файлах, метаданих, розширення файлів, розташування файлів, входження слів у файл тощо, а також класифікація вручну власником інформації або уповноваженою особою.

Сучасні системи DLP можуть попереджати про спробу несанкціонованого поширення інформації, запитувати причини такої спроби для прийняття рішення співробітником безпеки/керівником про дозвіл на цю активність або блокування таких спроб залежно від налаштувань, рівень допуску/дозволу співробітника та ступінь чутливості інформації, але у будь-якому разі інформація про таку спробу зберігається в журналах системи для можливості аналізу в подальшому.

Найкращі зразки систем DLP запобігають витоку багатьма можливими каналами (реального захисту немає тільки від переписування з екрана на листок і фотографування з екрана не на корпоративний телефон, але це також може бути визначено системою аналітики відеоспостереження, якщо воно розгорнуте в робочій зоні). Очевидні та неочевидні канали витоку: електронна пошта, знімні накопичувачі, мережеві та хмарні файлові архіви, соціальні мережі, месенджери, перетворення на зображення, копіювання інформації з файла на файл або інше місце, роздруківка та ін.

При цьому спрацювання системи DLP далеко не завжди свідчить про злий намір, у більшості випадків – це ненавмисне порушення політики співробітниками, що підтверджує необхідність навчання співробітників основам кібергігієни.

Система багатофакторної автентифікації (Multifactor authentication — MFA). Для зловмисника однією з найпривабливіших для злому систем на етапі Exploitation/Privilege Escalation послідовності етапів атак Kill Chain є отримання параметрів доступу до важливих робочих станцій чи систем. Отримання будь-яким способом (клавіатурний шпигун, соціальна інженерія, фішинг тощо) імені та пароля дозволяє проникнути в середину КІС і поширюватися до цільових систем.

Найпростішим способом перешкодити отриманню доступу до ресурсу мережі у такий спосіб є використання багатофакторної аутентифікації, яка передбачає для користувача необхідність пройти аутентифікацію кілька разів, використовуючи різні способи/фактори (комбінація імені та пароля, біометрія, одноразовий згенерований пароль (One Time Password — OTP), USB-ключ та ін.). Така система захищає від компрометації одного способу доступу, наприклад, від неавторизованого використання USB-ключа зловмисником або підглянутого пароля. Багатофакторна автентифікація робить можливість неавторизованого доступу набагато менш імовірним і різко підвищує надійність автентифікації та авторизації.

Системи захисту БД (Database Security — DBS). Практично у 100 % атак метою та найбільшою привабливістю для зловмисників є інформація КІС. У більшості випадків побудови централізованої моделі КІС корпоративні дані зберігаються у відмовостійкому територіально-розподіленому кластері БД. Саме тому отримання доступу до даних, які розташовані в базах даних, або їх знищення є реальною метою атаки. Це може бути виконано одним із розглянутих вище способів: через вразливі робочі станції та сервери, за допомогою привілейованих облікових записів, через помилки та вразливості в порталі та ін., а може бути безпосередньо використано доступ до бази даних з урахуванням її особливості. Тому окремо стоїть завдання захисту систем управління базами даних (СУБД) з урахуванням їх вразливостей, особливостей реалізації та доступу.

Функціями систем захисту БД є прецизійне управління доступами до тих чи інших елементів баз даних або загалом до БД для реалізації моделі рольового доступу користувачів у рамках рекомендацій та законів про захист приватної, медичної та іншої інформації; управління доступами адміністраторів баз даних лише до БД у зоні його відповідальності; контроль коректності, цілісності конфігурації БД та управління її змінами; контроль оновлень СУБД; аудит дій користувачів/додатків та занесення їх до журналу подій; виявлення аномальних активностей у БД та повідомлення про них команди безпеки та/або блокування таких дій, користувачів або програм.

Система аналізу вразливостей (Vulnerability Analysis System — VAS). Досвідчений адміністратор та співробітник команди безпеки розуміє, що всі реалізації програмно-апаратних рішень мають свої особливості, свої тонкі місця та вразливості, якими може скористатися досвідчений зловмисник для виконання атаки. Одні вразливості «закриваються» виробником рішення черговими оновленнями ПЗ, інші вразливості мають рекомендації для заходів щодо запобігання їх використанню, треті вразливості поки що не мають ні таких оновлень, ні рекомендацій і просто відомі. Крім того, існують вразливості, для використання яких зловмисники вже розробили шкідливе ПЗ та вразливості, для яких поки що таке ПЗ не випустили або поки що такою вразливістю неможливо або вкрай складно скористатися.

Системи аналізу вразливостей якраз і проводять (періодично або постійно) сканування інфраструктури на виявлення таких відомих вразливостей із наданням звіту за результатами, в якому вказується вразливість, знайдена в конкретному елементі КІС, рекомендації щодо усунення цієї вразливості. Кожній знайденій вразливості надається рейтинг залежно від серйозності наслідків її експлуатації та можливості її скористатися для того, щоб команда безпеки пріоритезувала роботи з усунення даних вразливостей, а за неможливості усунути вразливість купірувала її за допомогою інших систем.

Система імітації атак (Breach and Attack Simulation — BAS). Команді безпеки необхідно розуміти, наскільки вжиті дії та зусилля захистили інфраструктуру КІС від атак та проникнення. Чи все враховано і чи всі проломи та вразливості закриті (наскільки це можливо). Для цього виконують процедуру «тест на проникнення» (penetration testing), яка виконується командою і виконує роль атакуючого зловмисника (red team). Ця команда може складатися з фахівців самого підприємства (якщо вони мають відповідну компетенцію) або це може бути зовнішня команда фахівців у даному напрямі.

Цей тест виконується періодично, раз на рік або раз на півроку. Отже, команда кібербезпеки підприємства сподівається, що тест було виконано професійно, у них все добре і не з’явилися ніякі нові проломи/вразливості. Альтернативою такого періодичного тестування є використання системи імітації атак, яка налаштовується на ІТ-ландшафт КІС і запускає набір атак для всіх існуючих у КІС ІТ-систем та систем кібербезпеки, а також імітацію атак, розрахованих на слабку ланку захисту — користувача.

Такі симуляції атак можуть запускатися так часто, як це може бути ефективно для даної інфраструктури в автоматичному або автоматизованому режимі. Команда безпеки

вивчає підготовлені звіти з рекомендаціями щодо усунення знайдених «дір» у захисті та виконує «роботу над помилками» з наступним перезапуском симуляції атаки для підтвердження успішного виправлення знайдених проблем.

Система кіберпасток (Deception). Існує статистика, що в середньому з моменту проникнення зловмисників у IT-інфраструктуру підприємства до ідентифікації самого факту проникнення проходить понад 200 днів, а до моменту визначення, де і як сталося проникнення, ще більше 70 днів, причому за останні 5 років ці терміни принципово не змінювалися [8].

Найшвидше визначення факту вторгнення та скорочення терміну присутності зловмисників у IT-інфраструктурі для мінімізації збитків і втрат, якщо проникнення все ж таки вдалося, — основне завдання комплексу систем аналітики кібербезпеки. Один із найефективніших засобів виявлення злому є системи кіберпасток (Deception, Honeypot тощо). Принцип дії цих систем полягає у створенні фіктивних корпоративних IT-ресурсів, надто привабливих для зловмисника (каталог AD, БД, поштові сервери, системи управління підприємством, бухгалтерські програми тощо), які мають усі ознаки реальних систем, створюють той самий профіль трафіка, мають ті самі відкриті порти, але при цьому дають можливість себе виявити і підключитися. Факт спроби підключення, а також поведінки після підключення (фіктивний ресурс на відміну від справжнього можна легко виявити в інфраструктурі і він недовго чинить опір злому) сигналізує про те, що в інфраструктуру проник зловмисник. З його поведінки можна зробити висновки про цілі та спосіб проникнення для того, щоб підготуватися до захисту реальних ресурсів, убезпечити дані та постаратися виявити фізично зловмисника, поки він розбирається з фіктивною інформацією на фіктивному ресурсі.

Система збору, кореляції, аналізу журналів та дій (SIEM). Для того, щоб ідентифікувати спробу злому або шкідливу активність зловмисника в IT-інфраструктурі КІС, необхідно мати повну видимість усіх процесів у КІС. Для цього необхідно зібрати та проаналізувати багато тисяч записів у журналах подій, події безпеки та велику кількість іншої інформації. В результаті кореляції даних від багатьох IT-систем та систем кібербезпеки може бути виявлений кіберінцидент. Вважається, що тільки так можна виявити сучасні багатовекторні цільові атаки, спеціально розроблені для атаки на дану інфраструктуру. Саме такі атаки прийнято називати цільовою постійною загрозою підвищеної складності (Advanced persistent threat — APT), які несуть найбільшу загрозу.

Нездатність реальної команди кібербезпеки підприємства обробити, проаналізувати та прокорелювати десятки тисяч подій та записів на день привела до появи системи автоматичного збору, аналізу та кореляції подій в інфраструктурі, завданням якої є автоматичний збір подій у системі та аналіз за налаштованими правилами для виявлення потенційного інциденту безпеки та передачі інформації про нього команді безпеки для проведення розслідувань, прийняття рішення про наявність інциденту та реакції на нього. У періоди між цілеспрямованими масованими атаками на організацію таких інцидентів у середньому в організації з'являється на 2–5 день, що вже реально розслідувати силами кваліфікованої команди безпеки.

Система автоматизації дій під час розслідування чи реакції на інцидент (Security Orchestration Automation and Response — SOAR). У розслідуванні інциденту та реакції на нього важливе запобігання або зменшення шкоди від атаки, а, отже, мінімізація часу присутності зловмисників в інфраструктурі КІС, так як поки команда безпеки ідентифікує та локалізує присутність зловмисника в IT, зловмисник продовжує шкідливі дії. У процесі розслідування та реакції на інцидент дуже багато дій є рутинними й характерними для тієї чи іншої атаки чи активності. Наприклад, такі дії під час розслідування: з'ясування атакуючих IP-адрес, країни, історія появи та досвід боротьби, схожі атаки на цей же ресурс тощо, а для реакції: блокування даної IP-адреси або поштового домену, видалення або бло-

кування активного контенту та вкладень у всіх листах із даного поштового домену, відправлення файлів, відповідних ряду ознак, на перевірку в пісочницю, відключення від мережі даної робочої станції, блокування або зниження прав доступу для скомпрометованого облікового запису, запуск відповідних додатків та ін. Кожна команда безпеки сама формує послідовність дій, характерних для тієї чи іншої ситуації.

Виконання даних дій автоматично або автоматизовано за командою оператора або за тригера появи того чи іншого інциденту дозволяє економити десятки і сотні хвилин у самій напруженій стадії розслідування та реакції, що може істотно знизити ту шкоду, яку завдає зловмисник.

Автоматизацію процесів у кібербезпеці здійснюють системи класу SOAR, які мають велику кількість вбудованих послідовностей дій для більшості стандартних ситуацій, дозволяють налаштовувати та створювати нові послідовності дій. Створення нового набору команд/дій може виконати спеціаліст безпеки без навичок програмування, у графічному інтерфейсі, методом перетягування у правильне місце на схемі відповідних піктограм дій та стрілок умовних і безумовних переходів.

Для ефективної взаємодії з IT-інфраструктурою та системами безпеки SOAR мають вбудовану інтеграцію з абсолютною більшістю існуючих IT-систем та систем кібербезпеки, які дозволяють SOAR отримувати додаткову інформацію для збагачення події та виконання необхідних дій. Крім того, якщо такої інтеграції немає, то SOAR дозволяє створювати інтерфейси до третіх систем на основі вбудованого інструментарію.

4. Архітектура КСІК

Перелічені вище системи безпеки створюють екосистему корпоративної безпеки у складі чотирьох згаданих кластерів: безпека робочих станцій, безпека даних, мережева безпека та аналітика. Вибір необхідних систем кіберзахисту для побудови КСІК визначається на етапі проєктування з урахуванням IT-ландшафту, структури корпоративної мережі, критичності IT-ресурсів тощо.

У кожному конкретному випадку склад КІСК може відрізнятися залежно від наявності та важливості тієї чи іншої IT-системи. Наприклад, якщо немає порталу або його функціональність некритична, то необхідність WAF сумнівна.

Принципово важливими компонентами є рішення щодо захисту мережі типу NGFW, захисту робочих станцій і серверів від шкідливого ПЗ на базі EDR/XDR, захисту системи електронної пошти. Рекомендованими компонентами також є система управління доступом до NAC та віддаленим доступом з нульовою довірою, захист від витоків інформації, комплекс систем автентифікації та авторизації.

Рішення про доцільність використання інших систем кібербезпеки залежить від наявності відповідних IT-систем в організації, які потрібно захищати даною технологією кіберзахиста. При цьому для організацій середнього та великого розміру або з середньою чи високою складністю IT-ландшафту системи кластера аналітики кібербезпеки є критично важливими, особливо системи збору та кореляції подій та система аналізу вразливостей. Така увага системам аналітики приділяється передусім тому, що багато сучасних атак можна виявити тільки в результаті аналізу подій у кількох системах. При цьому кожна така подія в гіршому випадку буде підозрілою, але не викличе реакції спеціалізованої системи кіберзахисту – фаєрволу, захисту кінцевої точки тощо. Тільки сукупність цих подій може виявити факт здійснювання багатовекторної атаки. Також рекомендованими для включення до складу КСІК є система кіберпасток і система оркестрації та автоматизації реакції. Враховуючи вищевикладене, архітектура КСІК має бути такою (рис. 1).

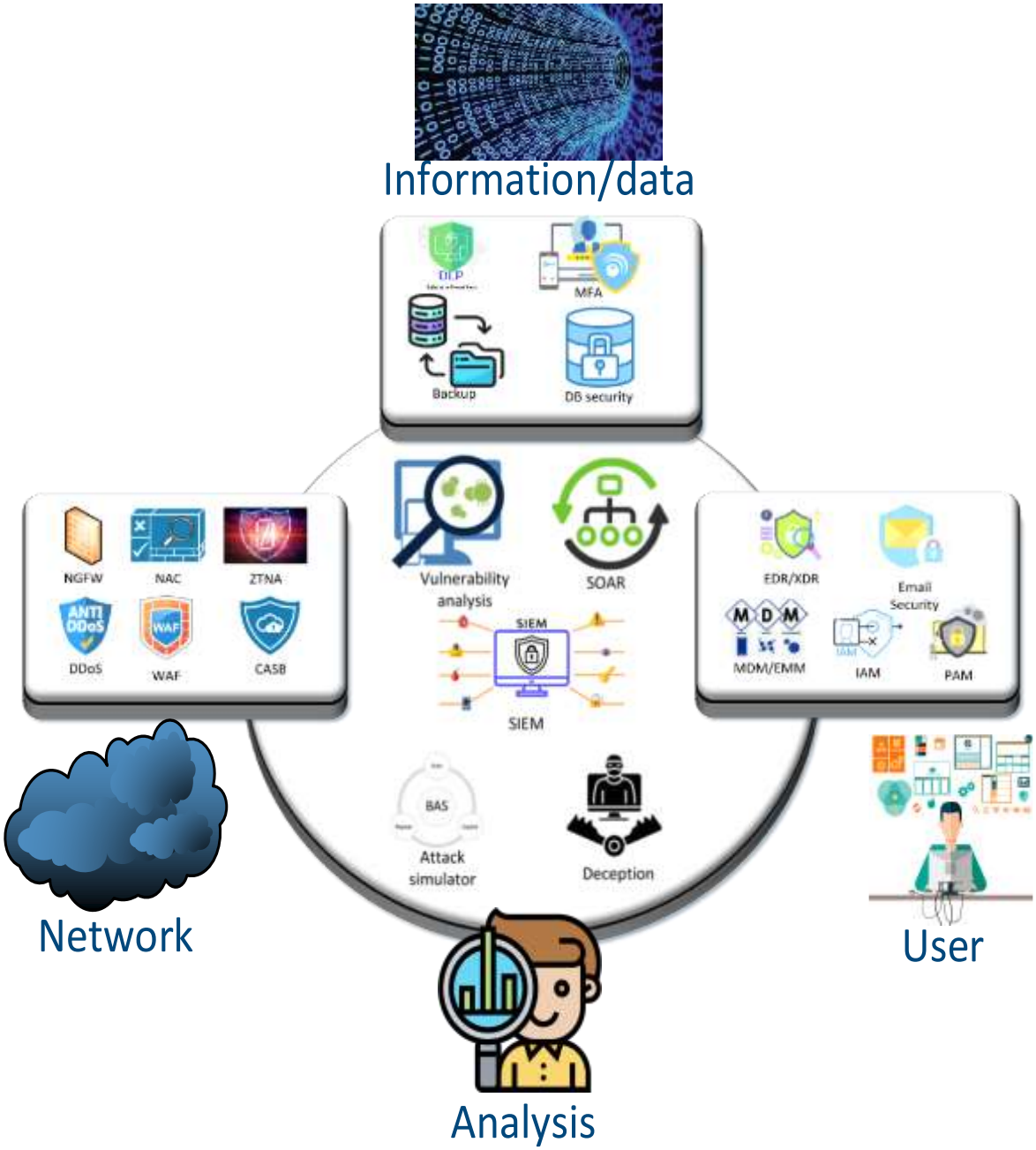

Рисунок 1— Архітектура КСІК

Крім розглянутих технічних засобів захисту від кібератак, суттєва увага повинна приділятися навчанню співробітників та адміністраторів. Вважається, що до 40 % атак спрямовані на вразливість людини, це так звана соціальна інженерія. Цей термін описує вивчення конкретної людини або групи людей для того, щоб зрозуміти їхню реакцію на запит, підготувати для них найбільш привабливе послання з тим, щоб вони стали точкою проникнення атаки в КІС.

5. Висновки

Отже, сукупність описаних технологій кіберзахисту, правильний вибір необхідних систем захисту від специфічних загроз, побудова аналітичної платформи аналізу подій, пошуку загроз та реакції на них дозволять побудувати ешелоновану систему ефективного кіберзахисту КІС. Постійне навчання співробітників кібергігієні, тестування та робота над помил-

ками можуть бути організовані в автоматизованому режимі за допомогою систем класу Security awareness training system, застосування яких може суттєво підвищити загальну кібербезпеку компанії. Крім того, існують спеціальні навчальні програми та полігони, які дозволяють підвищувати кваліфікацію та напрацьовувати досвід спеціалістам команди кіберзахисту.

СПИСОК ДЖЕРЕЛ

1. Економіка і регіон. URL: https://eir.nupp.edu.ua/files/2022/1_84_2022.pdf (дата звернення: 10.01.2023).
2. Лисецький Ю.М. Забезпечення інформаційної безпеки. *Global science: prospects and innovations:* зб. статей III Міжнар. наук.-практ. конф. (м. Ліверпуль, 2–4 лист. 2023 р.). Великобританія, Ліверпуль, 2023. С. 273–276.
3. Лисецький Ю.М., Калбазов Д.І. Інформаційна безпека корпоративних баз даних. *Математичні машини і системи*. 2023. № 3. С. 31–37.
4. Міжмережевий екран: що це та як працює? URL: https://ukeywaf.com/baza/mizhmerezhevyj-ekran-shho-cze-yak-praczyuye/ (дата звернення: 10.01.2023).
5. Лисецький Ю.М. Управління доступом до IT-систем. *Scientists and existing problems of human development*: зб. тез IX Міжнар. наук.-практ. конф. (м. Загреб, 14–17 лист. 2023 р.). Хорватія, Загреб, 2023. С. 378–379.
6. Лисецкий Ю.М. Информационная безопасность: защита от DDoS-атак. *System Analysis and Information Technologies SAIT 2014*: 16-th International conf. (Kyiv, 26–30 May 2014). Kyiv, 2014. P. 405–406.
7. Лисецький Ю., Калбазов Д. Особливості управління правами користувачів у корпоративних IT-системах. *Математичні машини і системи*. 2023. № 2. С. 28–33.
8. IBM Security Cost of a Data Breach Report. 2023. URL: https://www.ibm.com/reports/data-breach (дата звернення: 10.01.2023).

Стаття надійшла до редакції 18.03.2024