УДК 004

М.Іванченко, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО КОРПОРАТИВНОГО ЦЕНТРУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (SOC)

У статті розроблено програмне забезпечення, яке призначено для системи мережевого корпоративного центру управління інформаційною безпекою (SOC). Метою розробки є дослідження та принципи побудови системи мережевого корпоративного центру управління інформаційною безпекою (SOC). Об'єктом дослідження є процес мережевого корпоративного центру управління інформаційною безпекою (SOC). Предметом дослідження є методи мережевого корпоративного центру управління інформаційною безпекою (SOC). Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевого корпоративного центру управління інформаційною безпекою (SOC). В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

центр управління інформаційною безпекою (SOC)

Постановка проблеми. Центр операцій безпеки (SOC) – це централізований підрозділ, який займається питаннями безпеки на організаційному та технічному рівні. SOC оснащений командою аналітиків та інженерів з безпеки, а також сучасними технологіями виявлення та запобігання для моніторингу, аналізу та реагування на інциденти кібербезпеки.

Головною метою SOC є виявлення, оцінка, пом'якшення та звітування про кіберзагрози, забезпечення запобігання або раннього виявлення потенційних порушень безпеки та своєчасного реагування на них. Це включає постійний спостереження за IT-інфраструктурою організації, включаючи її мережі, пристрої, програми та дані, для захисту від загроз безпеці, починаючи від атак шкідливого програмного забезпечення до складного кібершпигунства.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого корпоративного центру управління інформаційною безпекою (soc).

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого корпоративного центру управління інформаційною безпекою (SOC).

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань: Огляд існуючих систем мережевого корпоративного центру управління інформаційною безпекою (SOC).; Дослідження системи мережевого корпоративного центру управління інформаційною безпекою (SOC).; Програмна реалізація системи мережевого корпоративного центру управління інформаційною безпекою (SOC).

Об'єктом дослідження є процес мережевого корпоративного центру управління інформаційною безпекою (SOC).

Предметом дослідження є методи мережевого корпоративного центру управління інформаційною безпекою (SOC).

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Центр операцій безпеки (SOC) – це команда експертів з інформаційної безпеки, які відповідають за моніторинг, виявлення, аналіз, запобігання та реагування на інциденти безпеки. Керований Центр операцій безпеки зазвичай надає консультації, розробку послуг та підтримку організаціям, яким потрібна зовнішня експертиза для захисту від загроз безпеці.

Окрім реагування на вторгнення, SOC також моніторить мережі на предмет незвичайної активності, такої як моделі трафіку, поведінка користувачів або зміни в обмеженнях доступу. Якщо щось здається підозрілим, SOC досліджує це, переглядаючи журнали та файли конфігурації на комп'ютерах і серверах, щоб з'ясувати, що сталося.

Центр кібербезпеки (SOC) можна розглядати як центральну нервову систему мережі, оскільки цей відділ відповідає за постійний моніторинг систем та проведення аналізу для виявлення та запобігання інцидентам кібербезпеки. Мета полягає в тому, щоб діяти до того, як станеться інцидент, але при цьому слід бути готовим до відновлення після інциденту, що складається з нової загрози.

SOC повинна швидко виявляти проблеми та встановлювати їхню серйозність, а також пропонувати рішення для запобігання атакам та припинення будь-яких поточних загроз.

Як працює Центр операцій безпеки

Центр безпеки (SOC) надає критично важливу інформацію про безпеку, щоб команди могли швидко реагувати на кіберінциденти. SOC збирають, співвідносять та аналізують дані з усіх різних комп'ютерів та мереж в організації. Це включає моніторинг у режимі реального часу, виявлення та реагування на оцінку вразливостей, виявлення вторгнень, аналіз та запобігання шкідливому програмному забезпеченню, мережеву криміналістику, а також технічне обслуговування та усунення несправностей.

Центри безпеки (SOC) найчастіше керуються спеціалізованим членом команди безпеки, який працює цілодобово, щоб контролювати активність у кількох системах та сегментах мережі. Член SOC розробляє звіти, використовуючи інформацію, отриману з журналів, для відстеження атак. Інформація, надана SOC, може бути використана для визначення пріоритетів реагування, визначення найбільш критичних вразливостей у середовищі та швидкої оцінки загального стану безпеки.

SOC має доступ до всіх різних компонентів безпеки в мережі, включаючи брандмауери, системи виявлення вторгнень (IDS), брандмауери додатків, балансувальники навантаження та веб-проксі. Член SOC може об'єднати ці різнорідні фрагменти інформації в одну цілісну картину того, що відбувається в середовищі. Крім того, член SOC може використовувати цю інформацію для швидкої оцінки всіх аспектів середовища, включаючи аномалії в трафіку та даних, нові оцінки вразливостей, незвичайну поведінку відомих інструментів та скриптів шкідливого програмного забезпечення, незвичайну активність веб-додатків, результати тестування на проникнення та інші події.

SOC не замінюють традиційні команди безпеки; радше вони забезпечують їм критичний рівень для покриття прогалин, які команди безпеки не можуть безпосередньо усунути.

Чому SOC такий важливий для бізнесу

Безпека – це дуже важливо. Якщо ви не захищаєтеся від зловмисників, ваша компанія може зазнати масової втрати даних або іншої конфіденційної інформації. І саме тому Центри операцій безпеки такі важливі – вони допомагають великим компаніям контролювати свою безпеку та захищатися від хакерів цілодобово, щодня.

Раніше компанії просто мали когось за столом, хто стежив за будь-якими потенційними загрозами. Але цього вже недостатньо. Зі зростанням компаній, а їхні процеси (і навіть їхні власні системи безпеки) ускладнювалися, вони виявили, що відстеження всього може бути мамонтовим завданням.

Атаки методом грубої сили на корпоративні мережі стають дедалі поширенішими. Вони можуть коштувати чимало грошей, і коли зловмисник намагається зламати захист однієї корпоративної мережі, стає зрозуміло, що витрачати гроші на найм людей по суті

марно, коли справа доходить до визначення реального рівня загрози. Потрібен високотехнологічний моніторинг самих систем безпеки. Те, що починалося як проста ідея для Центрів операцій безпеки, тепер перетворилося на величезну галузь, яка спирається на висококваліфікованих фахівців, які стежать за всім одночасно, забезпечуючи безпеку та надійність корпоративних даних.

Ключові переваги SOC

Звісно ж, наявність SOC має довгий список переваг для бізнесу. Ось деякі з них: 1) Центр операцій безпеки дозволяє компаніям збирати відповідні дані в одному центральному місці. 2) Центр операцій безпеки покращує здатність компаній швидко та рішуче реагувати на нові загрози. 3) Компанії, які інвестують у центри безпеки, з більшою ймовірністю дотримуються правил, що регулюють кібербезпеку. 4) Компанії з центром безпеки мають легшу співпрацю з правоохоронними органами. 5) Центр операцій безпеки дозволяє компаніям швидше виявляти вторгнення та атаки й мінімізувати їх вплив. 6) Центр операцій безпеки дозволяє компаніям краще навчати своїх співробітників кіберризикам та способам їх уникнення. 7) Центр операцій безпеки покращує можливості компаній контролювати активність авторизованих користувачів у своїх системах, значно зменшуючи внутрішні загрози. 8) Наявність центру операцій безпеки покращує можливості компаній моніторити, реагувати та повідомляти про кіберзагрози. 9) Наявність центру операцій безпеки дозволяє компаніям централізувати моніторинг, скорочуючи час повідомлення про інцидент та забезпечуючи швидше вирішення проблем. 10) Центр операцій безпеки дозволяє компаніям надавати кращі послуги своїм клієнтам, дотримуючись галузевих стандартів та державних норм. 11) Центр операцій безпеки дозволяє компаніям бути проактивними, а не реактивними, у боротьбі з кіберзагрозами. 12) Компанії, які інвестують у центри безпеки, з меншою ймовірністю стануть мішенню кіберзлочинців. 13) Центр операцій безпеки дозволяє компаніям дотримуватися галузевих стандартів щодо найкращих практик кібербезпеки. 14) Інвестиції в центр операцій безпеки дозволяють компаніям бути проактивними та звітувати про свої заходи управління ризиками, покращуючи свою репутацію як серед клієнтів, так і серед акціонерів. 15) Центри операцій безпеки дозволяють компаніям уникати штрафів та судових позовів, що виникають унаслідок витоків даних.

Які найбільші проблеми центрів безпеки операцій?

Відстеження загроз та мінімізація їхнього впливу на підприємство є постійним викликом для компаній, але цей виклик став легшим з розвитком технологій. Центри операцій безпеки є критично важливими для інформаційної безпеки. Вони відповідають за моніторинг, оцінку та захист IT-активів.

Ця відповідальність вимагає значного планування та знань як IT-інфраструктури, так і принципів кібербезпеки для успішного виконання. Постійно зростаюча мережева інфраструктура, старіюче обладнання, величезна площа атак та скорочення бюджетів ускладнюють їхню роботу.

Щоб подолати ці проблеми, центри операцій безпеки повинні впроваджувати інновації та автоматизацію для централізації своїх даних. Це означає перехід від розрізненої, ізольованої інформації до централізованої платформи, де їхні дані доступні та використовуються для спільного використання. Цей крок може бути особливо важливим для компаній з центрами операцій фізичної безпеки (SOC), оскільки вони мають найбільшу потребу в прозорості та більших засобах захисту від фізичних загроз.

Майбутнє державних операційних компаній

У світі, де кіберзлочинці стають дедалі витонченішими, Центри операцій безпеки повинні мати можливість швидко адаптуватися та розвиватися, щоб залишатися на крок попереду конкурентів. Це означає, що їм необхідно мати ресурси та підтримку IT-відділу своєї компанії, а також інструменти, доступні для успішної роботи команд безпеки. Майбутнє центрів операцій безпеки буде рухомим, реагуючи на загрози в режимі реального часу за допомогою автоматизації та машинного навчання. Однак вони ніколи не зможуть

замінити кваліфікованих та відданих фахівців з безпеки, яким доводиться виконувати складну роботу.

У складному та швидкозмінному ландшафті сучасних кіберзагроз організації стикаються з безпрецедентним викликом у захисті своїх цифрових активів, конфіденційних даних та забезпеченні безперервності операційної діяльності. Величезний обсяг та складність кібератак вимагають централізованого, проактивного та вузькоспеціалізованого підходу до безпеки. Саме тут Центр операцій безпеки (SOC) стає невід'ємним компонентом загальної стратегії кібербезпеки організації.

Центр операцій безпеки (SOC) – це централізована функція в організації або послуга, що надається третьою стороною, яка займається постійним моніторингом та аналізом стану безпеки організації. Його основна мета – виявляти, запобігати, розслідувати та реагувати на кіберінциденти та загрози цілодобово. SOC – це набагато більше, ніж просто набір інструментів безпеки, це нервовий центр, де люди, процеси та технології сходяться для забезпечення комплексних операцій безпеки. Він являє собою фундаментальний перехід від реактивних заходів безпеки до проактивного, заснованого на розвідці захисного механізму, призначеного для захисту організації від безлічі потенційних загроз, що ховаються в цифровому світі.

Основна роль Центру операцій безпеки (SOC): понад базовий захист

Роль SOC виходить далеко за рамки простого реагування на сповіщення; вона втілює стратегічний імператив підтримки цифрової стійкості. В епоху, коли кіберзагрози є постійними та дедалі складнішими, багато організацій усвідомлюють, що надійна система безпеки вимагає цілеспрямованого експертного нагляду. Команда операцій безпеки в SOC має головне завдання: забезпечити конфіденційність, цілісність та доступність (тріада ЦРУ) інформаційних активів організації.

Центр безпеки (SOC) діє як центральний розвідувальний центр, постійно збираючи та зіставляючи інформацію про безпеку з усього IT-середовища. Це включає дані з мереж, серверів, кінцевих точок, програм, баз даних та різних інструментів безпеки. Консолідуючи цей величезний обсяг інформації, аналітики SOC отримують цілісне уявлення про ландшафт безпеки, що дозволяє їм виявляти підозрілу активність, яка в іншому випадку могла б залишитися непоміченою. Така всебічна видимість має вирішальне значення для ефективного виявлення загроз, розслідування та швидкого реагування на інциденти. Стратегічна цінність SOC полягає в його здатності перетворювати необроблені дані безпеки на дієву інформацію, що дозволяє командам безпеки не лише виявляти та стримувати загрози, але й розуміти їх походження та запобігати майбутнім випадкам.

Ключові функції та обов'язки SOC

Щоденна діяльність SOC охоплює широкий спектр функцій, кожна з яких є критично важливою для створення та підтримки надійної системи безпеки. Ці функції виконує спеціальна команда аналітиків та фахівців з безпеки, використовуючи передові рішення безпеки та чітко визначені процеси.

Безперервний моніторинг безпеки та сортування за тривогами

Одним з основоположних обов'язків SOC є постійний моніторинг усіх систем, мереж та програм у режимі реального часу в інфраструктурі організації. Ця цілодобова пильність спрямована на виявлення будь-яких ознак аномальної поведінки або потенційних загроз. Процес моніторингу генерує велику кількість сповіщень від різних інструментів безпеки, таких як брандмауери, системи виявлення/запобігання вторгненням (IDS/IPS), рішення для виявлення та реагування на мережу (NDR), рішення для виявлення та реагування на кінцеві точки (EDR) та системи управління інформацією та подіями безпеки (SIEM).

Аналітики SOC відповідають за початкове сортування цих сповіщень, розрізняючи справжні інциденти безпеки та хибнопозитивні результати. Це вимагає глибокого розуміння нормальної поведінки мережі та законної системної активності. Ефективне сортування значно знижує втому від сповіщень, дозволяючи команді зосередити свою увагу та ресурси

на критичних подіях, які становлять реальний ризик. Мета полягає в тому, щоб швидко виявити підозрілу активність, перш ніж вона переросте в повноцінну кібератаку.

Виявлення та аналіз загроз

Після того, як сповіщення класифікується як потенційно шкідливе, команда SOC розпочинає глибше розслідування виявленої загрози. Це включає детальний аналіз журналів, даних мережевого трафіку, телеметрії кінцевих точок та іншої відповідної інформації безпеки, щоб зрозуміти природу, масштаб та потенційний вплив інциденту безпеки. Аналітики використовують розширену аналітику, моделювання поведінки та можливості машинного навчання, часто інтегровані в їхні інструменти безпеки, щоб зіставити, здавалося б, різнорідні фрагменти інформації та виявити закономірності, що вказують на кіберзагрозу.

Використання актуальної інформації про загрози є надзвичайно важливим на цьому етапі. Канали інформації про загрози надають інформацію про відомі вразливості, нові вектори атак, тактику, методи та процедури зловмисників (TTP), а також індикатори компрометації (IoC). Зіставляючи внутрішні спостереження із зовнішньою інформацією про загрози, аналітики SOC можуть точніше ідентифікувати загрози, розуміти їхні характеристики та прогнозувати їх потенційний розвиток, що дозволяє проводити більш ефективні та цілеспрямовані операції безпеки.

Реагування на інциденти та їх усунення

Кінцева мета виявлення загроз полягає в забезпеченні швидкого та ефективного реагування на інциденти. Коли виявляється підтверджений інцидент безпеки, команда SOC негайно запускає план реагування на інцидент. Цей критичний процес зазвичай включає кілька фаз: Ідентифікація: Підтвердження інциденту та збір початкової інформації; Стримування: Вжиття негайних заходів для ізоляції уражених систем або мереж, щоб запобігти подальшому поширенню інциденту. Це може включати відключення пристроїв, блокування IP-адрес або карантин шкідливого програмного забезпечення; Викорінення: Усунення першопричини інциденту, наприклад, видалення шкідливого програмного забезпечення, виправлення вразливостей або видалення шкідливих конфігурацій; Відновлення: Відновлення уражених систем і даних до нормального стану, що може включати відновлення з резервних копій, перебудову систем або переналаштування засобів безпеки; Аналіз після інциденту (вивчені уроки): Вирішальний крок, під час якого команда аналізує, що сталося, чому це сталося та як запобігти подібним інцидентам у майбутньому. Цей цикл зворотного зв'язку зміцнює загальний рівень безпеки організації.

Швидкість і точність реагування на інциденти є життєво важливими для мінімізації збитків, скорочення простоїв та підтримки довіри в організації. Фахівці з реагування на інциденти SOC співпрацюють, часто з іншими IT-відділами, для ефективного усунення загроз.

Управління вразливостями та оцінка ризиків

Проактивний SOC виходить за рамки реагування на активні загрози; він активно працює над зменшенням поверхні атаки організації. Це передбачає постійне управління вразливостями, яке включає виявлення, оцінку та визначення пріоритетів слабких місць безпеки в системах, додатках та мережевій інфраструктурі. Команди SOC часто проводять регулярне сканування вразливостей, тести на проникнення та аудити безпеки, щоб виявити потенційні точки входу для зловмисників.

Після виявлення вразливостей, SOC співпрацює з командами IT-операцій, щоб забезпечити своєчасне встановлення виправлень, посилення конфігурації та впровадження політик безпеки, розроблених для зменшення цих ризиків. Проактивно усуваючи слабкі місця, SOC допомагає зміцнити загальний рівень безпеки та зменшити ймовірність успішних кібератак. Оцінка ризиків – це безперервний процес, який оцінює потенційний вплив виявлених вразливостей та загроз на бізнес-операції та дані.

Полювання на загрози: проактивний захист

Хоча постійний моніторинг та автоматичні сповіщення є важливими, вони часто реагують на відомі загрози або заздалегідь визначені правила. З іншого боку, полювання на

загрози – це проактивний та ітеративний процес, у якому аналітики безпеки, яких часто називають мисливцями за загрозами, активно шукають невідомі або невиявлені загрози, що ховаються в мережі організації. Це передбачає використання глибокого контекстуального розуміння середовища, розвідки загроз та розслідувань на основі гіпотез.

Мисливці за загрозами працюють, виходячи з припущення, що організація вже була скомпрометована або зазнає малопомітної атаки. Вони шукають аномальну поведінку, малопомітні індикатори компрометації (IoC) та відхилення від нормальних базових показників, які автоматизовані інструменти можуть пропустити. Ця вузькоспеціалізована функція вимагає розширених аналітичних навичок, глибоких знань методологій зловмисників та доступу до багатих, детальних джерел даних, особливо до мережевих пакетних даних. Мета полягає у виявленні складних, прихованих кіберзагроз, таких як передові постійні загрози (APT), перш ніж вони зможуть завдати значної шкоди.

Інтеграція з управлінням інформацією та подіями безпеки (SIEM)

Система управління інформацією та подіями безпеки (SIEM) є базовою технологією майже для кожної SOC. Рішення SIEM агрегує та централізує дані журналів і подій практично з кожного пристрою та програми в IT-інфраструктурі організації. Це включає дані з брандмауерів, серверів, операційних систем, мережевих пристроїв, інструментів безпеки та програм.

Потім SIEM нормалізує ці різнорідні дані, роблячи їх узгодженими та зручними для пошуку. Найголовніше, що SIEM використовує правила кореляції та аналітичні механізми для виявлення закономірностей та зв'язків у даних, які вказують на підозрілу активність або потенційні інциденти безпеки. Наприклад, він може співвіднести невдалу спробу входу на одному сервері з успішним входом з того ж облікового запису користувача на іншому сервері в незвичному місці, позначаючи це як потенційну компрометацію.

Ключова відмінність між SIEM та SOC полягає в тому, що SIEM є потужним інструментом, який використовується *SOC*. SOC – це операційна команда та об'єкт, який використовує SIEM (разом з багатьма іншими інструментами та процесами) для досягнення своїх цілей моніторингу, виявлення, аналізу та реагування на загрози. Без SIEM здатність SOC отримувати повну видимість та співвідносити події була б серйозно обмежена, що зробить виявлення загроз, розслідування та реагування на інциденти набагато складнішими та трудомісткішими.

Автоматизація та оркестрація безпеки (SOAR)

Щоб впоратися зі зростаючим обсягом та складністю інцидентів безпеки, багато сучасних центрів охорони безпеки (SOC) інтегрують платформи оркестрації, автоматизації та реагування на безпеку (SOAR). Технології SOAR дозволяють командам SOC стандартизувати, автоматизувати та оркеструвати робочі процеси операцій безпеки.

Автоматизація передбачає автоматичне виконання завдань і процесів, таких як блокування шкідливої IP-адреси, виявленої за допомогою сповіщення SIEM, ізоляція зараженої кінцевої точки або збагачення інциденту даними розвідки про загрози. Оркестрація означає координацію кількох інструментів та систем безпеки для безперебійної спільної роботи в межах визначеного робочого процесу, часто ініційованого сповіщенням. Можливості реагування в SOAR надають інструменти для управління інцидентами, співпраці та створення звітів.

Впровадження автоматизації та оркестрації значно підвищує ефективність та швидкість роботи SOC. Це зменшує ручне навантаження на аналітиків безпеки, дозволяючи їм зосередитися на складних розслідуваннях та стратегічному пошуку загроз, а не на повторюваних завданнях. Це також призводить до швидшого реагування на інциденти, мінімізуючи вікно можливостей для зловмисників та зменшуючи потенційний вплив кібератаки.

Відповідність та звітність

Окрім безпосереднього зменшення загроз, SOC відіграє вирішальну роль у забезпеченні дотримання організацією різних нормативних вимог та галузевих стандартів.

Багато організацій підпадають під дію таких вимог щодо дотримання, як GDPR, HIPAA, PCI DSS та SOX, які вимагають суворого контролю безпеки та надійних механізмів звітності. SOC постійно контролює системи, щоб забезпечити їх відповідність цим правилам та внутрішнім політикам безпеки. Вони генерують детальні звіти про стан безпеки, виявлені інциденти, вразливості та зусилля з усунення наслідків, надаючи необхідну документацію для аудитів та демонструючи належну перевірку. Ця звітність не лише служить регуляторним цілям, але й надає вищому керівництву цінну інформацію щодо стану безпеки організації та поточних ризиків, допомагаючи приймати стратегічні рішення та розподіляти ресурси для рішень безпеки.

Неперевершена потужність пакетних даних у SOC

Хоча журнали та сповіщення надають цінну інформацію про те, що сталося в системі, вони часто пропонують узагальнений або відфільтрований огляд подій. Для справді повного розуміння мережевої активності та найдеталізованішого рівня деталізації, необхідного для розширеного виявлення та пошуку загроз, SOC значною мірою покладається на дані мережевих пакетів. Цей необроблений, нефільтрований потік інформації, що проходить мережею, забезпечує неперевершений рівень видимості, виступаючи головним джерелом достовірної інформації в розслідуваннях кібербезпеки.

Чому саме пакетні дані? Нефільтрована правда та глибока прозорість

Мережеві пакетні дані представляють собою кожен фрагмент інформації, що передається мережею, включаючи джерело, пункт призначення, протокол і корисне навантаження кожного зв'язку. На відміну від журналів, які генеруються певними програмами або системами і можуть не фіксувати всі деталі або навіть бути підроблені зловмисниками, пакетні дані пропонують незмінний запис мережевого трафіку. Це «істина», яка точно показує, що відбувалося в мережі.

Ця глибока видимість є критично важливою, оскільки: Відсутність сліпих зон: Пакетні дані фіксують усі мережеві комунікації, незалежно від того, чи генерують вони запис у журналі, чи їх бачать інші засоби безпеки. Це означає, що можна виявити приховані канали командування та управління (C2), спроби прихованого витоку даних або складні горизонтальні переміщення, що обходять засоби контролю безпеки кінцевих точок; Незаперечні докази: Для криміналістики та реагування на інциденти пакетні дані надають переконливі докази зловмисної діяльності. Вони можуть реконструювати цілі шляхи атаки, показати послідовність подій та точно визначити момент компрометації або витоку даних; Поза межами сигнатур: Хоча системи виявлення на основі сигнатур спираються на відомі шкідливі шаблони, аналіз пакетів може виявити аномальну поведінку, навіть для загроз нульового дня або варіацій відомого шкідливого програмного забезпечення, для яких ще не існує сигнатури. Поведінковий аналіз пакетних даних може виявити незвичне використання протоколу, шаблони зв'язку або розміри передачі даних.

Практичні висновки: від фрагментів до порушень

Здатність захоплювати, зберігати та аналізувати мережеві пакетні дані трансформує можливості SOC ефективно виявляти, розуміти, виявляти та видаляти загрози.

Ідентифікація: Точне виявлення аномалій та вторгнень. Пакетні дані дозволяють аналітикам SOC швидко виявляти аномалії, які можуть сигналізувати про кібератаку. Це включає:

Незвичайні мережеві потоки: виявлення підключень до підозрілих IP-адрес, нетипового використання портів або обсягів трафіку, що суттєво відхиляються від встановлених базових значень.

Зв'язок командування та управління (C2): Виявлення закономірностей, що вказують на канали C2, таких як активність маяків, використання нестандартних протоколів або зв'язок з відомими шкідливими доменами.

Витік даних: розпізнавання передачі великих обсягів даних до зовнішніх, несанкціонованих місць призначення або надсилання незвичайних типів файлів, що може свідчити про крадіжку даних.

Внутрішні загрози: моніторинг внутрішнього мережевого трафіку на предмет несанкціонованого доступу до конфіденційних систем, незвичайного переміщення даних привілейованими користувачами або порушень політик, що свідчать про зловмисну інсайдерську діяльність.

Аналізуючи пакетні дані в режимі реального або майже реального часу, команди SOC можуть отримати негайне уявлення про підозрілу активність, що дозволяє швидко виявляти потенційні інциденти безпеки до їх ескалації.

Полювання на загрози: слідування цифровим хлібним крихтам

Для проактивного пошуку загроз пакетні дані є незамінними. Мисливці за загрозами використовують пакетні дані для:

Реконструкція шляхів атаки: Відстежуючи потік мережевого трафіку, мисливці можуть відстежувати горизонтальне переміщення зловмисника в мережі, розуміти, як він отримав доступ, та ідентифікувати скомпрометовані системи. Це забезпечує повну картину ланцюжка знищення кібератаки.

Виявлення прихованих загроз: Досвідчені зловмисники часто використовують легітимні інструменти та протоколи, щоб зливатися зі звичайним мережевим трафіком, що ускладнює їх виявлення за допомогою традиційних заходів безпеки. Аналіз пакетів може виявити ці тонкі індикатори, такі як незвичне використання протоколів, зашифровані тунелі або приховані канали, що використовуються для зв'язку.

Перевірка гіпотез: Коли мисливець за загрозами підозрює певний тип атаки або наявність індикатора компрометації (IoC) у мережі, він може використовувати пакетні дані для перевірки своєї гіпотези. Наприклад, якщо відомо, що певне шкідливе програмне забезпечення зв'язується через певний порт, пакетні дані можуть підтвердити, чи справді будь-які внутрішні хости здійснюють такі з'єднання.

Розуміння масштабу: Пакетні дані допомагають визначити повний масштаб порушення, ідентифікуючи всі уражені системи та дані, що має вирішальне значення для комплексного стримування.

Видалення та відновлення: цілеспрямована та науково обґрунтована відповідь

Коли інцидент підтверджено, пакетні дані надають незаперечні докази, необхідні для цілеспрямованого стримування та ліквідації:

Точне стримування: Визначивши точне джерело та пункт призначення шкідливого трафіку, команди SOC можуть впроваджувати високоточні заходи стримування, такі як блокування певних з’єднань або ізоляція скомпрометованих хостів, мінімізуючи порушення законних операцій.

Ефективне знищення: Пакетні дані розкривають методи, що використовуються зловмисниками, спрямовуючи зусилля з знищення. Наприклад, якщо витік даних стався через певний протокол, команда точно знає, на чому зосередити свої зусилля для очищення та запобігання.

Криміналістика після інциденту: Для ретельного аналізу після інциденту пакетні дані є безцінними. Вони дозволяють судовим слідчим відтворювати мережеву активність, аналізувати корисні навантаження та розуміти повний вплив порушення, сприяючи покращенню політик та практик безпеки.

Аналіз першопричин: Розуміння того, «як» і «чому» відбувається атака, є надзвичайно важливим. Пакетні дані дозволяють провести глибокий аналіз першопричин, визначити початкову точку проникнення та використані вразливості, що життєво важливо для запобігання повторенню.

За межами реактивності: проактивна безпека з пакетними даними

Стратегічна інтеграція пакетних даних в операції SOC перетворює безпеку з виключно реактивної моделі, що керується сповіщеннями, на проактивний захист, що керується розвідкою. Забезпечуючи нефільтрований, комплексний огляд мережевої активності, це дає командам безпеки можливість виявляти, виявляти та усувати загрози з неперевершеною точністю та швидкістю. Ця можливість є основою для досягнення

справжньої кіберстійкості, дозволяючи організаціям випереджати складних супротивників та захищати свої найважливіші активи. Сучасні рішення для виявлення та реагування на мережі (NDR) спеціально розроблені для використання можливостей пакетних даних, пропонуючи глибоку видимість та поведінкову аналітику для розширення можливостей SOC.

Ключові ролі в команді SOC

Високоефективна SOC спирається на міждисциплінарну команду, кожен член якої вносить свій спеціалізований внесок у зусилля з колективної безпеки. Хоча конкретні посади та рівні можуть відрізнятися, основні функції загалом однакові:

Менеджер/керівник SOC: Ця особа здійснює стратегічний нагляд та керівництво всім SOC. Вона відповідає за визначення бачення SOC, встановлення операційних цілей, управління персоналом, забезпечення дотримання політик безпеки та ескалацію критичних інцидентів вищому керівництву. Менеджер SOC також відіграє ключову роль в ініціативах щодо постійного вдосконалення та сприяння культурі досконалості в команді.

Аналітики безпеки (рівень 1, 2, 3): це захисники на передовій, які формують ядро команди SOC. Їхні ролі зазвичай розподіляються на рівні залежно від досвіду та складності інцидентів, з якими вони працюють:

Аналітики 1-го рівня: часто їх називають «спеціалістами з сортування сповіщень», ці аналітики відповідають за початковий моніторинг сповіщень безпеки, фільтрацію хибнопозитивних результатів та проведення попередніх розслідувань. Вони дотримуються встановлених методичних рекомендацій для ескалації підтверджених інцидентів на вищий рівень. Їхні обов'язки зазвичай включають цілодобовий моніторинг, перевірку початкових сповіщень та збір базових даних.

Аналітики 2-го рівня: це більш досвідчені аналітики, які проводять глибші розслідування інцидентів, що ескалирували з 1-го рівня. Вони виконують детальний аналіз, використовують передові інструменти безпеки (включаючи SIEM та NDR) та працюють над стратегіями стримування. Вони вміють розуміти тактику зловмисників та розробляти дії негайного реагування.

Аналітики 3-го рівня: Найстарші та найкваліфікованіші аналітики безпеки, також відомі як «мисливці за загрозами» або «судові слідчі». Вони обробляють найскладніші та найсучасніші загрози, виконують проактивне полювання на загрози, проводять поглиблений судово-медичний аналіз та розробляють власні правила виявлення. Вони часто мають досвід у зворотному проектуванні, аналізі шкідливих програм та передових методологіях боротьби з постійними загрозами (APT).

Мисливці за загрозами: Хоча вони часто є підгрупою аналітиків 3-го рівня, деякі організації присвячують певні ролі пошуку загроз. Ці фахівці є проактивними, керованими гіпотезами слідчими, які активно шукають невідомі загрози, що обійшли існуючі засоби контролю безпеки. Вони використовують складні методи та величезні набори даних, включаючи мережеві пакетні дані, для виявлення прихованих супротивників.

Реагування на інциденти: Ці фахівці спеціалізуються на фазах стримування, ліквідації та відновлення після інцидентів. Хоча всі аналітики SOC беруть участь у реагуванні на інциденти, спеціалізовані фахівці з реагування на інциденти часто керують повним життєвим циклом серйозного порушення, координуючи зусилля кількох команд та забезпечуючи швидке повернення до нормальної роботи. Вони вміють аналізувати та звітувати про інциденти після інциденту.

Фахівці з управління вразливостями: Ці члени команди зосереджуються на виявленні, оцінці та визначенні пріоритетів вразливостей в інфраструктурі організації. Вони проводять сканування, аналізують результати та співпрацюють з IT-командами, щоб забезпечити усунення вразливостей, тим самим зменшуючи поверхню атаки.

Інженери/архітектори безпеки: Хоча інженери безпеки не завжди входять до безпосередньої операційної команди SOC, вони часто тісно співпрацюють з SOC. Вони відповідають за проектування, впровадження та підтримку інфраструктури та інструментів

безпеки (SIEM, EDR, NDR, брандмауери тощо), на які покладається SOC. Вони надають експертизу в оптимізації рішень безпеки та інтеграції нових технологій.

Спільний характер цих ролей є важливим для ефективної роботи SOC, що забезпечує постійний моніторинг, захист та вдосконалення всіх аспектів кібербезпеки організації.

Типи моделей SOC

Організації можуть впроваджувати Центр операцій безпеки кількома способами, кожен з яких має свої переваги та міркування, залежно від таких факторів, як бюджет, внутрішні можливості та конкретні вимоги безпеки.

Внутрішній SOC: Ця модель передбачає створення та функціонування SOC повністю всередині організації.

Переваги: Забезпечує повний контроль над операціями, процесами та даними безпеки. Дозволяє глибоку інтеграцію з внутрішніми бізнес-процесами та конкретними політиками безпеки. Команда отримує глибокі знання про унікальне середовище та ризики організації.

Недоліки: Вимагає значних початкових інвестицій у технології, інфраструктуру та кваліфікований персонал. Укомплектування цілодобової операції експертами-аналітиками безпеки може бути складним та дорогим через нестачу фахівців з кібербезпеки. Поточні операційні витрати, включаючи навчання та обслуговування інструментів, можуть бути високими.

Аутсорсинг SOC (SOC-as-a-Service / SOCaaS): У цій моделі організація укладає договір зі стороннім постачальником керованих послуг безпеки (MSSP) для виконання функцій SOC. SOC-as-a-Service (SOCaaS) – це популярна пропозиція, коли постачальник керує моніторингом, виявленням загроз, попереднім розслідуванням та реагуванням на інциденти з власних потужностей.

Переваги: Економічно ефективний, оскільки дозволяє уникнути капітальних витрат та проблем із персоналом, пов’язаних із внутрішньою SOC. Забезпечує негайний доступ до спеціалізованих експертів з кібербезпеки, часто з цілодобовим покриттям. Пропонує масштабованість та може надавати інформацію про загрози, що перевищує ту, яку може зібрати одна організація. Швидке розгортання рішень безпеки.

Недоліки: Менший прямий контроль над операціями безпеки та даними. Організації повинні ретельно перевіряти постачальників, щоб забезпечити довіру та дотримання вимог відповідності. Потенційні проблеми щодо суверенітету даних та того, як конфіденційна інформація безпеки обробляється третьою стороною.

Гібридний SOC: Ця модель поєднує елементи як внутрішнього, так і аутсорсингового підходів. Наприклад, організація може підтримувати менший внутрішній SOC для критичних систем та реагування на основні інциденти, одночасно передаючи цілодобовий моніторинг та первинне сортування сповіщень постачальнику послуг з управління операційною службою (MSSP).

Переваги: Поєднує контроль з економічною ефективністю та доступом до спеціалізованих експертів. Дозволяє організації зосередитися на своїх найбільш чутливих активах, використовуючи зовнішні ресурси для ширшого охоплення.

Недоліки: Потрібна ретельна координація та чіткий розподіл обов'язків між внутрішньою командою та зовнішнім постачальником, щоб уникнути прогалин або дублювання.

Кероване виявлення та реагування (MDR): Хоча MDR часто надається постачальниками послуг з управління загрозами (MSSP), це окрема послуга, яка зосереджена саме на розширеному виявленні загроз, розслідуванні загроз, пошуку загроз та швидкому реагуванні на інциденти. На відміну від традиційного SOCaaS, який може більше зосереджуватися на моніторингу безпеки та базовому оповіщенні, MDR йде глибше, пропонуючи проактивне виявлення загроз та управління інцидентами під керівництвом експертів.

Переваги: Забезпечує більш проактивний та практичний підхід до управління загрозами. Пропонує спеціалізованих мисливців за загрозами та реагування на інциденти, які

активно виявляють та усувають загрози. Може доповнити існуючу внутрішню команду безпеки.

Недоліки: Може бути дорожчим за базовий SOCaaS. Вимагає високого рівня довіри з постачальником, враховуючи його глибокий доступ до середовища організації.

Вибір моделі SOC значною мірою залежить від унікального профілю ризиків організації, наявності ресурсів та стратегічних цілей безпеки.

Побудова ефективної SOC: найкращі практики

Створення та функціонування ефективного Центру операцій безпеки вимагає не лише придбання передових інструментів безпеки; воно вимагає стратегічного підходу, що охоплює людей, процеси та технології. Дотримання найкращих практик може значно покращити здатність Центру операцій безпеки захищати організацію від кіберзагроз.

Визначте чіткі цілі та показники: Перш ніж створювати або оптимізувати SOC, вкрай важливо визначити його цілі. Які конкретні ризики він враховуватиме? Як буде вимірюватися його успіх? Цілі повинні відповідати загальним бізнес-цілям та дотриманню нормативних вимог. Ключові показники ефективності (KPI) та показники, такі як середній час виявлення (MTTD), середній час отримання знань (MTTK), середній час реагування (MTTR), кількість хибнопозитивних результатів та серйозність інцидентів, є важливими для постійного вдосконалення та демонстрації цінності.

Інвестуйте в правильний технологічний стек: Потужний SOC спирається на надійний набір рішень безпеки. Зазвичай це включає SIEM для агрегації та кореляції журналів, Endpoint Detection and Response (EDR) або Extended Detection and Response (XDR) для видимості кінцевих точок, Network Detection and Response (NDR) для глибокої видимості мережі (особливо пакетних даних), Security Orchestration, Automation, and Response (SOAR) для ефективності, а також платформи розвідки загроз. Ключем є інтеграція та сумісність між цими інструментами для створення єдиної екосистеми безпеки.

Формуйте кваліфіковану команду: лише технологій недостатньо. Ефективність SOC залежить від досвіду її аналітиків та спеціалістів з безпеки. Інвестуйте в постійне навчання та професійний розвиток, щоб підтримувати навички в актуальному стані з урахуванням кіберзагроз та технологій, що розвиваються. Сприяйте культурі безперервного навчання, обміну знаннями та співпраці в командах SOC. Розгляньте можливість перехресного навчання для розвитку резервних можливостей та стійкості.

Встановлення надійних процесів та інструкцій: Чіткі, добре задокументовані процеси є основою ефективних операцій SOC. Розробіть комплексні інструкції реагування на інциденти для різних типів інцидентів безпеки, що окреслюють покрокові процедури виявлення, аналізу, стримування, ліквідації та відновлення. Впроваджуйте стандартизовані робочі процеси для сортування тривог, управління вразливостями та звітності. Регулярні навчання та симуляції (навчання «Червона команда» проти «Синьої команди») допомагають удосконалити ці процеси та забезпечити готовність команди до реальних сценаріїв.

Інтеграція інформації про загрози: Щоб випереджати розвиток кіберзагроз, SOC повинен постійно отримувати та інтегрувати відповідну інформацію про загрози. Це включає інформацію про нові вразливості, нові вектори атак, групи зловмисників та індикатори компрометації (IoC). Інтеграція цієї інформації в правила SIEM, запити на пошук загроз та процеси управління вразливостями дозволяє SOC проактивно виявляти та пом'якшувати ризики.

Впровадження автоматизації та оркестрації: для боротьби зі втомою від сповіщень та покращення часу реагування використовуйте автоматизацію для повторюваних завдань (наприклад, блокування шкідливих IP-адрес, ізоляція кінцевих точок, збагачення сповіщень). Платформи SOAR можуть оркеструвати складні робочі процеси, забезпечуючи послідовне та швидке виконання дій реагування, звільняючи аналітиків безпеки для зосередження на складніших аналітичних та пошукових заходах.

Постійне вдосконалення: SOC не є статичною структурою; вона повинна постійно адаптуватися та вдосконалюватися. Регулярно переглядайте дані про інциденти, проводите

аналіз після інцидентів для виявлення отриманих уроків та вдосконалюйте процеси та технології на основі цих даних. Збирайте відгуки від команди SOC та інших зацікавлених сторін для оптимізації операцій та покращення загального стану безпеки. Регулярно оцінюйте нові рішення безпеки та коригуйте стратегію для реагування на нові кіберзагрози.

Ретельно впроваджуючи ці найкращі практики, організації можуть створити та вдосконалити високоефективний Центр операцій безпеки, який забезпечує надійні, проактивні можливості кіберзахисту від сучасного складного ландшафту загроз.

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого корпоративного центру управління інформаційною безпекою (SOC). Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого корпоративного центру управління інформаційною безпекою (SOC).

– Досліджена система мережевого корпоративного центру управління інформаційною безпекою (SOC).

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого корпоративного центру управління інформаційною безпекою (SOC). Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого корпоративного центру управління інформаційною безпекою (SOC). Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
2. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.

3. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
4. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
5. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
6. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
7. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
8. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
9. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
10. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
11. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
12. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
13. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
14. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
15. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
16. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
17. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
18. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи ћозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
19. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
20. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
21. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
22. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
23. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling

strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
24. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
25. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
26. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
27. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
28. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
29. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
30. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
31. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
32. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.