НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри

Комп'ютерних систем, мереж та кібербезпеки

_____ Касаткін Д.Ю., к. пед.н., доц.

підпис ПІБ, вчене звання і ступінь

«___»_____ 2025 р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

На тему: «Система управління реагування на комп’ютерні інциденти»

Спеціальність F7 «Комп’ютерна інженерія»

Гарант освітньої програми:_____ / Нікітенко Є.В./

підпис ПІБ

Керівник дипломного проекту:_____ / Мамченко С.М. /

підпис ПІБ

Виконав:_____ / Білан Р.А. /

підпис ПІБ

КИЇВ - 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____/ Касаткін Д.Ю., к.пед.н., доц. /
підпис ПІБ, вчене звання і ступінь
«___» _____ 2025 р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ СТУДЕНТУ

Білана Романа Андрійовича
(прізвище, ім'я, по батькові)
Спеціальність (напрям підготовки): F7 Комп'ютерна інженерія

Тема кваліфікаційної бакалаврської роботи: Система управління реагування на комп'ютерні інциденти

затверджена наказом ректора НУБіП України від "_16_" _12___ 2024р. №2251«С»
Термін подання завершеної роботи на кафедру ___28.05.2025 року
Вихідні дані до кваліфікаційної бакалаврської роботи Система управління реагування на комп'ютерні інциденти

Перелік питань, що підлягають розробці:
1. Аналіз технічного завдання
2. Аналіз різновидів комп'ютерних інцидентів
3. Особливості комп'ютерних інцидентів IoT
4. Управління реагування комп'ютерними інцидентами
5. Система управління реагування комп'ютерними інцидентами

Перелік графічного матеріалу (за потреби) _____

Дата видачі завдання "_16_"___12_____2024 р.

Керівник бакалаврської роботи _____ _Мамченко С.М., д. пед.н., професор
(підпис) (прізвище та ініціали)
Завдання прийняв до виконання _____ __Білан Р.А._____
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз предметної області	04.02.2025 р.	Виконано
2	Проектування системи	15.03.2025 р.	Виконано
3	Реалізація системи	10.04.2025 р.	Виконано
4	Тестування системи	01.05.2025 р.	Виконано
5	Оформлення пояснювальної записки	13.06.2025 р.	Виконано
6	Оформлення графічного матеріалу	13.06.2025 р.	Виконано

Студент _____ **Роман БІЛАН**
(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ **Сергій МАМЧЕНКО**
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Обсяг роботи 66 сторінок, 7 ілюстрації, 1 таблиця, 19 джерел літератури.

Дипломна робота на тему «Система управління реагування на комп'ютерні інциденти» присвячена дослідженню актуальних проблем забезпечення інформаційної безпеки в умовах зростаючої кількості кіберзагроз та розвитку цифрових технологій, зокрема Інтернету речей (IoT)

У роботі розкрито сутність поняття «комп'ютерний інцидент», наведено класифікацію загроз, описано сучасні методи виявлення, аналізу та реагування на інциденти безпеки. Проведено огляд технологій SIEM, SOC, CSIRT та стандартів ISO/IEC 27035, 27001, NIST SP 800-61. Особливий акцент зроблено на захисті IoT-пристроїв, які стають дедалі поширенішими у корпоративних та державних системах, але при цьому мають велику кількість вразливостей.

Результатом дослідження є формування практичних пропозицій щодо побудови ефективної системи реагування на комп'ютерні інциденти, що забезпечує стійкість IT-інфраструктури, зменшення ризиків та підвищення загального рівня кібербезпеки.

Ключові слова: комп'ютерний інцидент, кібербезпека, SIEM, реагування, IoT, політика безпеки, воєнний стан, ризики, CERT-UA, NIST.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

AI – Artificial Intelligence / штучний інтелект

CERT-UA – Комп'ютерна аварійна команда України

CISO – Chief Information Security Officer / керівник з інформаційної безпеки

CSIRT – Computer Security Incident Response Team / команда реагування на інциденти

DDoS – Distributed Denial of Service / розподілена атака на відмову в обслуговуванні

EDR – Endpoint Detection and Response / виявлення та реагування на рівні кінцевих пристроїв

IoT – Internet of Things / Інтернет речей

IRP – Incident Response Plan / план реагування на інциденти

ISMS – Information Security Management System / система управління інформаційною безпекою

IT – Information Technology / інформаційні технології

MFA – Multi-Factor Authentication / багатофакторна автентифікація

NIST – National Institute of Standards and Technology / Національний інститут стандартів і технологій (США)

NGFW – Next Generation Firewall / міжмережевий екран нового покоління

PCI DSS – Payment Card Industry Data Security Standard / стандарт безпеки даних платіжних карток

SIEM – Security Information and Event Management / система управління інформацією та подіями безпеки

SOC – Security Operations Center / центр операційної безпеки

VPN – Virtual Private Network / віртуальна приватна мережа

Wiper – тип шкідливого ПЗ, що знищує інформацію

ВСТУП

Сучасне суспільство рухається до цифрового способу роботи, де дані є одним із ключових стратегічних активів. В умовах глибокої комп’ютеризації бізнес-завдань, державного управління, освіти та інших сфер забезпечення безпеки інформаційних систем від кіберризиків має велике значення. Щодня по всьому світу реєструються тисячі комп’ютерних інцидентів, які можуть призвести до серйозних фінансових втрат, втрати життєво важливої інформації та навіть порушити роботу інформаційної інфраструктури.

Комп'ютерні інциденти - це події, які свідчать про ймовірне порушення або порушення принципів політики інформаційної безпеки. Деякі такі інциденти включають несанкціонований доступ, вірусні атаки, фішингові кампанії, спроби підбору пароля, DDoS-атаки тощо. Своєчасне виявлення, аналіз і ефективне реагування відіграють вирішальну роль у мінімізації шкоди від загроз. Таким чином, актуальність розробки та вдосконалення систем реагування на комп’ютерні інциденти не викликає сумнівів. У реальних умовах, особливо в середовищі середніх і великих підприємств, окрім технічних дій, процес реагування на інцидент передбачає набагато більше.

Ефективне реагування допомагає мінімізувати час простою системи, запобігти витоку даних, захистити репутацію організації та підтримувати безперервність її діяльності.

У цій роботі вивчаються принципи та підходи до побудови систем реагування на комп’ютерні інциденти, переглядаються поточні рішення та створюється модель або концепція, які можна використовувати для покращення реагування в умовах обмежених ресурсів.

У роботі розглядаються як теоретичні аспекти, так і практичні приклади побудови таких систем. Актуальність теми зумовлена також стрімким зростанням в Україні та світі атак як на державні структури, так і на приватні компанії.

1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ РЕАГУВАННЯМ НА КОМП'ЮТЕРНІ ІНЦИДЕНТИ

1.1 Розслідування інцидентів інформаційної безпеки

В останні роки типові захисні заходи інформаційної безпеки не можуть гарантувати повноцінного захисту інформації компанії, її інформаційних систем, сервісів, мереж та мережевого периметра. Безперечно, після впровадження методів захисту, швидше за все, залишаться вразливі місця в інформаційній інфраструктурі організації, які можуть створити передумови для шахрайських дій, що призведе до можливих інцидентів інформаційної безпеки. Більше того, з часом можуть з'являтися нові вразливості, які раніше були не ідентифіковані. Зауважимо, що інциденти ІБ можуть негативно вплинути на функціонування та діяльність компанії. Внаслідок недостатнього рівня підготовки структури до реагування на інциденти ІБ атакована організація може зазнати істотного як фінансового, так і матеріального збитку. Таким чином, організаціям, які відповідально ставляться до інформаційної безпеки, важливо застосовувати комплексний та регулярний підхід до наступного:

− виявлення та розслідування інцидентів інформаційної безпеки, надання їх експертної оцінки;

− реагування на інциденти ІБ, у тому числі активізацію необхідних додаткових захисних дій для недопущення або зменшення наслідків, а також відновлення після хакерських атак;

− набуття досвіду з інцидентів ІБ, запровадження запобіжних захисних засобів та удосконалення єдиного підходу до менеджменту комп'ютерних інцидентів. Якою б досконалою не була система забезпечення інформаційної безпеки в організації, завжди залишається ризик.

Як показує практика, організація може жодним чином не виявляти перші стадії атак, а виявляти вже лише її наслідки – втрату грошей чи недоступність того чи іншого сервісу. Тому будь-яка подія інформаційної безпеки, яка була кваліфікована як інцидент – має розслідуватися. Без етапу розслідування не буде зроблено висновків і, як наслідок, можливо інцидент повторюватиметься надалі[7].

Реагування на інциденти інформаційної безпеки (ІБ) – це структурована сукупність дій, спрямована на встановлення деталей інциденту, мінімізацію збитків від інциденту та запобігання повторенню інциденту ІБ. На практиці існує кілька фаз реагування на інцидент у сфері ІБ, а саме:

− Аналіз мережної активності. Фахівці групи реагування на інциденти інформаційної безпеки здійснюють оцінку мережевого трафіку та діагностують підозрілі інформаційні системи.

− Криміналістичний аналіз. Експерти проводять криміналістичне експрес-обстеження всіх серверів, що працюють у компанії, задіяних шахраями, з метою встановлення причин атак, переміщення атакуючих по комп'ютерних системах і мережах.

− Діагностика шкідливого коду Аналітик здійснює фундаментальний статичний та динамічний аналіз знайдених під час реагування моделей шкідливого коду.

Вищезгадане дає можливість експертам виключити його закріплення у комп'ютерних системах та уникнути повторної компрометації ІТ інфраструктури компанії. Розслідування інцидентів кібербезпеки починається з фіксації, збору та аналізу свідчень. Потім відбувається пошук відповідальних та винних осіб, а також встановлення безпосередніх причин, через які інцидент ІБ стався. Далі відбувається аналіз ІТ-інциденту, в якому також виявляють недоліки документів та методик, на основі чого створюються рекомендації щодо реагування на інциденти та налаштування захисту таким чином, щоб реагування та розслідування було можливим.

Готується звіт експертизи з прикріпленими даними, який можна використовувати для розслідування інциденту інформаційної безпеки на підприємстві як самотужки, так і через інші служби. Процес регулювання інцидентів інформаційної безпеки повинен мати певні послідовні стадії: від визначення його потреби до поширення та моніторингу. Усі процедури щодо запобігання наслідкам та першопричинам інцидентів повинні неминуче документуватися.

Безперечно, документування сценаріїв реагування на кожен потенційний інцидент ІБ має проводитись експертами та фіксуватися у відповідних регламентах та правилах. Документ, оформлений у вигляді регламенту, повинен мати такі структурні підрозділи: − чітке формулювання подій, визначених інцидентами стосовно механізму ІБ підприємства. Наприклад, експлуатація зовнішньої електронної пошти можливо буде порушенням ІБ для державного підприємства та рядовою дією для приватної компанії;

− порядок повідомлення про подію. Повинні бути позначені:

− формат оповіщення (усний, письмовий або за допомогою повідомлення);

− співробітники, яких потрібно повідомити;

− годинні рамки повідомлення після закінчення надходження інформації про інцидент;

− конкретні процедури щодо ліквідації результату інциденту, а також порядок їх впровадження;

− етапи розслідування. На етапах важливо встановити відповідальних за нього співробітників, процес збору та процедуру фіксації доказів, прийнятні способи виявлення винуватця;

− процедуру притягнення до дисциплінарної відповідальності винних працівників компанії;

− дії щодо покращення безпеки, які важливо впроваджувати за результатами розслідування інциденту;

− порядок мінімізації збитків та усунення результатів інцидентів. При підготовці регламентів важливо спиратися на розроблені методики і документацію, що довели свою корисність, наприклад, звіти, журнали. Регламенти, які визначають механізм управління інцидентами ІБ, мають бути складовим елементом бізнес-процесів.

Вони повинні позначити методи та способи класифікацій подій, та процес виявлення цих подій з подальшим внесенням до регламентуючої документації.

1.2 Аналіз вимог стандартів ISO/IEC та української нормативної бази в частині управління інцидентами інформаційної безпеки

У світі розробка стандартів, технічних звітів, керівництв та рекомендацій в галузі інформаційної безпеки (ІБ) проводиться безперервно; послідовно публікуються проекти і версії стандартів, присвячених тим чи іншим аспектам ІБ на різних стадіях узгодження і затвердження.

Розробка нормативних документів з ІБ, повністю або частково присвячених керуванню інцидентами ІБ, здійснюється спеціалізованими міжнародними організаціями і консорціумами, наприклад такими як: CERT, ISO, IEC, IETF, ITUT, IEEE, OMG, SANS Institute, X/Open тощо. Значна робота щодо стандартизації питань ІБ, зокрема керування інцидентами, проводиться спеціалізованими організаціями і на національному рівні, в першу чергу в США – NIST, CMU/SEI; Німеччині та Великобританії – BSI.

Все це дозволило сформувати широку нормативно-методологічну базу у вигляді міжнародних, національних та галузевих стандартів, а також

нормативних і керівних матеріалів, що регламентують діяльність в сфері керування інцидентами ІБ.

Проте, як свідчить сучасна практика, найважливішу роль в світі відіграють стандарти ISO. Стандарти ISO серій 9000, 27002, 20000, 27000 описують правила створення систем керування різними процесами та гармонійно поєднуються один з одним. Усі вони, за основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як процес, а саме як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього. Крім цього, стандарти зазначених серій використовують єдину модель PDCA як структуру життєвого циклу всіх процесів системи менеджменту. Основні нормативно-методологічні документи ISO/IEC, що за певними аспектами регламентують процеси керування інцидентами ІБ, наведені в таблиці 1.1.

Як свідчить світова практика стандарт ISO/IEC 27002 на сьогодні став найпоширенішим інструментом створення системи керування інформаційною безпекою (СКІБ), стандартом де-факто щодо керування ІБ. Стандарт розроблений в 2005 році на основі версії ISO 17799, опублікованій у 2000.

ISO/IEC 27002– це збірка практичних рекомендацій, яка дає деталізоване керівництво щодо розробки, впровадження та оцінки заходів керування ІБ, а також загальні принципи побудови системи керування ІБ.

1.3 Розгляд проблематики IOT

За останні роки пристрої IoT стали повсюдно поширеними та необхідними інструменти, якими люди користуються щодня. Кількість пристроїв, підключених до Інтернету, продовжує зростати з кожним роком. Підраховано, що до 2025 р буде щонайменше 41,6 мільярда пристроїв IoT, підключених до Інтернету. Business Insider прогнозує збільшення на 512 % у порівнянні до 2018 року (8 мільярдів пристроїв IoT). Експоненційне зростання

викликає серйозні проблеми з безпекою.

Наприклад, багато пристроїв IoT мають прості вразливості, як-от ім’я користувача та пароль за замовчуванням, а також відкриті порти telnet/ssh. Часто ці пристрої розміщують у слабких або незахищені мережі, наприклад домашній або загальнодоступній. Насправді IoT пристрої піддаються атакам так само, як і традиційні обчислення системи. Нові пристрої Інтернету речей можуть відкрити новий доступ точки для зловмисників і розкрити всю мережу. Близько 20 % підприємств у всьому світі стикалися з принаймні з однією атакою, пов’язаною з IoT.

У минулому кібератаки переважно мали форму порушення даних або компрометації пристроїв. Загалом, порушення зачіпають важливі системи в промисловості, комп'ютерні пристрої, банки, автоматизовані транспортні засоби, смартфони тощо. Більше того, є чимало прикладів, коли вони завдали серйозних і значних збитків.

Оскільки пристрої IoT зараз є невід’ємною частиною життя більшості людей, кібератаки стали більш небезпечними через їх широке використання. У порівнянні з минулим, зараз набагато більше люди знаходяться в зоні ризику, і вони повинні знати про це. Як пристрої IoT стають все більш поширеними, кібератаки, ймовірно, істотно змінюються як з точки зору причин, так і методів. Кіберзлочинці, наприклад, можуть викликати безпрецедентний рівень вторгнення порушуючи конфіденційність, якщо вони зламали наприклад камеру спостереження. Ці атаки можуть навіть поставити під загрозу життя людей

Оскільки пристрої IoT зараз є невід’ємною частиною життя більшості людей, кібератаки стали більш небезпечними через їх широке використання. У порівнянні з минулим, зараз набагато більше люди знаходяться в зоні ризику, і вони повинні знати про це.

Як пристрої IoT стають все більш поширеними, кібератаки, ймовірно, істотно змінюються як з точки зору причин, так і методів.

Кіберзлочинці, наприклад, можуть викликати безпрецедентний рівень вторгнення порушуючи конфіденційність, якщо вони зламали наприклад камеру спостереження. Ці атаки можуть навіть поставити під загрозу життя людей. [12]

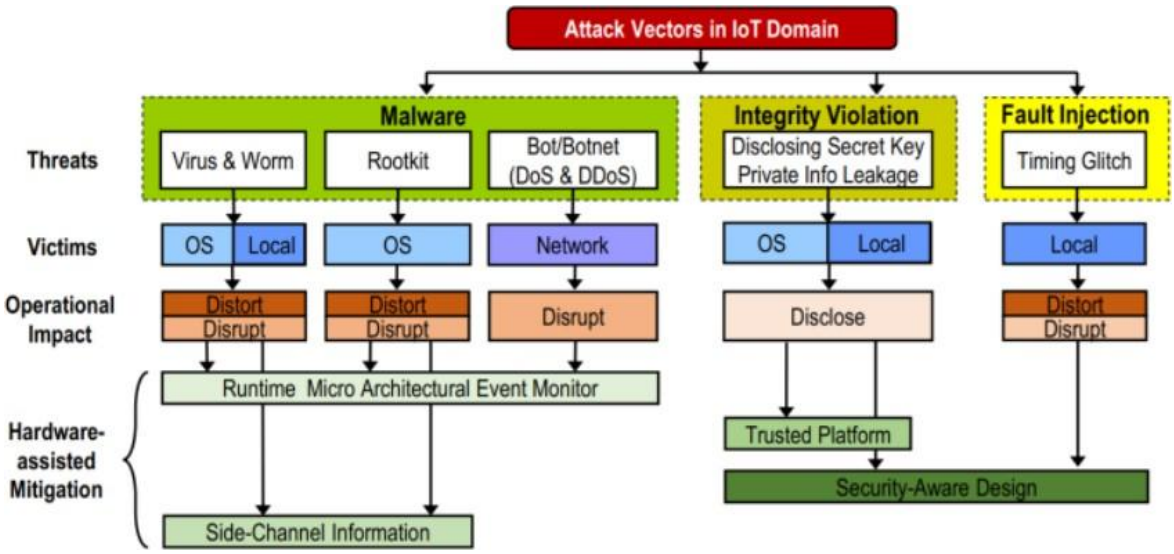
Ще одним фактором, що погіршує ситуацію, є закономірність в Інтернеті речей галузі, де швидкість виходу на ринок переважає питання безпеки. Наприклад, багато пристроїв IoT мають прості вразливості, як-от за замовчуванням ім'я користувача та пароль, а також відкриті порти telnet/ssh. Слабка або незахищена мережа, такі як будинок або громадські місця, є частими місцями, де встановлюються ці пристрої. Підданість нападам проти пристроїв IoT, на жаль, стало реальністю, якщо не гірше ніж традиційні обчислювальні системи. У 2021 році Касперський повідомив, що атак IoT більше за перші шість місяців 2021 року подвоїлася порівняно з попереднім півріччя. Крім того, зловмисники також покращилися їхні навички, щоб зробити ці атаки ще більш витонченими нові атаки, такі як VPNFilter, Wicked, UPnProxy, Hajime, Masuta і Mirai ботнет. Зловнисники постійно вдосконалюють свої навички, щоб зробити ці атаки більш збитковими. На даний момент в новинах більшість масштабних атак на пристрої IoT були DDoS-атаки (наприклад, атака за допомогою ботнета Mirai).

Пристрої Інтернету речей уразливі до викрадення та використання в розподілених атаках відмови в обслуговуванні (DDoS) , а також цілеспрямованому введенні коду, атаках «людина посередині ». Зловмисне програмне забезпечення легше приховувати у великому обсязі даних Інтернету речей, а пристрої Інтернету речей іноді навіть мають уже вбудовані шкідливі програми.

Крім того, деякими пристроями IoT можна керувати дистанційно або вимкнути їхню функціональність зловмисниками. Основною метою кібератак є спотворення вихідних даних (і наступних дій через неправильні дані)

пристрою, або порушення поточних процесів (відмова в обслуговуванні), або розкриття будь-якої секретної інформації, що зберігається на пристрої, таке як секретні ключі та паролі.

Сучасні пристрої збирають масиви даних своїх користувачів. Деяким із них для роботи потрібен не тільки пароль, а й ім'я користувача, його контактна інформація, відомості про біографію. Така кількість інформації вимагає надійного та якісного захисту, проте на даний момент IoT не може похвалитися захищеністю. На Рисунку 1.1 показано, як пристрій IoT може



зазнати атак наступних типів

Рисунок 1.1 – Існуючі атаки на пристрої IoT

Шкідливе ПЗ

Сучасні пристрої Інтернету речей можуть бути заражені різними шкідливими програмами на різних етапах своєї роботи. Найчастіше шкідливе ПЗ (віруси, трояни і черв'яки) зазвичай націлене на локальну експлуатацію та експлуатацію лише на рівні операційної системи залежно від складності атаки та її виконання. Основне завдання шкідливого ПЗ полягає в тому, щоб порушити поточні операції та перехопити контроль над пристроєм

Найпоширеніше використовуються є руткіти (набори утиліт, які хакер встановлює на зламаному їм пристрої після отримання початкового доступу, що дозволяє хакеру закріпитися у зламаній системі та приховати сліди своєїдіяльності). Вони надають хакерам постійний привілейований доступ до системи, активно приховуючи свою присутність. Тим самим зловмисник опановує всю обчислювальну потужність і дані пристрою, а також може розміщувати невидимі користувачам драйвери і служби. Крім того, пристрої Інтернету речей можуть стати жертвою атак типу «відмова в обслуговуванні» (DoS) або розподіленої відмови в обслуговуванні (DDoS), які з кожним днем стають серйозною проблемою. Такий вразливий пристрій може працювати як бот для зараження інших допустимих пристроїв у мережі або споживати пропускну здатність мережі та обчислювальну потужність пристроїв, надаючи зловмиснику додаткові ресурси. Цифри дозволяють краще оцінити масштаби кібернетичних атак на розумні пристрої. Співробітники «Лабораторії Касперського» з початку 2019 року реєструють атаки хакерів на розумні девайси за допомогою ханіпотів(honeypot) — спецприманок для хакерів. Їм вдалося зафіксувати понад 105 мільйонів атак на IoT-пристрої, які проводилися з 276 тисяч унікальних IP-адрес[8].

Ботнет IoT

Зловмисник може заразити пристрій IoT зловмисним програмним забезпеченням через незахищений порт або фішингові шахрайства та зв’язати його в ботнет IoT, який використовується для ініціювання масових кібератак.

Хакери можуть легко знайти шкідливий код в Інтернеті, який виявляє вразливі машини або приховує код від виявлення, перш ніж інший модуль коду подає сигнал пристроїв про атаку або крадіжку інформації.

Ботнети IoT часто використовуються для розподілених атак відмови в обслуговуванні (DDoS), щоб перевантажити мережевий трафік цілі.

Масштабним прикладом була здійснена атака на пристрої IoT за допомогою ботнета Mirai. Mirai сканує Інтернет на пристроях IoT, які працюють на процесорі ARC. Цей процесор працює на урізаній версії операційної системи Linux. Mirai може ввійти в пристрій і заповнити його.

18 березня 2019 року дослідники безпеки в Palo Alto Networks опублікували,був змінений і оновлений для досягнення цієї ж цілі в більшому масштабі. Дослідники виявили, що Mirai використовує 11 нових видів експорту, загальне число сягає 27, і новий список облікових даних адміністратора за умовчанням. Деякі зміни націлених на бізнес-обладнання, включаючи телевізори LG Supersign та безпровідні презентаційні системи Wipg-1000. Mirai може бути ще більш потужним, якщо він може взяти на себе бізнес-обладнання та керувати бізнес-мережами. Нові функції надають ботнету велику поверхню атаки. Зокрема, наведення промислових пристроїв також надає йому доступ до більшої пропускної здатності, що в кінцевому підсумку приводить до більшої потужності ботнету для DDoS-атаки.

Цей варіант Mirai продовжує атакувати клієнтські маршрутизатори, камери та інші пристрої, підключені до мережі. Mirai уразив майже 500 000 пристроїв. Mirai пошкодив сервіси, такі як Xbox Live і Spotify і веб-сайти, такі як BBC і Github, орієнтуючись безпосередньо на DNS-провайдерів. З таким кількістю заражених машин Dyn (поставщик DNS) був зупинений DDOS-атакою з обсягом трафіку в 1,1 терабайт.

DNS-загрози

Багато організацій використовують Інтернет речей для збору даних зі старих машин, які не завжди були розроблені відповідно до новітніх стандартів безпеки. Коли організації поєднують застарілі пристрої з Інтернетом речей, це може піддати мережу вразливості старих пристроїв. Підключення пристроїв IoT часто покладаються на DNS, децентралізовану систему імен 1980-х років, яка може не впоратися з масштабами розгортання Інтернету речей.

Хакери можуть використовувати вразливості DNS для DDoS-атак і тунелювання DNS, щоб отримати дані або запровадити зловмисне програмне забезпечення. Вразливості DNS не стануть загрозою безпеці IoT за допомогою розширень безпеки системи доменних імен (DNSSEC. Ці специфікації захищають DNS за допомогою цифрових підписів, які забезпечують точність і незмінність даних. Коли пристрій IoT підключається до мережі для оновлення програмногозабезпечення, DNSSEC перевіряє, що оновлення йде туди, куди має бути, без зловмисного переспрямування.

IoT вимагач

В даному випадку хакери заражають пристрої шкідливим програмним забезпеченням, щоб перетворити їх на бот-мережі, які досліджують точки доступу або шукають дійсні облікові дані у мікропрограмі пристрою, які вони можуть використовувати для входу в мережу. Маючи доступ до мережі через пристрій IoT, зловмисники можуть вилучити дані в хмару і погрожувати зберегти, видалити або зробити дані загальнодоступними, якщо не заплатить викуп. Іноді платежі недостатньо для організації, щоб повернути всі свої дані, і програма-вимагач автоматично видаляє файли незалежно від того. Програми-вимагачі можуть вплинути на підприємства або важливі організації, наприклад, державні служби або постачальників продуктів харчування.

Тіньовий Інтернет речей

Адміністратори не завжди можуть контролювати, які пристрої підключаються до їхньої мережі, що створює загрозу безпеці IoT, яка називається тіньовим Інтернетом речей . Пристрої з IP-адресою, такі як фітнес-трекери, цифрові помічники або бездротові принтери, можуть створити зручність для персоналу або допомогти співробітникам у роботі, але вони не обов’язково відповідають стандартам безпеки організації.

Без видимості пристроїв IoT в тіні адміністратори не можуть забезпечити, щоб апаратне та програмне забезпечення мало б базові функції безпеки або відстежувало пристрої на наявність шкідливого трафіку. Коли хакери отримують доступ до цих пристроїв, вони можуть використовувати підвищення привілеїв для доступу до конфіденційної інформації в корпоративній мережі або кооптувати з'єднувати для бот-мережі або DDoS-атаки.

Атаки на основі штучного інтелекту

Атаки на основі штучного інтелекту відбуваються з 2007 року, в основному для атак соціальної інженерії (імітують людський чат) і для посилення DDoS-атак. Зловмисне використання штучного інтелекту з'явилося у 2018 році, коли було опубліковано новаторське дослідження про загрозу. З часом більш досконалі алгоритми стають краще імітувати звичайних користувачів у мережі, щоб перешкодити системам виявлення, які шукають дивну поведінку. Найбільшим останнім досягненням у використанні штучного інтелекту в кібератаках є демократизація інструментів для створення та використання систем штучного інтелекту.

Дистанційний запис

Була інформація від WikiLeaks, що спецслужби безпеки знають про існування експлойтів нового дня в прибудовах IoT, смартфонах і ноутбуках. Ці експлойти нульового дня також можуть використовуватися кіберзлочинцями для запису розмов користувачів Інтернету речей.

Наприклад, хакер може атакувати розумну камеру в організації та записувати відеозаписи повсякденної ділової діяльності. Завдяки такому підходу кіберзлочинці можуть таємно отримати конфіденційну ділову інформацію. Такі загрози безпеці IoT також призводять до серйозних порушень конфіденційності.

Розширені постійні загрози

Розширена постійна загроза — це цілеспрямована кібератака, коли зловмисник отримує незаконний доступ до мережі та залишається непоміченим протягом періоду часу. Зловмисники намагаються зберегти мережеву активність та викрадати результати за допомогою розширених постійних загроз. Такі кібератаки важко запобігти, виявити або пом’якшити.

Завдяки IoT великі обсяги критичних даних легко передаються між кількома пристроями. Кіберзлочинець може націлитися на ці пристрої Інтернету речей, щоб отримати доступ до особистих або корпоративних мереж. Завдяки такому підходу кіберзлочинці можуть викрасти конфіденційну інформацію[10].

Розкриття закритого ключа

Отримання доступу до закритого ключа (використовується для шифрування) та/або особистої інформації, що зберігається на пристрої IoT, є ласим шматочком для зловмисника, оскільки це дозволяє скомпрометувати корінь довіри систем. Це дозволяє зловмиснику отримати контроль за процесами зв'язку, захопити обчислювальні потужності пристрою, і найважливіше - конфіденційну інформацію.

Програмно-кероване введення несправностей

Інший клас атак на IoT пристрої – це програмна вставка збоїв в апаратне забезпечення під час роботи пристрою.

Незважаючи на те, що цей тип атак відносно складний, тому що вимагає глибоких знань апаратного забезпечення, що залежить від платформи, а також базового програмного забезпечення, засіб такої атаки дуже складно реалізувати. Оскільки цей клас атак шукає та використовує незначні вразливості в устаткуванні, марно використовувати чисто програмні захисні механізми.

Зрозуміло, існують ефективні програмні рішення для пом'якшення існуючих проблем безпеки IoT пристроїв. Однак складні атаки та кіберзагрози не завжди можна запобігти за допомогою таких програмних методів, тому що програмний механізм захисту, використовуваний у пристрої IoT, може бути вразливий для віддалених атак. Крім того, він не обов'язково має широкий захист, часто його можна оминути та зламати без відома користувача.

Зони атаки на пристрої IoT

Пристрої можуть бути основним засобом, за допомогою якого ініціюються атаки. Частинами пристрою, з яких можуть виникнути вразливості, є його пам’ять, мікропрограмне забезпечення, фізичний інтерфейс, веб-інтерфейс та мережеві служби. Зловмисники також можуть скористатися перевагами незахищених налаштувань за замовчуванням, застарілих компонентів і незахищених механізмів оновлення, серед іншого.

Атаки можуть виникати з каналів зв’язку, які з’єднують компоненти IoT один з одним. Протоколи , які використовуються в системах IoT, можуть мати проблеми з безпекою, які можуть вплинути на всі системи. Системи Інтернету речей також схильні до відомих мережевих атак, таких як відмова в обслуговуванні (DoS) і спуфінг.

Програми та програмне забезпечення.

Уразливості веб-додатків і пов’язаного програмного забезпечення для пристроїв Інтернету речей можуть призвести до скомпрометованих систем.

Наприклад, веб-програми можуть використовуватися для крадіжки облікових даних користувача або оновлень шкідливого програмного забезпечення.

Таблиця 1.1 – Нормативно-методологічні документи ISO/IEC, що стосуються керування інцидентами ІБ

№ п/п	Позначення документа	Назва документа
1	ISO/IEC 27002	Information technology. Security techniques. Code of practice for information security management Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки
2	ISO/IEC 27001	Information technology. Security techniques. Information security management systems. Requirements Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги
3	ISO/IEC 27035	Information technology. Security techniques. Information security incident management Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки
4	ISO/IEC 20000	Information technology. Service management. Part 2: Code of practice Інформаційні технології. Менеджмент послуг. Частина 2. Настанова щодо застосування систем управління послугами

Стандарт ISO/IEC 27001 створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління ІБ (СУІБ), що стосуються в тому числі і процесів керування інцидентами ІБ. [3]

Остання версія офіційно прийнята в Україні як ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.

Вимоги (ISO/IEC 27001:2022, IDT) 17.08.2023р. Згідно з ISO/IEC 27001 для обробки подій і інцидентів ІБ необхідно організувати процес реагування на інциденти. Основними завданнями процесу реагування на інциденти ІБ є:

– координація реагування на інцидент ІБ;

– підтвердження / спростування факту виникнення інциденту ІБ;

– забезпечення збереження і цілісності доказів виникнення інциденту ІБ, створення умов для накопичення і зберігання точної інформації про інциденти ІБ, що мали місце, про корисні рекомендації;

– мінімізація порушень порядку роботи і пошкодження даних ІТ-системи, відновлення в найкоротші терміни працездатності компанії при її порушенні в результаті інциденту;

– мінімізація наслідків порушення конфіденційності, цілісності і доступності інформації ІТ-систем;

– захист прав компанії, встановлених законом; – створення умов для порушення цивільної або кримінальної справи проти зловмисників; – захист репутації компанії і її ресурсів;

– швидке виявлення і/або попередження подібних інцидентів в майбутньому; – навчання персоналу компанії діям щодо виявлення, усунення наслідків і запобігання інцидентам ІБ. В рамках ISO/IEC 27001 висуваються наступні вимоги до процесу реагування на інциденти ІБ, які повністю відповідають вищерозглянутим рекомендаціям щодо керування інцидентами ІБ у ISO/IEC 27002: Моніторинг, вимірювання, аналіз та оцінювання СКІБ [2, п. 9.1].

Організація повинна оцінювати результативність інформаційної безпеки, ефективність системи управління інформаційною безпекою та визначати:

a) що саме потрібно моніторити й вимірювати, включаючи процеси інформаційної безпеки та заходи безпеки;

b) методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів;

c) коли моніторинг та вимірювання потрібно виконувати;

d) хто повинен виконувати моніторинг та вимірювання;

e) коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати;

f) хто повинен аналізувати й оцінювати ці результати. Організація повинна зберігати відповідну задокументовану інформацію як доказ результатів моніторингу та вимірювань.

Задачам керування інцидентами ІБ присвячено стандарт ISO/IEC 27035. Даний документ описує інфраструктуру керування інцидентами в рамках циклічної моделі PDCA. Стандарт представлено в трьох частинах.

ISO/IEC 27035 визначає формальну модель процесу реагування на інциденти. Цілями проходження цієї моделі є упевненість в тому, що:

– події і інциденти ІБ виявляються і обробляються ефективним чином, особливо в частині класифікації;

– виявлені інциденти ІБ враховуються і обробляються найбільш відповідним і ефективним чином;

– наслідки інцидентів ІБ можуть бути мінімізовані в процесі реагування на інциденти ІБ, можливо із залученням процесів відновлення після збоїв і аварій (DRP/BCP); 13

за рахунок аналізу інцидентів і подій ІБ підвищується вірогідність запобігання майбутнім інцидентам, поліпшуються механізми і процеси забезпечення ІБ.

Процес реагування на інциденти ІБ складається з наступних етапів: Планування і підготовка. На даному етапі здійснюється розробка схеми реагування на інциденти ІБ, розробка і затвердження ряду організаційно регламентуючих документів, виділення людських і матеріальних ресурсів, проведення необхідного навчання та апробація вибраної схеми реагування на інциденти ІБ. Даний етап є підготовчим і призначений для організації і регламентації діяльності з реагування на інциденти ІБ. На цьому етапі необхідно:

– виділити людські і матеріальні ресурси;

– розробити схему реагування на інциденти ІБ;

– розробити і затвердити ряд організаційно-регламентуючих документів;

– провести необхідне навчання персоналу і апробацію вибраної схеми реагування на інциденти ІБ.

Процедура керування IT-інцидентами регулюється стандартом ISO/IEC 20000

З позицій ISO/IEC 20000 процес керування ІБ має два важливих значення: – виконання вимог безпеки, закріплених в SLA (Service Level Agreement) та інших вимогах зовнішніх і внутрішніх угод, законодавчих актів і встановлених правил;

– забезпечення базового рівня ІБ, незалежного від зовнішніх вимог. Вхідними даними для процесу служать SLA, що містять вимоги безпеки, за можливості, доповнені документами, що визначають політику організації в цій області, а також інші зовнішні вимоги. Процес також одержує важливу інформацію, що відноситься до проблем безпеки, з інших процесів, наприклад про інциденти, пов'язані з ІБ[4].

Вихідні дані включають інформацію про досягнуту реалізацію SLA разом із звітами про нештатні ситуації з погляду безпеки, а також інформацію про регулярні заходи щодо поліпшення СКІБ.

2 АНАЛІЗ ІСНУЮЧИХ СИСТЕМ РЕАГУВАННЯ НА КОМП'ЮТЕРНІ ІЕЦИДЕНТИ

2.1 SIEM-системи

SIEM (Security information and event management) у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management). Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними. На рисунку 2.1 показано приклад роботи системи.

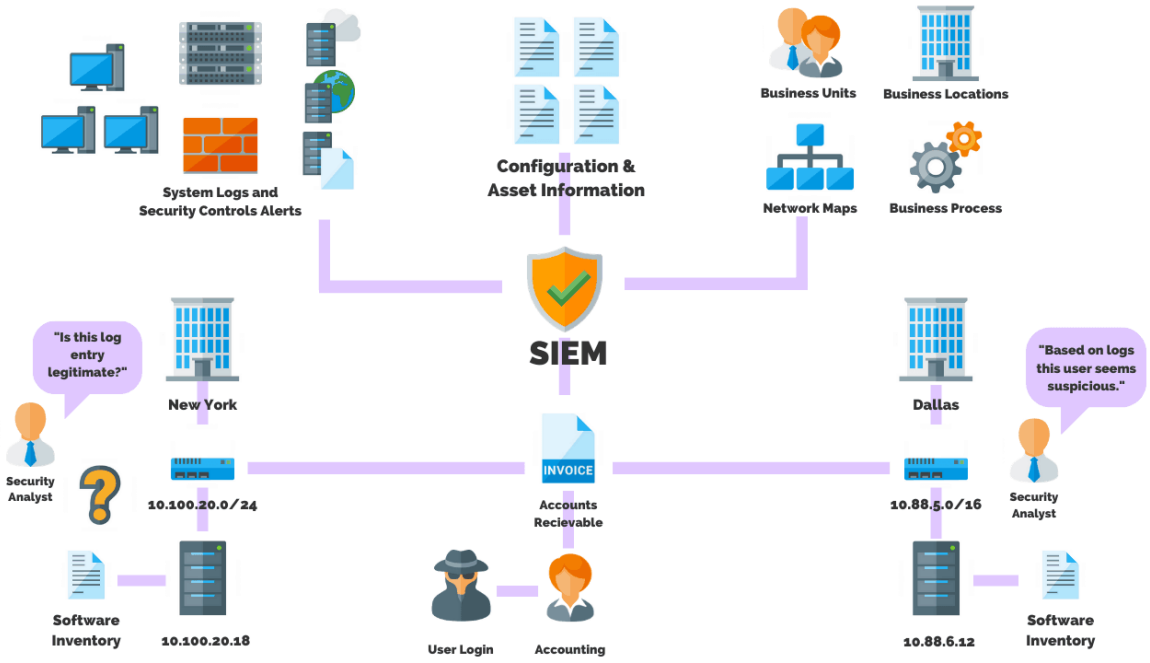


Рисунок 2.1 Робота SIEM-системи

Постачальники продають SIEM як програмне забезпечення, як прилади або як керовані послуги; ці продукти також використовуються для реєстрації даних безпеки та створення звітів для цілей відповідності.

Акроніми SEM, SIM і SIEM іноді використовуються в контексті взаємозамінності. Сегмент систем управління безпекою, що має справу з моніторингом в реальному часі, кореляцією подій, оголошеннями і відображенням на кінцевих пристроях зазвичай називають управлінням подіями (SEM). Друга область забезпечує довготривале зберігання, аналіз і звітність за накопиченими даними відома як управління ІБ (security information management — SIM). У міру зростання потреб у додаткових можливостях безперервно розширюється і доповнюється функціональність даної категорії продуктів. Організації орієнтуються на системи великих даних, таких як Apache Hadoop, для збільшення можливостей SIEM через збільшення сховищ даних та більш гнучної аналітики. [2]

Наприклад, потреба голосової орієнтації або vSIEM (англ. (voice security information and event management)) є свіжим прикладом розвитку у цьому напрямку.

Поняття управління подіями інформаційної безпеки (SIEM), введене Марком Николеттом і Амритом Вільямсом з компанії Gartner в 2005 р., описує:

1) можливості продукту по збору, аналізу та поданню інформації від мережевих пристроїв і пристроїв безпеки,

2) додатків ідентифікації (управління обліковими даними) і управління доступом,

3) інструментів підтримки політики безпеки і відстеження вразливостей, операційних систем, баз даних та журналів додатків,

4) відомостей про зовнішні загрози.

5) Основна увага приділяється управлінню привілеями користувачів і служб, служб каталогів і іншим змінам конфігурації, а також забезпечення аудиту та огляду журналів, реакцій на інциденти.

Функціональність:

1) Агрегація даних: управління журналами даних; дані збираються з різних джерел: мережеві пристрої та сервіси, датчики систем безпеки, сервери, бази даних, програми; забезпечується консолідація даних з метою пошуку критичних подій.

2) Кореляція: пошук спільних атрибутів, зв'язування подій у вагомі кластери. Технологія забезпечує застосування різних технічних заходів для інтеграції даних з різних джерел для перетворення вихідних даних в значущу інформацію. Кореляція є типовою функцією підмножини Security Event Management.

3) Сповіщення: автоматизований аналіз корелюючих подій і генерація повідомлень (сигналів) про поточні проблеми. Оповіщення може виводитися на "приладову панель самого додатка, так і бути направлено в інші сторонні канали: e-mail, GSM-шлюз і т. ін.

4) Засоби відображення (інформаційні панелі): відображення діаграм, які допомагають ідентифікувати патерни відмінні від стандартної поведінки.

5) Сумісність (трансформування): застосування додатків для автоматизації збору даних, формування звітності для адаптації агрегованих даних до чинних процесів управління інформаційною безпекою та аудиту.

6) Зберігання даних: застосування довготривалого зберігання даних в історичному порядку для кореляції даних за часом та для забезпечення трансформування. Довготривале зберігання даних критично для проведення комп'ютерно-технічних експертиз, оскільки розслідування мережевого інциденту, зазвичай, відбувається з часовою затримкою від моменту порушення

7) Експертний аналіз: можливість пошуку по безлічі журналів на різних вузлах; може виконуватися в рамках програмно-технічної експертизи.

Приклади використання :

- SIEM може виявити вразливість нульового дня та поліморфні віруси. Передусім це пов'язано з низькими показниками антивірусного виявлення проти цього типу швидкозмінних шкідливих програм.

- Автоматичний парсинг, нормалізація та класифікація журналів може відбуватися автоматично. Незалежно від типу комп'ютера або мережевого пристрою, аби пристрій міг журналювати події.

- Візуалізація з SIEM, разом з використанням подій безпеки та журналом збоїв, може допомогти у виявленні шаблонів.

- Протокол відхилень може вказати на неправильну конфігурацію або проблему безпеки. Що може бути виявлено з допомогою SIEM, якщо використовувати розпізнавання шаблонів, оповіщення та інформаційні панелі.

- SIEM може виявити секретні, шкідливі повідомлення та зашифровані канали.

- Кібератака може бути виявлена за допомогою SIEM з точністю, яка дозволяє визначити як нападника так і жертву.

2.2 Задачі та питання яка вирішує SOC

SOC(Security Operation Center) - це команда фахівців з безпеки яка відповідає за моніторинг та боротьбу з загрозами та інцидентами для IT-інфраструктури організації, оцінку систем безпеки, виявлення та виправлення вразливостей, а також підвищення стійкості до кібератак.

Основна відповідальність команди центру безпеки (SOC) полягає у тому, щоб забезпечити захист інформаційних активів організації від несанкціонованого доступу (ризик конфіденційності), несанкціонованої зміни даних/інформації (ризик цілісності) та відмови в обслуговуванні (ризик доступності). Таким чином, SOC забезпечує захист IT-інфраструктур організації як локальної (у центрі обробки даних), так і в хмарі (наприклад, хмара Microsoft або Oracle, Azure SaaS), а також конфіденційних даних про клієнтів/бізнес, маючи видимість на всі вразливі місця, загрози та джерела загроз для ефективного пом'якшення та захисту до виникнення порушення.

Це досягається шляхом швидкого виявлення та виявлення підозрілих/зловмисних дій із застосуванням відповідного плану реагування для пом'якшення впливу або виникнення таких дій. Якщо порушення таки трапляються, аналітики SOC несуть головну відповідальність за захист організації від такої загрози шляхом протидії атаці. Аналітик SOC відіграє провідну роль у реалізації стратегії кіберзахисту організації, гарантуючи, що ролі та відповідальність, необхідні для актуалізації стратегії, визначені та розподілені в той час як ресурси, необхідні/бюджетні для впровадження та забезпечення безпеки організації. Будучи зберігачем/власником процесу

плану реагування на інциденти безпеки організації, аналітик SOC відповідає за

розробку та впровадження політики та процедури реагування на інциденти безпеки організації та забезпечує участь керівництва у процесі. У плані реагування на інциденти повинні бути визначені можливі інциденти безпеки та їх класифікація або ранжування з точки зору критичності/серйозності та впливу. Потім повинні бути визначені процедури ескалації та підзвітності за різні рівні/категорії інцидентів, а аналітик SOC зобов'язаний забезпечити належну ескалацію інцидентів та їх лікування відповідно до плану/процедури реагування на інциденти.

У плані реагування на інциденти повинні бути визначені можливі інциденти безпеки та їх класифікація або ранжування з точки зору критичності/серйозності та впливу. Аналітик центру безпеки повинен мати можливість бачити дії, що виконуються у всіх інформаційних активах організації, наприклад, брандмауер периметра, пристрої основної мережі (комутатори, маршрутизатори, системи запобігання вторгненням, системи виявлення вторгнень), віртуалізована інфраструктура (VMware, ESXi Host), підприємство сервери (Windows, UNIX, LINUX), бази даних, корпоративні системи резервного копіювання та зберігання даних, кінцеві точки (робочі станції, ноутбуки, КПК, мобільні пристрої), пристрої голосового зв'язку (VOIP) та інші інфраструктури підприємства. Таким чином, аналітик повинен переконатися, що як мінімум критичні активи організації, як зазначено вище, знаходяться в моніторингу. Щоб досягти цього, аналітик SOC повинен отримати звіти про класифікацію активів та аналіз впливу на бізнес (BIA) від функції ризику, щоб дати йому можливість визначити пріоритети моніторингу інформаційних активів на основі їхньої важливості для організації (також відомий як моніторинг на основі ризику). [1]

Враховуючи обмеженість ресурсів та обмежені ліцензії, доступні на корпоративних платформах моніторингу інцидентів безпеки/журналів організації та кореляції (наприклад, інструменти SIEM, FIM та DAM), дуже важливо прийняти підхід моніторингу на основі ризиків, щоб аналітик SOC мав належну видимість щодо всіх інформаційних активів порядку від найбільш критичного до найменш критичного. Таким чином, BIA та звіти про класифікацію активів використовуються для визначення активів/серверів.

Аналітики SOC ведуть журнали інцидентів безпеки для організації, які є базою даних усіх інцидентів безпеки, зафіксованих в IT-активах організації та виявлених інструментами моніторингу SOC. Журнал інцидентів здебільшого повідомляється керівництву на періодичній основі та регулюючим органам відповідно до вимог для прийняття рішень та відповідності.

За допомогою журналу інцидентів організація має видимість і розуміння природи, типу та частоти інцидентів безпеки, що відбуваються в IT-інфраструктурі організації, та дозволити їй виконати оцінку основних причин та наслідків таких інцидентів для прийняття рішення про відповідний план пом'якшення та лікування. запобігти появі у майбутньому.

Журнал інцидентів може бути поданий до бази даних управління проблемами (PMDB) організації для вирішення повторюваних інцидентів, які класифікуються як проблеми для аналізу першопричин та дій для усунення. Журнал інцидентів також може стати основою для визначення ефективності заходів безпеки та контролю, запроваджених в IT-інфраструктурі організації. На основі запису або журналу інцидентів безпеки організації, аналітик SOC може вимагати розробити програму навчання та підвищення відповідальності для інформування працівників та адміністраторів IT-інфраструктур в організації щодо найкращих методів безпеки та прийнятного використання інформаційних активів, які

підвищуватимуть безпеку. інформаційних активів та інфраструктури організації.

Основні задачі SOC:

1) Виконувати моніторинг в системах, шукати та аналізувати вторгнення в режимі реального часу.
2) Запобігати кіберзагрозам, діючи на випередження: безперервно сканувати комп'ютерні мережі на вразливості та аналізувати інциденти безпеки.
3) Швидко реагувати на підтверджені інциденти та виключати помилкові спрацьовування.
4) Формувати звіти про стан безпеки, кіберінциденти та патерни поведінки зловмисника
5) Аналіз мережевого трафіку та журналів.
6) Аналіз шкідливих програм та криміналістична експертиза.
7) Створення та розгортання сповіщень безпеки
8) Переглядати антивірусні засоби та засоби захисту від шкідливих програм, засоби захисту кінцевих точок(EDR) та запобігання втрати даних.

Найважче у роботі SOC – постійно аналізувати великі обсяги даних. Центр забезпечення безпеки збирає, зберігає та аналізує від десятків до сотень мільйонів подій безпеки щодня.

Структура команди SOC:

1.SOC Tier 1 — щодня отримує та переглядає сповіщення. Переглядає останні сповіщення SIEM, щоб побачити їх актуальність та терміновість. Здійснює сортування, щоб переконатися, що відбувається справжній інцидент безпеки. Контролює та налаштовує інструменти моніторингу безпеки.

2.SOC Tier 2 — розглядає реальні інциденти безпеки. Оцінює інциденти, виявлені аналітиками рівня 1. Використовує дані про загрози, такі як оновлені правила та індикатори компрометації (IOC), щоб точно визначити уражені системи та масштаби атаки. Аналізує запущені процеси та конфігурації в уражених системах. Здійснює поглиблений аналіз розвідки загроз, щоб знайти зловмисника, тип атаки та дані чи системи, на які вплинуло. Створює та реалізує стратегію стримування та відновлення.

3.SOC Tier 3 — більш досвідчений, ніж Tier 2. Займається критичними інцидентами.

Виконує оцінку вразливості та тести на проникнення, щоб оцінити стійкість організації та виділити слабкі місця, які потребують уваги. Переглядає сповіщення, дані щодо загроз та даних безпеки. Визначає загрози, що проникли в мережу, а також прогалини та вразливості безпеки, які наразі невідомі.

4.SOC Manager— керує та визначає пріоритети дій під час ізоляції, аналізу та стримування інциденту. Вони також повідомляють внутрішнім і зовнішнім зацікавленим сторонам будь-які особливі вимоги щодо інцидентів високої серйозності.

2.3 CSIRT: роль, структура, функціонування

CSIRT є життєво важливим компонентом сучасної кібербезпеки, відповідальним за швидке реагування на такі інциденти, як витоки даних та атаки програм-вимагачів. CSIRT не лише зменшують збитки, але й зосереджуються на запобіганні ризикам. Зі зростанням кіберзагроз CSIRT залишаються важливими, адаптуючись до нових технологій та організаційних потреб для захисту від потенційних збоїв та фінансових втрат.

У цьому розділі розглядається склад та призначення групи реагування на інциденти комп'ютерної безпеки (CSIRT). CSIRT — це група фахівців з різним досвідом роботи в галузі IT та кібербезпеки. Їхня мета — швидко та ефективно реагувати на інциденти кібербезпеки, а також працювати над запобіганням виникненню таких інцидентів.

CSIRT – це група людей, організованих у формальний підрозділ, чиєю визначеною місією є забезпечення швидкого, орієнтованого на результат реагування на інциденти кібербезпеки, такі як витік даних або атаки програм-вимагачів. Зменшення ризиків також зазвичай є пріоритетом CSIRT, оскільки запобігання атаці краще, ніж реагування на неї.

З цією метою CSIRT надають послуги з оцінки та управління ризиками з метою запобігання кібернадзвичайним ситуаціям. Основне припущення полягає в тому, що будь-яка організація, яка покладається на комп'ютери, повинна мати формальну можливість реагування на інциденти, яку виконує спеціальна команда.

CSIRT, ймовірно, не виконує кожен процес реагування на інциденти. Швидше, команда доповнює власні зусилля, координуючи дії інших груп, працюючи на основі підготовлених ними планів та протоколів. Зокрема, CSIRT намагається стримати загрозу або атаку, усунути загрозу, а потім контролювати відновлення. Наприклад, якщо шкідливе програмне забезпечення захоплює сервер, команда безпеки дотримуватиметься існуючого протоколу CSIRT та ізолює сервер, щоб шкідливе програмне забезпечення не могло поширитися по мережі. Потім CSIRT координуватиме виконання процесу, який усуває шкідливе програмне забезпечення та відновлює належну роботу сервера.

Часто CSIRT проводить розслідування після інциденту та виконує або доручає іншим виконувати подальші завдання, наприклад,

встановлення патчів операційних систем, скидання налаштувань брандмауерів або забезпечення того, щоб захисні технології, такі як системи виявлення вторгнень (IDS), були налаштовані для виявлення будь-якого шкідливого програмного забезпечення, що потрапило на сервер. У рамках цього процесу CSIRT може оновлювати свій план реагування. Крім того, CSIRT може брати участь у перегляді та доопрацюванні політик безпеки. Він також може керувати аудитами.

Основна робота CSIRT — це реагування на інциденти. Бажаний результат полягає у швидкості, але також і правильності процесу реагування.

Кожна CSIRT працює по-різному, але цілі завжди однакові: мінімізувати пошкодження систем і даних, усунути загрозу та швидко відновити працездатність систем.

Підготовка є одним із ключових факторів успіху. Це не гламурна робота, і може здаватися, що CSIRT «нічого не робить» між надзвичайними ситуаціями. Однак правда полягає в тому, що CSIRT постійно вдосконалює свої політики та процедури, а також взаємодіє зі своїми партнерськими групами в організації. Наприклад, CSIRT регулярно оновлює систему оркестрації безпеки, автоматизації та реагування (SOAR) центру операцій безпеки (SOC) та його посібники з інцидентів. З іншого боку, CSIRT завжди вивчає найновіші дані про загрози, можливо, синхронно з Центром обміну та аналізу інформації (ISAC).

Компоненти CSIRT

CSIRT вже багато років є невід'ємною частиною ландшафту інформаційної безпеки, що відображається в самій назві — повертаючись до епохи, коли кілька великих комп'ютерів домінували в тому, що тоді називалося відділом управлінських інформаційних систем (MIS). Сьогодні ніхто не сказав би: «У нас стався комп'ютерний інцидент». Однак тоді, якщо «комп'ютер», можливо, масивний мейнфрейм у «скляному будинку»,

мав проблему безпеки, CSIRT був готовий відреагувати. Кібербезпека стала набагато серйознішою та складнішою за минулі десятиліття, але потреба в CSIRT залишається. Скоріше, організаціям потрібен CSIRT більше, ніж будь-коли[5].

CSIRT є необхідністю, оскільки ставки дуже високі в сучасному світі серйозних загроз. Компанії та організації державного сектору повинні захищатися від наполегливих та витончених супротивників. У деяких випадках атаки здійснюються з боку держав. Серйозний інцидент у сфері кібербезпеки може завдати значної шкоди операціям, фінансам та репутації.

Добре спланована та швидка реакція є абсолютним імперативом. Саме це пропонують CSIRT.

Сьогодні роль CSIRT поєднується з низкою різних галузей IT та безпеки. Наприклад, якщо в компанії є SOC, команда, яка його керує, працюватиме з CSIRT, можливо, використовуючи його процедури. У деяких випадках самі технології взяли на себе деякі традиційні обов'язки CSIRT. Наприклад, платформа SOAR може мати політики CSIRT, вбудовані в її робочі процеси та «посібники» щодо пом'якшення загроз.

Кожен CSIRT має свій власний чіткий склад. Однак більшість CSIRTS поєднують людей та політики таким чином, що чітко визначають їхні місії. Що стосується людей, CSIRT зазвичай має основну групу відданих членів, яка доповнюється експертами, що працюють з CSIRT за потреби. Члени команди незмінно мають різний досвід та навички. Наприклад, деякі є експертами із захисту систем Windows, а інші знають про Linux. Основна команда може бути призначена до CSIRT на повний робочий день, але це трапляється здебільшого у дуже великих організаціях. У більшості випадків члени команди CSIRT мають «денну роботу» у відділах IT та кібербезпеки.

Щодо політики, окрім місії CSIRT та письмових визначень відповідних груп, CSIRT створює та підтримує набір документів, які визначають, як функціонує CSIRT. Наприклад, CSIRT зазвичай має централізований план реагування на інциденти, який письмово декларує, як команда здійснює процеси реагування на інциденти на місці порівняно з реагуванням на інциденти по телефону. План показує, як CSIRT координує реагування на інциденти, розподіляючи ресурси команди між кількома групами учасників.

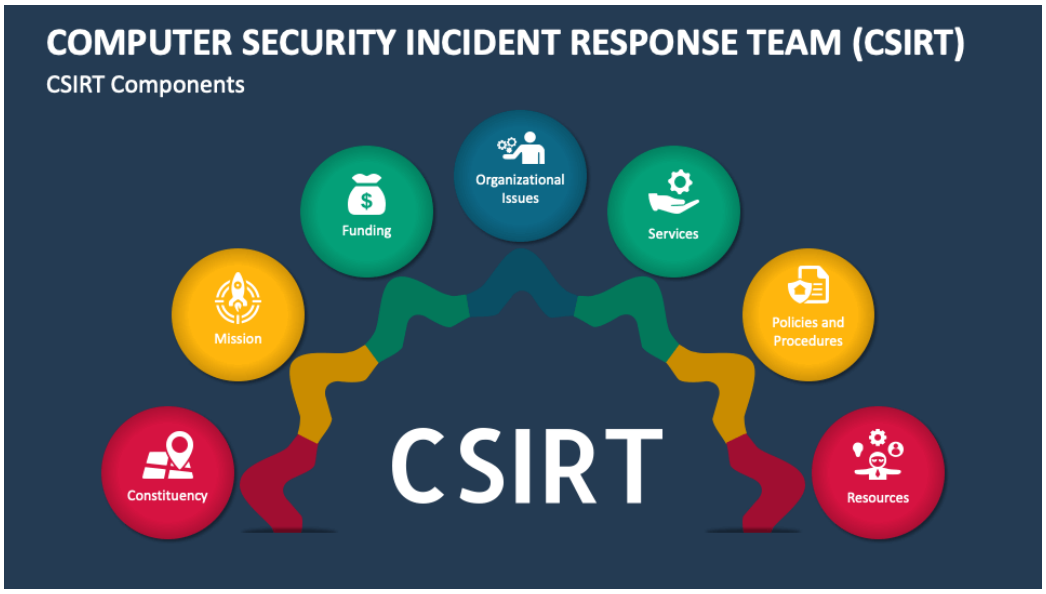


Рисунок 2.2 Компоненти CSIRT

В яких країнах використовують CSIRT

1. США

- Національна команда: US-CERT (частина CISA – Cybersecurity and Infrastructure Security Agency).
- Особливості: Працює в тісній співпраці з приватним сектором, органами влади та міжнародними партнерами. Має добре

структуровану систему обміну інформацією про загрози (наприклад, через платформу AIS).

- Переваги: Високий рівень автоматизації, великі інвестиції в кібербезпеку, постійна взаємодія з провідними технологічними компаніями.

2. Німеччина

- Національна команда: CERT-Bund (керується Федеральним відомством з інформаційної безпеки – BSI).
- Особливості: Обслуговує державні структури та інфраструктурно важливі об’єкти.
- Переваги: Має сучасні технічні засоби аналізу інцидентів, добре інтегрована у європейську систему реагування через ENISA.

3. Японія

- Національна команда: JPCERT/CC (Japan Computer Emergency Response Team Coordination Center).
- Особливості: Перша CSIRT в Азії. Співпрацює з урядом, промисловістю та академічними установами.
- Переваги: Високий рівень фахової підготовки, фокус на дослідження кіберзагроз.

4. Естонія

- Національна команда: CERT-EE (діє під Агентством інформаційних систем Естонії – RIA).
- Особливості: Стала одним із прикладів ефективного кіберзахисту після масованої кібератаки у 2007 році.
- Переваги: Високий рівень діджиталізації держави, добре скоординована кіберполітика.

5. Велика Британія

- Національна команда: NCSC (National Cyber Security Centre), фактично функціонує як CSIRT.
- Особливості: Частина розвідувальної структури GCHQ. Має повноваження як для захисту, так і для активного реагування.
- Переваги: Ефективне публічне інформування, регулярні звіти про загрози, сильна взаємодія з приватним секторо

6. Нідерланди

- Національна команда: NCSC-NL.
- Особливості: Окрім реагування, активно займається попередженням атак через обмін інформацією.
- Переваги: Прозора робота, широке міжнародне співробітництво.

3 РЕКОМЕНДАЦІЇ З УДОСКОНАЛЕННЯ ЗАХИСТУ ІОТ ВІД КОМП'ЮТЕРНИХ ІНЦИДЕНТІВ

3.1 **Архітектурні принципи та технічні підходи до захисту IoT на основі туманних обчислень**

Інтернет речей дедалі більше перетворюється на основний чинник проривних змін у сфері інформаційних технологій. З постійним розвитком IoT кількість його користувачів поступово збільшується, а обсяг передачі даних стрімко зростає, що призводить до перевантаження хмарного сервера. Класична парадигма централізованих хмарних обчислень стикається з низкою проблем, таких як висока затримка, низька пропускна спроможність і збої в роботі мережі. Як нова модель обчислень, туманні обчислення пропонують новий спосіб зменшити навантаження на хмарні сервери. Туман забезпечує оброблення та збереження інформації IoT локально на пристроях IoT замість того, щоб відправляти їх у хмару. На відміну від хмари, туман надає послуги зі швидшим відгуком і вищою якістю. Тому туманні обчислення можна вважати найкращим вибором для того, щоб дозволити Інтернету речей надавати ефективні та безпечні послуги для багатьох користувачів IoT. Однак раціональне використання ресурсів туманного вузла все ще залишається складним і ключовим моментом.

Якщо порівнювати тришарову архітектуру системи хмарних обчислень (рівень кінцевого користувача хмарних обчислень, мережний рівень і хмарний рівень) з архітектурою туманних обчислень, то другу систему можна розподілити на п’ять шарів: рівень кінцевого користувача, рівень мережі доступу, туманний рівень, основний мережний рівень і хмарний рівень, відповідно, як показано на рис. 3.1. Неважко помітити, що ближче до нижнього рівня, то більша зона поширення і менша затримка передачі даних кінцевого користувача на цей рівень .

На рисунку 3.2 наведено основне обладнання та найважливіші функції зазначених п’яти рівнів.

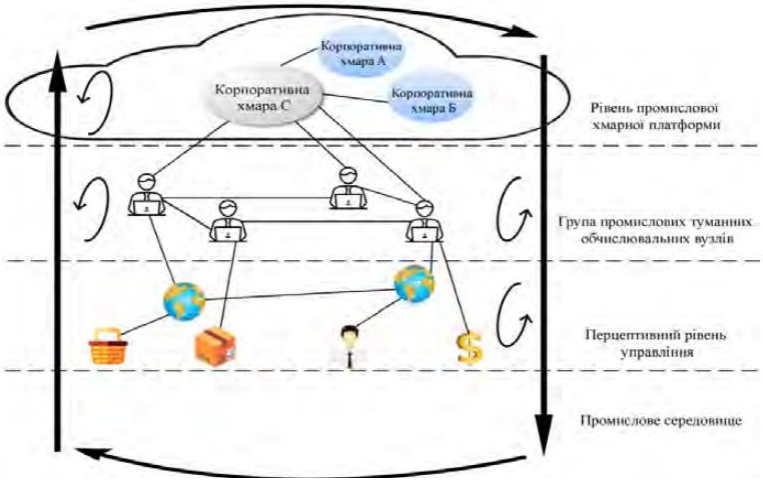


Рисунок 3.1. Схема архітектури туманних обчислень

Рівень	Основне обладнання	Основна функція
Рівень кінцевого користувача	Термінальні пристрої та сенсорні вузли мобільних телефонів користувачів, портативних комп’ютерів тощо	Термінальні пристрої та сенсорні вузли мобільних телефонів, портативних комп’ютерів тощо
Рівень мережного доступу	Бездротове мережне обладнання є основою, яку доповнює дротове мережне обладнання	Надсилати завдання кінцевого користувача на відповідний вузол туману за заздалегідь визначеним правилом
Туманний рівень	Туманний периферійний вузол, мікротуман, туманний сервер	Забезпечити певний рівень обчислень, зберігання та зв’язку
Основний мережний рівень	Основне мережне обладнання	Надсилайте завдання, що виходять за межі обчислення шару туману або ємності зберігання, до хмарного центру оброблення даних
Хмарний рівень	Сервер хмарного дата-центру	Резервне копіювання даних, оброблення великих обчислювальних завдань

Рисунок 3.2 Системна архітектура туманних обчислень

У запропонованій концепції туманних обчислень завдяки розширенню туманного шару з можливостями обчислень і зберігання між хмарним сервером і термінальним пристроєм ключові дані та обчислювальні сервіси, необхідні для локалізації на хмарному сервері, переміщуються на туманний сервер, розташований ближче до термінального пристрою. Забезпечуючи кешування даних, локалізовані обчислення та інші функції, можна краще задовільнити попит на високий трафік і низьку затримку мобільних застосунків. Основними елементами рівня кінцевого користувача зазвичай є мобільний телефон, портативний комп'ютер та інші термінальні пристрої[11].

Із розвитком технології сенсорних мереж сенсорний вузол також відіграватиме важливу роль на цьому рівні. Ними можуть бути розміщені десь стаціонарні пристрої, наприклад датчики на світлофорах по обидва боки дороги або мобільні термінали, зокрема мобільні телефони й ноутбуки користувачів. На цьому рівні ці пристрої є генераторами і користувачами контенту. На зазначеному рівні генеруються завдання, а оброблені результати повертаються на цей самий рівень. Крім того, термінальний пристрій також має виявити та вказати туманний вузол, що відповідає переадресації завдання .

Логічно розподілити IoT на три основні рівні: рівень сприйняття, транспортний рівень і рівень оброблення. Крім того, застосування інформації, сформованої на рівні оброблення, також можна розглядати як прикладний рівень. Кожен логічний рівень охоплюється базовою архітектурою безпеки IoT. Сторона сенсорного рівня та транспортного рівня, близькі до рівня зондування, здебільшого розподіляються за допомогою туманного обчислювального рівня, як показано на рис. 3. Розглянуто та запропоновано різні заходи безпеки для апаратного рівня та рівня вбудованих пристроїв під шаром туманних обчислень для захисту від проблем безпеки, з якими система IoT має зіткнутися знизу . Наприклад, щоб забезпечити відстеження та цілісність даних, необхідно

використовувати функцію антиклонування датчика на фізичному рівні; щоб поліпшити управління надійністю, необхідна функція фізичного неклонування та лічильники продуктивності апаратного забезпечення; щоб поліпшити конфіденційність і захист приватності, необхідно застосовувати легковаговий алгоритм шифрування. На додаток до вищезазначених елементів захисту існують різні алгоритми, такі як алгоритми шифрування, хеш-функції та алгоритми обміну ключами, що можуть бути використані для парольних елементів захисту безпеки IoT[13].

Використання різних криптографічних алгоритмів і вибір оброблення інформації в різних місцях оброблення може суттєво вплинути на споживання енергії. Тому, щоб не споживати занадто багато енергії, необхідно обрати певне місце оброблення і криптографічний алгоритм відповідно до обсягу інформації.

Рисунок 3.3 Відносне положення туманного обчислювального шару в системі Інтернету речей

Наприклад, у межах датчика він може обробляти дані розміром до 1 КБ; якщо обсяг інформації у межах 1 МБ, то як місце оброблення можна використовувати вузол туману; якщо дані в межах 1 ГБ або перевищують 1 ГБ, вони мають оброблятися на шлюзі або в об’єднаній інфраструктурі вищого рівня. Щоб скоротити час відгуку системи, необхідно повністю

локалізувати інформацію, що значно підвищить ефективність системи IoT. Потужні мікроконтролери роблять систему інтелектуальних датчиків на чипі все більш досконалою. Наприклад, флеш-мікроконтролер виробництва AD має вбудовану програмну флеш-пам'ять обсягом 64 КБ і флешпам'ять даних 4 КБ, 2304 байти оперативної пам'яті даних і значну кількість периферійних пристроїв, таких як 12-розрядний АЦП/ЦАП (аналого-цифровий перетворювач / цифро-аналоговий перетворювач), лічильник часових інтервалів, сторожовий таймер тощо. Ядро 8052 використовується з тактовою частотою до 20 МГц.

Такого рівня системи на кристалі достатньо для підтримки легких криптографічних операцій. Оскільки для управління сенсорною мережею в IoT зазвичай використовується 16/32-розрядний удосконалений RISC-процесор зі скороченим машинним набором інструкцій + вбудована архітектура Linux у поєднанні з повною підтримкою потужності та апаратного забезпечення, він повністю здатний забезпечити більш високий рівень захисту шифрування, робота якого здебільшого еквівалентна персональному комп'ютеру. Зарубіжні дослідники провели ґрунтовне вивчення, узагальнили наявні елементи шифрування різних рівнів IoT за результатами досліджень і склали відносно надійну рекомендацію (див. рис. 3.4).

	Датчик	Вузол	Шлюз	Спільна архітектура
Додавання та розшифровування	PRESENT	CLEFIA	ASE	RSA
Алгоритм	mCRYPTON	AES	ECC	
Хеш-функція	DM-PRESENT	PROP	HMAC	SHA-3
Алгоритм обміну ключами	DH-512	DH-512	ECDH	DH
Цифровий підпис	ECDSA-163	ECDSA-233	DSA	ECDSA-409

Рисунок 3.3 . Елементи шифрування кожного рівня Інтернету речей

Щоб побудувати архітектуру безпеки IoT на основі рівня туманних обчислень, перше питання полягає у виборі правильної апаратної конфігурації туманних обчислень. Необхідно знайти відповідні заходи безпеки й розгорнути місце для створення та перевірки відповідного методу шифрування. Використовуючи новий рівень туманних обчислень

для тестування наявного полегшеного методу шифрування на предмет затримки та енергоспоживання, можна покращити коефіцієнт безпеки, удосконаливши наявний простий метод шифрування або перейшовши на більш надійний алгоритм безпеки, щоб відповідати вищезазначеним вимогам. Після цього варто прагнути оптимізувати базову архітектуру системи IoT, а також консолідувати та зміцнити основу системи IoT способом зменшення обчислювальних затримок, викликаних використанням заходів безпеки, без зниження показників безпеки та збільшення енергоспоживання.

Для того, щоб побудувати систему безпеки IoT на основі туманних обчислень, необхідно повністю застосовувати всі види ресурсів, що вводяться на рівні туманних обчислень. На основі дотримання наявних заходів безпеки досягається максимальна інтенсивність безпеки. Згідно з показниками коефіцієнт безпеки традиційних датчиків недостатньо високий, оскільки вони генерують лише відповідні цифрові результати вимірювань щодо об'єктивної кількості, зібраної ними самими, а потім безпосередньо шифрують і завантажують результати. Тепер є спосіб підвищити коефіцієнт безпеки датчика, який полягає в тому, щоб спробувати витягти унікальний ідентифікатор кожного датчика, а потім модифікувати відповідний алгоритм безпеки в датчику, щоб унікальний ідентифікатор датчика також використовувався для обчислення шифрування. Ці параметри значно покращать безпеку вихідної інформації. Через обмеженість різних ресурсів на терміналах IoT легковагові алгоритми безпеки все ще залишаються найбільш широко використовуваними методами для терміналів IoT. Якщо IoT-термінал може надати більше обчислювальної потужності та простору завдяки туманним обчисленням, він має достатньо можливостей для підтримки алгоритмів безпеки з вищим ступенем захисту і складнішими обчисленнями. Отже, IoT-термінали можуть значно підвищити свою обчислювальну потужність і продуктивність безпеки. Однак для того, щоб реалізувати цю ідею,

необхідно належним чином удосконалити та впровадити алгоритм безпеки на основі повного дослідження, зрозуміти наявні легковагові алгоритми безпеки, прискорити роботу, підвищити рівень безпеки та знизити енергоспоживання. без зниження показників безпеки та збільшення енергоспоживання. Для того, щоб побудувати систему безпеки IoT на основі туманних обчислень, необхідно повністю застосовувати всі види ресурсів, що вводяться на рівні туманних обчислень.

На основі дотримання наявних заходів безпеки досягається максимальна інтенсивність безпеки. Згідно з показниками коефіцієнт безпеки традиційних датчиків недостатньо високий, оскільки вони генерують лише відповідні цифрові результати вимірювань щодо об'єктивної кількості, зібраної ними самими, а потім безпосередньо шифрують і завантажують результати. Тепер є спосіб підвищити коефіцієнт безпеки датчика, який полягає в тому, щоб спробувати витягти унікальний ідентифікатор кожного датчика, а потім модифікувати відповідний алгоритм безпеки в датчику, щоб унікальний ідентифікатор датчика також використовувався для обчислення шифрування. Ці параметри значно покращать безпеку вихідної інформації. Через обмеженість різних ресурсів на терміналах IoT легковагові алгоритми безпеки все ще залишаються найбільш широко використовуваними методами для терміналів IoT. Якщо IoT-термінал може надати більше обчислювальної потужності та простору завдяки туманним обчисленням, він має достатньо можливостей для підтримки алгоритмів безпеки з вищим ступенем захисту і складнішими обчисленнями. Отже, IoT-термінали можуть значно підвищити свою обчислювальну потужність і продуктивність безпеки. Однак для того, щоб реалізувати цю ідею, необхідно належним чином удосконалити та впровадити алгоритм безпеки на основі повного дослідження, зрозуміти наявні легковагові алгоритми

безпеки, прискорити роботу, підвищити рівень безпеки та знизити енергоспоживання[19].

3.2 Впровадження передових засобів виявлення та реагування (SIEM, ШІ, автоматизація)

Ландшафт кібербезпеки розвивається безпрецедентними темпами. Згідно з нещодавнім звітом Kaspersky Human Factor 360, 77% компаній зазнали щонайменше одного порушення кібербезпеки у 2023 році, причому багато хто зіткнувся з кількома інцидентами того ж року.

Кібератаки не лише зростають за частотою, але й стають складнішими та витонченішими, використовуючи методи на основі штучного інтелекту для обходу традиційних засобів захисту, що робить виявлення та реагування в режимі реального часу важливішими, ніж будь-коли.

Крім того, організації повинні вирішувати проблеми, що виникають через нормативні вимоги — галузеві норми, такі як GDPR, CCPA та ISO 27001 — що стосуються зберігання даних, аудиту та розслідування інцидентів. Оскільки ЄС запровадив Закон про цифрову операційну стійкість або DORA, який набув чинності 17 січня 2025 року, організації змушені впроваджувати ще надійніші системи безпеки.

IT-командам також доводиться справлятися зі стрімким розширенням дистанційної роботи, використанням власних пристроїв (BYOD) та впровадженням SaaS-додатків – усе це розширило корпоративні периметри за межі традиційних систем безпеки. Керівники IT-відділів вищої ланки, які вже перебувають під тиском, стикаються з глобальною нестачею кваліфікованих фахівців з кібербезпеки. Станом на початок 2025 року розрив у кібернавичках збільшився на 8 відсотків порівняно з 2024 роком, що підкреслює зростання попиту на експертизу в галузі кібербезпеки.

Від видимості до дії: сила SIEM

Зіткнувшись із постійно скороченими бюджетами, компанії централізують IT-безпеку, об'єднуючи дані про загрози та ризики в одну систему. Система управління інформацією та подіями безпеки (SIEM) посилює захист, аналізуючи дані кібербезпеки в режимі реального часу. Вона покращує виявлення по всій мережі, пришвидшує реагування на інциденти, забезпечує кращу видимість та покращує відповідність вимогам, пропонуючи надійніший захист від загроз[2].

Але з розвитком кібератак повинна розвиватися і технологія безпеки SIEM. Однією з ключових переваг сучасних рішень SIEM є можливість візуалізації даних та ефективного визначення пріоритетів інцидентів. Покращені панелі інструментів та інструменти звітності дозволяють командам безпеки швидко оцінювати серйозність загроз, налаштовувати сповіщення та визначати пріоритет інцидентів з високим рівнем ризику над інцидентами з низьким пріоритетом, зменшуючи тягар хибнопозитивних результатів. Рішення SIEM можуть інтегруватися зі сторонніми інструментами, такими як брандмауери, системи EDR та управління ідентифікацією, що забезпечує цілісний підхід до безпеки. Агрегуючи аналітичні дані з кількох джерел, SIEM забезпечує комплексне уявлення про загрози в IT-екосистемі. Щоб скоротити час реагування та мінімізувати вплив інцидентів безпеки, можливості автоматизованого реагування є ще однією трансформаційною функцією SIEM. Завдяки попередньо визначеним робочим процесам та сценаріям, рішення може автоматично зменшувати загрози, такі як ізоляція скомпрометованих кінцевих точок або блокування шкідливих інтернет-протоколів (IP), без ручного втручання.

Миттєва аналітика загроз підвищує точність виявлення систем SIEM, співвідносячи сповіщення про безпеку з глобальними аналітичними потоками, що дозволяє командам безпеки проактивно виявляти нові загрози, перш ніж вони переростуть у серйозні порушення. Розроблені для

масштабованості та ефективності, платформи SIEM можуть обробляти зростаючі обсяги даних, забезпечуючи обробку подій у режимі реального часу та високошвидкісну кореляцію даних у міру зростання потреб безпеки. Додавання штучного інтелекту до комплексу центрів операцій безпеки розширює потенціал SIEM, розкриваючи ще більший потенціал.

Трансформаційна роль штучного інтелекту в SIEM

Штучний інтелект революціонізує SIEM-системи, перетворюючи їх з реактивних інструментів на проактивні, інтелектуальні рішення безпеки. Одночасно аналізуючи величезні обсяги даних безпеки, ШІ може виявляти аномалії та закономірності, які традиційні методи часто пропускають. Сучасні SIEM-системи використовують передову аналітику на основі ШІ, машинне навчання та глибоке навчання для підвищення загальної ефективності кібербезпеки. Використовуючи прогнозні алгоритми, нейронні мережі та статистичні моделі, ШІ допомагає розставляти пріоритети сповіщень, зменшувати кількість хибнопозитивних результатів та призначати активам оцінки ризику на основі ШІ. Цей інтелектуальний процес сортування оптимізує операції безпеки, гарантуючи, що команди безпеки зосереджуються на найважливіших загрозах, і дозволяє швидше реагувати. Це безпосередньо зменшує середній час виявлення (MTTD) та середній час реагування (MTTR). ШІ також постійно навчається на історичних моделях атак, адаптуючись до нових та нових загроз, роблячи SIEM-системи все більш гнучкими та стійкими.

Окрім технічних можливостей, SIEM на базі штучного інтелекту має глибокий вплив на бізнес-операції. Прискорюючи виявлення та реагування на загрози, організації можуть запобігати дороговартісним витокам даних, захищати конфіденційну інформацію клієнтів та

підтримувати дотримання галузевих норм. Можливості автоматизації SIEM на базі штучного інтелекту значно зменшують ручне навантаження аналітиків безпеки, дозволяючи їм зосередитися на стратегічному пом'якшенні загроз та розширених завданнях безпеки, а не на рутинному моніторингу та управлінні сповіщеннями.

Крім того, ШІ покращує операції, безперешкодно інтегруючи аналітику загроз у режимі реального часу, збагачуючи дані про події зовнішніми даними про загрози, що покращує прийняття рішень та дозволяє проактивно виявляти загрози. Ця інтеграція посилює здатність SIEM виявляти складні загрози та визначати вразливості до того, як вони будуть використані. [17]

Оскільки кібератак стає все складнішим і частішим, системи SIEM на базі штучного інтелекту є важливими для підтримки надійної системи безпеки. Завдяки постійному розвитку та навчанню на основі нових даних, SIEM на базі штучного інтелекту перетворює традиційні операції безпеки на самовдосконалений, динамічний механізм захисту, що дозволяє компаніям випереджати кіберзагрози, оптимізуючи ресурси кібербезпеки.

Майбутнє кібербезпеки полягає в SIEM на базі штучного інтелекту. Оскільки кіберзагрози продовжують зростати у складності, поєднання SIEM зі штучним інтелектом стає важливим компонентом сучасних стратегій кібербезпеки. SIEM на базі штучного інтелекту покращує виявлення загроз та реагування на них, водночас забезпечуючи проактивний підхід до управління кіберризиками. Організації, які застосовують це потужне поєднання, будуть краще підготовлені до захисту від постійно мінливого ландшафту кіберзагроз. Інвестування в SIEM на базі штучного інтелекту – це не просто покращення безпеки, а забезпечення стійкості бізнесу у все більш цифровому світі. Ті, хто

впроваджує цю технологію, стануть лідерами в інноваціях у сфері кібербезпеки, випереджаючи супротивників та захищаючи свої критично важливі активи на довгі роки.

3.3 Кібербезпека під час війни: базові заходи з кіберзахисту для українських організацій та людей

Війна проти України на цифровому фронті ведеться вже не один рік. Ось декілька цифр.

За даними звіту від Microsoft, у 2021 році, ще до початку широкомасштабного вторгнення, проти нашої держави було спрямовано майже п‘яту частину усіх кібератак у світі. За цим показником ми поступаємось лише США.

Протягом наступного 2022 року, за даними Державного центру кіберзахисту, їх кількість зросла майже втричі. Починаючи з 24 лютого і до кінця минулого року урядова команда реагування на комп’ютерні надзвичайні події CERT-UA опрацювала 2 194 кіберінциденти. З них 120 атак були спрямовані на фінансовий сектор, 156 — на комерційні організації, 92 — на сектор телекомунікацій та розробників програмного забезпечення. У 2023-му ця інтенсивність зберігається. За І квартал цього року в CERT протидіяли 549 кібератакам. Україна наразі відстежує зловмисну активність понад 85 хакерських груп, більшість з яких пов’язані саме з росією. 90% із них або належать до силових структур країни-агресора, або узгоджують з ними свої дії. Партнери розуміють гостроту проблеми і допомагають на рівні держави. На початку червня США оголосили про надання Україні додаткових $37 мільйонів для зміцнення кібербезпеки. Ці гроші будуть спрямовані, передусім, на захист критично важливих для держави мереж.

Варто також відзначити, що, незважаючи на складну ситуацію і численні виклики для кібербезпеки, Україна їм протистоїть. Вона посідає 24-те зі 160 місць у рейтингу Національного індексу кібербезпеки, який

щорічно складає Фонд електронного врядування Естонії. Це доволі потужний показник, бо в цьому переліку ми випереджаємо навіть такі європейські країни, як Австрія, Швейцарія, Ірландія та Норвегія. Однак, 24 місце говорить про те, що слабкі місця в українському кіберзахисті все ще присутні і працювати точно є над чим.

Слабкі місця в кіберпросторі :

1. Досить висока залежність від іноземних виробників програмного забезпечення. В тому числі, з недружніх країн, таких як росія та білорусь.

2. Неналежний контроль за виконанням заходів із забезпечення кіберзахисту та інформаційної безпеки.

3. Вразливість цифрової інфраструктури підприємств через розосередження співробітників — віддалений формат роботи та передача задач на аутсорсінг.

4. Недосконале законодавство у сфері кібербезпеки та повільне переймання відповідного досвіду ЄС та впровадження нормативних актів інших країн.

Організація потужної атаки також потребує ресурсів і злагодженої дії зі сторони зловмисників. Тому націлені вони, зазвичай, на платоспроможний великий або середній бізнес.

Під загрозою енергетичні компанії, великі промислові, логістичні підприємства, телеком-компанії та розробники ПЗ. Але найсерйозніші атаки останніми роками йдуть на державний і особливо фінансовий сектор. Насамперед, цілями злочинців стають великі банки, які формують фінансову систему країни. [9]

Вони забезпечують доступ населення до базових фінансових сервісів — оплати рахунків, переведення коштів, керування власними фінансами загалом. Тому вони збирають, обробляють та зберігають велику кількість конфіденційної інформації, якою прагнуть заволодіти кіберзлодії. Отже, подбати про свою цифрову безпеку, передусім, має великий бізнес, але це не означає, що невеликі підприємства в безпеці.

Вони також можуть постраждати від кібератак, і для них цей удар може бути ще болючішим, ніж для великих компаній.

Загрози для бізнесу можуть бути як внутрішніми, так і зовнішніми. До перших належать вразливе програмне забезпечення та витоки через співробітників, або через їх провину. Найпопулярнішими зовнішніми є шкідливе ПЗ, DDoS-атаки, фішингові атаки, втрата пристроїв зі збереженими паролями, проникнення у мережу. Також атаки можуть бути комбінованими.

Потрапивши до мережі компанії, найчастіше зловмисники намагаються знищити або пошифрувати дуже важливу для неї інформацію. Насамперед, злодії намагаються видалити або пошкодити резервні копії, щоб не було можливості відновити дані.

Базовий захист будь-якої великої компанії від кіберзлочинців можна розділити на дві основні складові:

1.Навчання персоналу основам цифрової гігієни та кіберграмотності

Найслабкіше місце у кіберзахисті будь-якої компанії — люди. Насамперед, це стосується великих підприємств — адже чим більше співробітників, тим вразливішою є компанія. Тому що люди можуть відкривати фішингові листи, які надходять електронною поштою, заходити на підозрілі сайти, користуватися примітивними паролями та робити інші

недопустимі речі. Звичайно, якщо вони не розуміють, що все це несе загрозу.

Тому підлеглі мають знати, шо таке цифрова гігієна, вміти розпізнавати підозрілу активність, ознаки кібератак та знати порядок дій у таких випадках.

2.Побудова оборони від атак

Цим має займатись відділ IT-безпеки. На жаль, такий зараз є далеко не в усіх навіть великих бізнесах, не кажучи вже про малий. Так, люди, які здатні його очолити та зробити ефективним, коштують недешево. І його відсутність — суттєве заощадження коштів. Але в перспективі це може обійтись набагато дорожче або взагалі загрожувати існуванню компанії.

Це відділ, який, по-перше, навчатиме колег тій самій кіберграмотності, по-друге, моніторитиме та аналізуватиме вразливості, що постають перед підрозділами компанії, по-третє, вибудує багатоешелоновану оборону від атак, яка дозволить витримати удар. Налаштовувати брендмаузери, слідкувати за тим, щоб колеги користувались надійними паролями та використовували двофакторну аутентифікацію, шифрування важливих даних — все це складна, комплексна робота, але робити її необхідно.

Серед передових постачальників рішень для інформаційної безпеки можна відзначити такі компанії, як Microsoft, Barracuda, Fortinet, Commvault, Cisco, Palo Alto, CloudFlare, Ciber Future Foundation, Dell Technologies.

Microsoft пропонує цілий комплекс продуктів для захисту бізнесу: пакет захисту для підприємств від комплексних атак Microsoft 365

Defender; хмарне SIEM-рішення Microsoft Sentinel, яке надає розумну аналітику щодо захисту від загроз; рішення для ідентичностей та доступу Microsoft Entra та інші продукти. Базові сценарії кібербезпеки вбудовані навіть в офісний пакет Microsoft Office 365.

Як безпечно завантажувати й використовувати застосунки та файли

Кіберзлочинці постійно вигадують нові способи для обману користувачів через шкідливі застосунки та програми. Завантажити безкоштовний фільм, гру чи музику – завжди ризик інфікування шкідливим програмним забезпеченням. А мета зловмисників – отримати доступ до вашої особистої інформації.

Для безпеки ваших даних і пристроїв дотримуйтесь таких правил завантаження застосунків і файлів:

Використовуйте лише ліцензійне програмне забезпечення із перевірених джерел (магазинів Play Market, App Gallery, App Store і Google Play чи офіційних сайтів-розробників). Звертайте увагу на те, хто опублікував додаток, адже деякі магазини мають сумнівні копії популярних додатків. Російські віруси нині часто поширюються через “піратські” програми. [1]

Не завантажуйте файлів і застосунків із невідомих джерел (сумнівні сайти, сторінки й канали в соцмережах, невідомі відправники).

потенційно небезпечні розширення файлів: .exe, .bin, .ini, .iso, .dll, .com, .sys, .bat, .js, .apk;

потенційно безпечні розширення файлів: .docx, .zip, .rar, .pdf.

Встановили файл – перевірте його за допомогою антивіруса. Але нове шкідливе програмне забезпечення або код можуть бути визначеними тільки антивірусом, який регулярно оновлюється.

Якщо не можете придбати платну версію програми, знайдіть безкоштовний аналог, але не завантажуйте зламаних версій платних програм: зазвичай вони містять шкідливий програмний код.

Оберіть заборону встановлення застосунків з неперевірених джерел та автоматичного завантаження файлів, а для браузера – функцію “щоразу запитувати про місце зберігання файла перед завантаженням”. Якщо випадково перейдете за посиланням, яке автоматично розпочинає процес завантаження, він не розпочнеться, поки ви не підтвердите це.

Уникайте використання застосунків російських розробників: ВК, Одноклассники, Яндекс.Браузер, 1С, Mail.ru та інші – росіяни можуть їх відслідковувати. Перед завантаженням обов’язково перевіряйте інформацію про те, хто розробник та власник застосунка, чи не заборонений він в Україні.

Контролюйте дозволи, які запитує програма під час встановлення. Не всім застосункам для нормальної роботи необхідний доступ до вашої геолокації чи персональної інформації.

Оновіть застосунки у своєму смартфоні та програмне забезпечення на комп’ютері. Це необхідно, адже розробники постійно працюють над покращенням своїх безпекових протоколів.

Захист від шкідливих програм

Найперше, що допоможе вам захистити свої пристрої від “шкідників” – встановлення антивірусних програм. Рекомендовані програми: Avast, ESET, McAfee, Zillya.

Як не натрапити на антивірус-підробку?

Завантажуйте антивірусну програму тільки з офіційного сайту розробника чи з перевірених джерел (Play Market, App Gallery, App Store і Google Play). Якщо не можете придбати платну версію програми – знайдіть безкоштовний аналог, але не завантажуйте зламані версії платних програм. Регулярно оновлюйте антивірус. Тільки тоді програма вчасно попередить про загрозу.

Систематично перевіряйте ваш пристрій на наявність загроз, що можуть зашкодити вашим даним.

Також перевіряйте антивірусом USB-накопичувачі та інші зовнішні пристрої, які підключаєте до комп'ютера.

Періодично "скидайте" налаштування свого смартфона.

Так можна знешкодити програми "keylogger"-и, які відслідковують дії користувача.

Не переходьте за сумнівними посиланнями. Такими є:

1. Отримані від невідомих відправників на електронну скриньку, в SMS чи повідомленні в месенджерах і соцмережах;
2. Повідомлення із закликом до термінової дії та ті, де використовується надзвичайно актуальна та часто згадувана у ЗМІ тема;
3. Ті, що ведуть на сумнівні сайти чи канали в соцмережах;
4. Ті, що не мають протоколу безпеки: https – безпечне, http – потенційно небезпечне;
5. Ті, що містять слово /download/ – при переході за такими посиланнями одразу розпочинається завантаження файлу. Зловмисники, найвірогідніше, завантажать шкідливий код або приведуть на фішинговий сайт.

Звертайте увагу на різку та помітну зміну в роботі пристрою: різке зниження заряду, повільна робота, поява файлів, яких ви не створювали, чи програм, яких не встановлювали, поява невідомих програм в автозавантаженні при увімкненні пристрою тощо. Можливо, це наслідок діяльності шкідливих програм.

Надійні паролі

Подбайте про захищеність ваших пристроїв та облікових записів. Ненадійні паролі – легка здобич для ворожих хакерів і шахраїв.

Дотримуйтесь цих простих правил:

Замініть паролі в соцмережах, банківських акаунтах та на всіх сайтах, де може бути ваша персональна інформація, на надійніші.

Усі паролі рекомендовано змінювати раз на місяць.

Регулярно перевіряйте паролі на витік. Ось корисний сервіс, де можна це зробити.

На сайті потрібно ввести свій e-mail або номер телефону. Якщо паролі зареєстрованих на них облікових записів було зламано, сайт миттєво сповістить вас про це. Якщо ні, то витоку ваших даних не було.

Використовуйте менеджери паролів – це спеціальні застосунки, які зберігають ваші паролі в зашифрованому вигляді, і вам не доведеться запам’ятовувати всі складні комбінації, а лише пароль від самого застосунку. (Рекомендовані: 1Password, KeePassXC, Dashlane або менеджери в антивірусних програмах).

Двофакторна аутентифікація – це звичайна двоетапна перевірка при вході в акаунт. Налаштуйте її. Тоді при спробі зламу ви отримаєте SMS-повідомлення з проханням підтвердити вхід в акаунт.

Встановлюйте екранний пароль, графічний ключ або біометричний захист (відбиток пальця, розпізнавання обличчя чи голосу) для розблокування пристроїв.

Замініть стандартний PIN-код до SIM-карти.

Надійними паролями є ті які не містять поширених поєднань букв і слів; символів, що повторюються або йдуть один за одним (0000, 1111, abc123); вашого імені, прізвища, дати народження; імені, прізвища або дати народження ваших батьків, дітей, чоловіка або дружини.

Натомість містять спеціальні символи, цифри, великі та малі літери в кількості понад 8, а також слова, яких немає в українській чи англійській, і, бажано, в інших мовах теж створені за допомогою сервісу генерування паролів (наприклад, cyberpolice.gov.ua/generate-password) [18]

1. Використовуються тільки в одному сервісі (на кожен сервіс чи поштову скриньку – свій унікальний пароль)
2. Не зберігаються у вас на смартфоні або ноутбуці в нотатках чи на наліпці на вашому ноутбуці, що стоїть посеред офісу
3. Їх немає у базі com
4. Їх не знають ваші рідні, кохані, колеги
5. Ті, що істотно відрізняються від минулого пароля, що використовувався на цьому ж сервісі

Безпечні налаштування браузерів:

Підтримувати браузери у робочому стані – це своєчасно оновлювати їх, як і решту інстальованих на пристрої програм та саму операційну систему. А ще – завантажувати їх лише з офіційних сайтів і використовувати лише мінімум розширень до них.

Ось показники, які потрібно налаштувати у ваших браузерах:

1. У меню “Налаштування”
2. Конфіденційність та безпека – Безпека – Безпечний перегляд – Покращений захист
3. Конфіденційність та безпека – Безпека – Додатково – Завжди використовувати безпечне з’єднання
4. Завантажені файли – Завжди вказувати місце для завантаження

ВИСНОВКИ

У процесі написання дипломної роботи було проведено всебічне дослідження теоретичних і практичних аспектів управління реагуванням на комп’ютерні інциденти. В умовах стрімкого розвитку цифрових технологій та зростання обсягів кібератак особливої актуальності набуває питання своєчасного виявлення, аналізу та ефективного реагування на загрози, що виникають в інформаційних системах.

Проаналізовано класифікацію інцидентів інформаційної безпеки, їхні джерела, типи та потенційні наслідки для організацій. Досліджено методики виявлення і реагування на інциденти з урахуванням міжнародних стандартів (зокрема ISO/IEC 27035, ISO/IEC 27001) та національної нормативної бази. Виявлено, що ефективне управління інцидентами потребує чітко структурованих процесів, відповідального персоналу, налагоджених каналів комунікації та постійного моніторингу IT-інфраструктури.

Особливу увагу приділено системам SIEM та організаційним структурам типу SOC (Security Operations Center) і CSIRT (Computer Security Incident Response Team), які відіграють ключову роль у процесах

автоматизованого збору, аналізу та реагування на інциденти. Зазначено, що лише технічних засобів недостатньо — важливим є поєднання технологій, процесів і людського фактору.

Також розглянуто виклики та нові загрози в контексті безпеки пристроїв Інтернету речей (IoT), які становлять новий фронт атак для зловмисників. Показано, що слабкий захист IoT-пристроїв, недбале адміністрування, відсутність оновлень та низький рівень обізнаності персоналу є головними вразливими місцями сучасних організацій.

У рамках підрозділу 3.3 було проаналізовано специфіку кіберзахисту в умовах війни, коли кіберпростір використовується як ще один елемент гібридної агресії. Надано перелік базових технічних і організаційних заходів, які рекомендовано запроваджувати українським організаціям. Акцент зроблено на важливості формування культури кібергігієни та регулярного навчання персоналу.

У результаті дослідження сформульовано рекомендації щодо побудови ефективної системи реагування на комп’ютерні інциденти з урахуванням українського та міжнародного досвіду. Реалізація запропонованих підходів сприятиме зниженню ризиків для бізнесу, забезпеченню стійкості інформаційних систем та підвищенню рівня національної кібербезпеки в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Вінницька обласна військова адміністрація «Захист ваших ґаджетів від шкідливих програм» [Електронний ресурс] - https://www.vin.gov.ua/

2. Базалій, М. І. Інформаційна безпека: навчальний посібник. – К.: КНЕУ, 2020. – 342 с.

3. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.

4. ДСТУ ISO/IEC 27035-1:2021. Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 1.

5. Звіт CERT-UA: «Аналітика інцидентів у 2023 році» [Електронний ресурс] – Режим доступу: https://cert.gov.ua

6. Кіберполіція України: «Поради з кіберзахисту під час війни» [Електронний ресурс] – https://cyberpolice.gov.ua

7. Короткий, С. П. Кібербезпека: теорія і практика / С. П. Короткий. – Харків: ХНУРЕ, 2022. – 289 с.

8. Мельник, А. А. Інформаційна безпека в комп'ютерних системах. – К.: Ліра-К, 2021. – 256 с.

9. "МінфінМедіа". «Кібербезпека бізнесу під час війни» [Електронний ресурс]- https://www.project.minfin.com.ua/kiberbezpeka-biznesu-pid-chas-vijny

10. Національний координаційний центр кібербезпеки при РНБО. Офіційні рекомендації. – https://ncscc.gov.ua

11. Журило, О. і Ляшенко, О. (2024) «Архітектура та системи безпеки IoT на основі туманних обчислень» с. 54–66

12. NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide. – National Institute of Standards and Technology, 2012.

13. NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government. – NIST, 2021.

14. PCI Security Standards Council. Best Practices for Implementing a Security Awareness Program. – 2020.

15. Романенко, О. В. Організація захисту інформації в інформаційно-комунікаційних системах: навч. посіб. – Львів: Новий Світ, 2019. – 304 с.

16. Система кіберзахисту: концептуальні підходи і практика / за ред. І. К. Горбуліна. – К.: НІСД, 2020. – 400 с.

17. Сухонос, В. В. Основи кібербезпеки: навчальний посібник. – Суми: СумДУ, 2022. – 248 с.

18. Українська академія кібербезпеки. Освітні ресурси [Електронний ресурс] – https://uacs.org.ua

19. Шевченко, А. В. Безпека інформаційних систем: підручник. – К.: Наука і освіта, 2021. – 320 с.