ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ CROWDSTRIKE FALCON»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Тарас БІЛОХВОСТ

Виконав: здобувач(ка) вищої освіти групи БСДМ-62
БІЛОХВОСТ Тарас
(ПРІЗВИЩЕ, Ім'я)

Керівник: СОБЧУК Андрій
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК ПОСИЛАНЬ

ІС – інформаційна система

ІБ – інформаційна безпека

CIA – конфіденційність, цілісність, доступність

ПЗ – програмне забезпечення

SDN – Software-defined networking

SCADA – supervisory control and data acquisition

TLS – Transport Layer Security

ICE - Interactive Connectivity Establishment

UEM - Unified Endpoint Management

BYOD - Обмеження підключення пристроїв

AI - Штучний інтелект

ВСТУП

Актуальність дослідження. В умовах стрімкого розвитку інформаційних технологій та поширення кіберзагроз питання захисту кінцевих точок інформаційної системи набуває особливої актуальності для будь-якої організації. Адже саме кінцеві пристрої, такі як комп'ютери, ноутбуки, смартфони і планшети працівників компанії, є найбільш вразливою ланкою мережі з точки зору кібербезпеки. Згідно зі статистикою, у 2022 році майже 90% успішних кібератак було здійснено саме через кінцеві точки. Це пов'язано з тим, що сучасні загрози, такі як цільові атаки, шифрувальники і wiper-віруси, фокусуються в першу чергу на компрометації саме кінцевих пристроїв. Захист кінцевих точок набуває все більшої актуальності в умовах зростання кіберзагроз. Адже саме кінцеві пристрої, такі як комп'ютери, ноутбуки чи смартфони, є найбільш вразливим елементом корпоративної мережі. На жаль, традиційні мережеві системи захисту не здатні повною мірою забезпечити безпеку ендпойнтів. А користувачі часто припускаються помилок через недостатню обізнаність у питаннях кібербезпеки. Це створює сприятливі умови для атак з боку зловмисників. Особливі ризики несе тренд на віддалену та гібридну роботу. Адже працівники використовують різноманітні пристрої у різних локаціях, часто поза контролем IT-підрозділу. Це суттєво ускладнює задачу захисту корпоративних даних. Загрози ендпойнтам актуальні для компаній будь-якого маштабу. Навіть невеликі фірми можуть стати об'єктом для атак. А зловмисники активно використовують їх як плацдарм для подальшого проникнення до систем більших гравців ринку.

Наслідки від успішних атак на ендпойнти можуть коштувати компаніям мільйонів доларів. Адже дані уразливості призводять до витоку чутливої інформації, збоїв IT-інфраструктури, репутаційних втрат. Тож ефективний захист кінцевих точок - запорука успішного бізнесу в сучасних умовах.

Отже, недостатній рівень захисту кінцевих точок призводить до значних фінансових втрат, витоку конфіденційних даних, порушення бізнес-процесів

та репутаційних ризиків для компанії. Тому вивчення сучасних технологій захисту кінцевих пристроїв, а також розробка рекомендацій щодо побудови ефективної системи захисту endpoints є надзвичайно актуальним завданням.

Об'єкт дослідження – процес забезпечення захисту кінцевих точок в інформаційній системі організації.

Предмет дослідження – технології захисту кінцевих точок (endpoints) як засоби забезпечення інформаційної безпеки організації в умовах кіберзагроз.

Мета роботи – підвищення рівня захищеності інформаційної системи організації шляхом удосконалення технологій захисту кінцевих точок на основі дослідження існуючих загроз, аналізу сучасних рішень endpoint security та розробки практичних рекомендацій щодо їх впровадження з урахуванням потреб конкретної компанії.

Відповідно до поставленої мети дослідження були визначені наступні *наукові завдання*:

– дослідити підходи забезпечення захисту в інформаційній системі організації;

– визначити методи виявлення атак в комп'ютерних мережах;

– визначення вимог до захисту кінцевих пристроїв в організації;

– визначення принципів побудови системи захисту кінцевих точок;

– розробка практичних рекомендацій щодо впровадження системи захисту кінцевих точок.

Методи дослідження. Для комплексного вивчення проблеми захисту кінцевих точок інформаційної системи та розробки ефективних практичних рішень у дослідженні буде використано сукупність теоретичних і емпіричних методів.

Зокрема, застосування загальнонаукових методів аналізу, синтезу, абстрагування та моделювання дозволить проаналізувати предметну область захисту кінцевих точок, виявити існуючі загрози безпеці endpoints та тенденції їх розвитку. Використання методів класифікації й порівняння технологій забезпечить можливість оцінити їх потенціал, переваги та недоліки.

Застосування методів експертних оцінок і анкетування надасть необхідні емпіричні дані щодо ефективності наявних на ринку рішень endpoint security та дозволить врахувати думку фахівців з інформаційної безпеки. Використання статистичних методів обробки результатів анкетування забезпечить їх репрезентативність та наукову обґрунтованість. А застосування методу аналізу ієрархій дозволить визначити оптимальне рішення для захисту endpoints організації з урахуванням вимог та обмежень. Отже, використання комплексу сучасних методів дослідження дозволить отримати ґрунтовні та методологічно обґрунтовані результати в даній предметній області.

Практичне значення одержаних результатів в дослідженні результатів полягає в отриманні конкретних рекомендацій щодо побудови комплексної системи захисту кінцевих точок організації. На основі аналізу існуючих загроз, оцінки ефективності технологій та урахування потреб і обмежень конкретних компаній будуть надані чіткі практичні рекомендації щодо архітектури системи захисту endpoints, вимог до обраних технологій, послідовності етапів побудови захисту тощо. Крім того, значення матимуть конкретні рекомендації щодо параметрів налаштування системи, оптимального набору засобів захисту endpoints залежно від масштабу та специфіки бізнесу, заходів з підвищення обізнаності персоналу тощо. Такі результати дозволять IT-відділам підприємств розробити і реалізувати дієву стратегію захисту кінцевих точок і, як наслідок, істотно підвищити рівень інформаційної безпеки компанії в цілому та убезпечити її від фінансових втрат через кібератаки.

Апробація результатів кваліфікаційної роботи.

1 ТЕОРЕТИЧНІ ЗАСАДИ ДО ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ ОРГАНІЗАЦІЇ

1.1. Підходи до забезпечення захисту в інформаційній системі організації

Ефективний захист інформаційної системи є запорукою успішного функціонування та розвитку будь-якої організації в сучасних умовах. Адже інформація та IT-інфраструктура компанії постійно піддаються кіберзагрозам, наслідки реалізації яких можуть бути фатальними. Тому побудова надійної системи інформаційної безпеки на основі сучасних підходів є надзвичайно актуальним стратегічним завданням [1].

Інформаційна система (ІС) організації являє собою сукупність інформаційних, технічних та програмних засобів, а також персоналу, що забезпечує обробку даних з метою прийняття управлінських рішень. Захист ІС передбачає реалізацію відповідних організаційних, правових і технічних заходів для протидії кіберзагрозам та забезпечення конфіденційності, цілісності, доступності даних і безперервності бізнесу.

Система інформаційної безпеки компанії складається з трьох компонентів:

1. Технічний захист (засоби захисту інформації, антивіруси, міжмережеві екрани, VPN, системи виявлення вторгнень тощо).
2. Організаційний захист (політики ІБ, розподіл повноважень, навчання персоналу, аудит).
3. Фізичний захист (контроль доступу до приміщень, резервне живлення і т.д.).

Для реалізації єдиної політики ІБ та ефективного управління усіма складовими системи необхідна інтеграція цих компонентів в єдиний комплекс.

Існує декілька базових підходів до побудови комплексної системи інформаційної безпеки компанії:

1. Підхід, заснований на переліку загроз (threat-oriented). Система захисту будується як сукупність засобів протидії конкретним загрозам (віруси, DDoS, вторгнення тощо).

2. Підхід на основі оцінки ризиків (risk-based). Реалізуються заходи, що мінімізують ймовірні наслідки та збитки від інцидентів ІБ з урахуванням специфіки компанії.

3. Підхід, заснований на забезпеченні властивостей інформації (CIA – конфіденційність, цілісність, доступність).

4. Стандартизований підхід (ISO 27001, PCI DSS, NERC). Використовуються готові схеми та переліки вимог.

5. Ресурсно-орієнтований підхід (asset-oriented). Акцент робиться на захисті найбільш критичних інформаційних активів.

Кожен з цих підходів має свої переваги і недоліки в конкретних умовах. Найчастіше на практиці застосовується комбінований підхід, який об'єднує різні методики з метою комплексного захисту всіх інформаційних ресурсів компанії.

Існують такі основні моделі архітектури систем захисту інформації:

– Централізована модель. Передбачає зосередження засобів безпеки в єдиному центрі та управління ними з одного місця.

– Розподілена модель. Компоненти системи захисту розгорнуті на різних ділянках мережі чи сегментах ІС.

– Ієрархічна модель. Поєднує централізовані та локальні засоби, згруповані за рівнями управління.

– Модель багаторівневого (глибокого) захисту. Передбачає впровадження декількох різних рубежів безпеки по глибині мережі.

Вибір оптимальної моделі залежить від багатьох чинників: масштабу компанії, особливостей ІТ-інфраструктури, вимог бізнесу тощо. На практиці можуть комбінуватися кілька підходів [2, с.45].

Ефективна система ІБ має базуватися на таких основних принципах:

1. Комплексний, масштабований захист усіх інформаційних активів та мережевої інфраструктури.

2. Сегментація мережі за рівнями довіри, ідентифікація та аутентифікація користувачів і пристроїв.

3. Принцип найменших привілеїв, делегування прав доступу відповідно до ролей.

4. Глибока перевірка й логування трафіку, виявлення аномалій та реакція на інциденти.

5. Чітка регламентація заходів і процесів безпеки, узгодження з бізнес-процесами.

6. Розподіл зон відповідальності за ІБ між підрозділами і персоналом, налагодження процесів взаємодії.

Технічний захист інформації в системі організації передбачає: а) Захист від шкідливого програмного забезпечення (антивірус, IPS, антиспам, веб-фільтрація). б) Управління доступом до інформаційних ресурсів, перевірка прав доступу (фаєрволи, системи контролю доступу, DLP-системи). в) Контроль і реєстрація дій користувачів (системи аудиту та SIEM). г) Захист від вторгнень та DDoS-атак (HIPC, WAF, DoS-захист). ґ) Захист від витоку інформації технічними каналами (захист від ПЕМВН, TEMPEST). д) Забезпечення захищеного віддаленого доступу (VPN, RDP-захист). е) Резервне копіювання і відновлення даних. є) Криптографічний захист інформації та каналів зв'язку [2, с.35].

Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми – комп'ютерні злочини стали характерною ознакою сьогодення. Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є такі:

– швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;

– широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

– постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп'ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Серед основних статей варто виокремити такі:

– збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатність системи (мережі);

– вартість викрадених і скомпрометованих даних;

– витрати на відновлення роботи системи, на перевірку її цілісності, на доробку уразливих місць тощо [4, с.20-21].

Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників ІС та інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

Таким чином, побудова ефективної багатокомпонентної системи інформаційної безпеки є критично важливим завданням для сучасних організацій. Вона потребує застосування комплексного підходу з урахуванням усього спектру можливих загроз, ризиків та вразливостей на всіх рівнях ІТ-інфраструктури. Відповідно, подальші дослідження у цій сфері, розробка та

вдосконалення методів і засобів захисту інформації є вкрай актуальними і мають значний прикладний потенціал.

1.2. Дефініція понять подія, кіберінцидент, кібератака

У науковому контексті, для забезпечення точності та однозначності, важливо чітко визначити поняття «подія», «кіберінцидент» та «кібератака», особливо в контексті кібербезпеки та управління інформаційною безпекою.

Подія в контексті кібербезпеки визначається як будь-яка спостережувана зміна в стандартному операційному середовищі або стані інформаційної системи, яка може мати значення для безпеки. Це може включати як звичайні операції, так і виявлення потенційно підозрілих або ненормативних активностей. Не всі події вважаються шкідливими або небезпечними; деякі з них можуть бути частиною звичайної роботи системи.

В цілому події можна охарактеризувати як дії або сукупності обставин, що відбуваються в динамічному середовищі [1, 7]. У сфері інформаційної безпеки подія розглядається як будь-яка активність в кіберпросторі, що може впливати на роботу інформаційних систем компанії. Згідно з позицією Національної організації з питань стандартів та технологій США, подія (event) є будь-якою спостережуваною відмінністю в стані системи або мережі [4]. Інші науковці розглядають подію як будь-який ідентифікований випадок зміни стану системи, послуги чи процесу або порушення політики інформаційної безпеки або норм функціонування [5, 7]. Тобто подія є відхиленням від регламентного функціонування ІТ-системи та може вказувати на потенційну загрозу чи проблему. Не всі події є індикаторами безпекових проблем, але всі вони можуть бути підставою для подальшого аналізу.

Отже, поняття «подія» має широке тлумачення і може охоплювати як позитивні (заплановані зміни), так і негативні ситуації, що потенційно можуть свідчити про атаки, збої чи мати інші наслідки.

Кіберінцидент – це подія, яка фактично порушує або може порушити безпеку інформаційної системи та/або інформації, яка на ній обробляється. Це включає в себе порушення конфіденційності, цілісності або доступності інформації та може виявлятися у вигляді несанкціонованого доступу, зловмисного програмного забезпечення, фішингових атак, та інших форм кіберзловживань. Кіберінциденти вимагають негайного реагування для мінімізації їх впливу на організацію.

Поняття «інцидент» використовується в різних контекстах і загалом означає небажану, ненавмисну подію, що призводить до негативних наслідків [2, 8]. Кіберінцидент визначається як інцидент інформаційної безпеки, що призводить до негативного впливу на послуги інформаційної системи в умовах кіберпростору [6, 9]. Такі наслідки можуть полягати у порушенні конфіденційності, цілісності, доступності інформації чи IT-сервісів. Це може включати різні події, які фактично чи потенційно завдають шкоди системам, мережевим операціям або даним. Кіберінциденти можуть варіюватися від простих до складних, залежно від обсягу впливу та рівня складності порушення. Це може бути несанкціонований доступ до системи, розповсюдження шкідливих програм, атаки DoS (Denial of Service) та багато іншого.

В документах НАТО [5] кіберінцидент трактується як порушення безпеки чи аварія в кіберпросторі, що може бути як випадковим збоєм, так і атакою. Кіберінцидентом також вважається отримання несанкціонованого доступу до критично важливих інформаційних ресурсів. Тобто це широке поняття, що охоплює як несвідомі дії, так і атаки.

Отже, кіберінцидент є несприятливою подією, що спричиняє шкоду інформаційним ресурсам і системам в умовах кіберпростору часто внаслідок атаки.

Кібератака розглядається як цілеспрямоване використання засобів кіберпростору для впливу на критичну інформаційну інфраструктуру, процеси управління, державні ресурси або економіку країни з метою нанесення шкоди

[2]. На відміну від випадкових кіберінцидентів, кібератака є навмисними діями зі сторони зловмисників.

Група дослідників класифікує кібератаки за наступними ознаками [3]: за типом атакованих активів (дані, ПЗ, інфраструктура); за механізмами реалізації; за мотивами (фінансовий зиск, шпигунство, хактивізм тощо); за масштабом впливу; за природою атаки (цілеспрямована чи автоматична) тощо.

Подія в інформаційній системі → вказує на зміну стану системи або функціонування. Інцидент в кіберпросторі (кіберінцидент) → небажана подія з негативними наслідками, може бути як ненавмисною, так і умисною (атакою). Кібератака → цілеспрямоване шкідлива дія в кіберпросторі, навмисне нанесення збитків активам організації. Тобто, кібератака є різновидом кіберінциденту, а кіберінцидент є негативною подією в інформаційній системі, що може бути спричинена як атакою, так і випадковими факторами.

Таким чином, кібератака є умисним застосуванням зловмисного програмного забезпечення, методів соціальної інженерії або експлуатації вразливостей із метою порушення роботи інформаційних систем, крадіжки даних або завдання іншої шкоди організації чи державі.

Узагальнюючи наукові підходи, можна зробити висновок про складність і неоднозначність тлумачення базових понять у сфері кібербезпеки. У розділі запропоновано уточнене бачення дефініцій «подія», «кіберінцидент» і «кібератака» та показано їх співвідношення. Наведена модель дозволяє зрозуміти природу загроз та атак у кіберпросторі, що є підґрунтям для побудови ефективних систем захисту. Подальші дослідження у цій галузі дадуть змогу деталізувати та конкретизувати термінологічний апарат в сфері протидії кіберзагрозам.

1.3. Методи виявлення атак в комп’ютерних мережах

Кібератаки на комп'ютерні мережі є серйозною загрозою для інформаційної безпеки. Вони можуть призвести до порушення доступності, цілісності та конфіденційності інформації. Для захисту від кібератак важливо своєчасно виявляти їх. Виявлення атак в комп'ютерних мережах є складним завданням. Атака може бути здійснена різними методами, і її ознаки можуть бути приховані. Кібербезпека стає все більш актуальною проблемою в сучасному цифровому світі. Комп'ютерні мережі регулярно піддаються різним типам кібератак, включаючи атаки типу «відмова в обслуговуванні», фішинг, шкідливе програмне забезпечення та ін. [5, с.120]. Для захисту мереж від атак використовуються системи виявлення та запобігання вторгнень (IDS/IPS). Вони аналізують трафік та активність в мережах на предмет виявлення підозрілих і зловмисних дій. Ефективні IDS/IPS потребують досконалих методів виявлення атак.

Для виявлення атак використовують різні методи, які можна розділити на дві групи:

- Методи виявлення аномалій
- Методи виявлення зловживань

Методи виявлення аномалій ґрунтуються на тому, що атаки, як правило, призводять до відхилення від нормального функціонування мережі. Ці методи аналізу даних мережі з метою виявлення відхилень від нормального стану.

До методів виявлення аномалій відносяться:

- Аналіз трафіку
- Аналіз продуктивності
- Аналіз безпеки

Аналіз трафіку є одним з найпоширеніших методів виявлення аномалій. Він полягає в аналізі мережевого трафіку з метою виявлення відхилень від нормального стану.

Для аналізу трафіку використовують різні методи, такі як:

- Пошук шаблонів
- Аналіз розподілу даних
- Методи машинного навчання

Аналіз продуктивності полягає в аналізі продуктивності мережі з метою виявлення відхилень від нормального стану.

Для аналізу продуктивності використовують різні методи, такі як:

- Порівняння продуктивності з історичними даними
- Порівняння продуктивності з іншими мережами
- Використання порогових значень

Аналіз безпеки полягає в аналізі безпеки мережі з метою виявлення відхилень від нормального стану.

Для аналізу безпеки використовують різні методи, такі як:

- Пошук вразливостей
- Пошук шкідливого програмного забезпечення
- Пошук несанкціонованого доступу

Методи виявлення зловживань ґрунтуються на тому, що атаки, як правило, включають в себе певні дії, які не є нормальним функціонуванням мережі. Ці методи аналізу даних мережі з метою виявлення дій, які не є нормальним функціонуванням мережі.

До методів виявлення зловживань відносяться:

- Правила поведінки
- Симуляція
- Методи машинного навчання

Правила поведінки є набором правил, які визначають, які дії є допустимими в мережі. При виявленні дії, яка не відповідає жодному з правил, це може бути ознакою атаки. Симуляція полягає в тому, що створюється модель нормальної роботи мережі. При виявленні дії, яка не відповідає моделі, це може бути ознакою атаки.

Методи машинного навчання використовують для навчання моделі, яка може виявляти атаки. Модель навчається на наборі даних, який містить приклади нормального функціонування мережі та приклади атак.

Вибір методу виявлення атак залежить від багатьох факторів, таких як:

- Тип мережі
- Розмір мережі
- Види атак, від яких потрібно захищатися
- Фінансові можливості

Для невеликих мереж з невеликим обсягом трафіку можуть бути достатніми методи виявлення аномалій, засновані на аналізі трафіку. Для великих мереж з великим обсягом трафіку можуть бути потрібні методи виявлення зловживань, такі як правила поведінки або методи машинного навчання.

Існує кілька основних підходів до виявлення атак в комп'ютерних мережах [6, с.117-118]:

1. Виявлення вторгнень на основі сигнатур. Ці методи порівнюють діяльність в мережі з відомими сигнатурами/шаблонами атак. Сигнатури описують унікальні ознаки певної атаки. Перевага – здатність ідентифікувати відомі атаки з високою точністю. Недолік – неефективні проти нових, раніше невідомих атак.

2. Виявлення аномалій. Ці методи будують модель «нормальної» діяльності в мережі. Будь-яка активність, що значно відхиляється від цієї базової моделі, розглядається як аномалія/атака. Перевага – можливість виявлення нових типів атак. Недолік – можливі хибні спрацьовування внаслідок неповноти базової моделі.

3. Гібридні методи. Поєднують методи кількох типів, наприклад, виявлення аномалій + сигнатурний аналіз, для більш ефективного виявлення вторгнень.

Нижче наведено огляд деяких новітніх прикладів методів виявлення атак в комп'ютерних мережах.

- Гібридна модель на основі роїв частинок та глибокого навчання для виявлення вторгнень в мережах SDN [4]. Використовує переваги оптимізації роями частинок та можливостей глибокого навчання. Показала високу точність виявлення на тестових датасетах.
- Метод з використанням нейронних мереж для аналізу TLS трафіку з метою виявлення атак [5]. Модель навчена класифікувати TLS пакети на легітимні або зловмисні. Має швидкодію та точність на рівні 97%.
- Поєднання машинного навчання та аналізу графів для виявлення бот-мереж в системах SCADA [6]. Побудовано модель зв'язків між вузлами мережі та проаналізовано їх статистичні властивості для пошуку аномалій, що можуть свідчити про атаки.
- Агентно-орієнтовна модель на основі поведінкового аналізу користувачів для виявлення внутрішніх атак [7]. Модель будує профілі поведінки легітимних користувачів мережі та ідентифікує аномалії. Наприклад, нестандартна активність з облікового запису адміністратора.

Ефективне виявлення атак в комп'ютерних мережах потребує сучасних інтелектуальних методів аналізу. Найперспективнішим напрямком є гібридні та ансамблеві моделі, що поєднують кілька типів алгоритмів, таких як машинне навчання, аналіз графів, евристичні методи тощо. Майбутні дослідження повинні фокусуватись на розробці швидкодіючих, масштабованих та адаптивних моделей виявлення кібер-загроз.

Висновки до 1 розділу

Інформація та інформаційні ресурси є критично важливим активом для будь-якої сучасної організації. В умовах стрімкого розвитку інформаційно-комунікаційних технологій та постійного зростання кіберзагроз, питання захисту інформації набуває особливої актуальності.

Ефективна система захисту інформації в організації повинна ґрунтуватися на комплексному підході та охоплювати як технологічні, так і організаційно-правові аспекти. Ключовими складовими такої системи є:

1. Політики та процедури інформаційної безпеки. Встановлення чітких правил доступу до інформаційних активів, принципів обробки та передачі даних, вимог щодо аутентифікації та авторизації користувачів.

2. Організація служби інформаційної безпеки. Створення структурного підрозділу або визначення конкретних посадових осіб, відповідальних за питання захисту інформації.

3. Контроль доступу до інформації. Впровадження технічних засобів identifikacії та аутентифікації користувачів, надання персональних прав доступу згідно з посадовими обов'язками.

4. Захист периметру мережі. Використання міжмережевих екранів, систем виявлення та запобігання вторгненням, засобів криптографічного захисту каналів зв'язку.

5. Захист комп'ютерного обладнання та програмного забезпечення. Своєчасне оновлення ПЗ, встановлення антивірусних програм, шифрування даних, резервне копіювання.

6. Освіта та обізнаність користувачів щодо інформаційної безпеки. Проведення тренінгів для персоналу, формування культури безпеки в організації.

7. Аудит та контроль ефективності системи захисту інформації. Періодичний аналіз стану інформаційної безпеки, тестування на проникнення, оцінка ризиків та вразливостей.

Узагальнюючи, можна зазначити, що побудова комплексної системи захисту інформації в організації потребує поєднання організаційних та технічних заходів. Жоден окремо взятий засіб чи технологія не забезпечать належного рівня безпеки. Лише цілісний та системний підхід дозволить мінімізувати ризики порушення конфіденційності, цілісності та доступності інформації. Подальші дослідження в цій сфері повинні фокусуватися на

розробці адаптивних систем захисту з функціями машинного навчання для протидії новим типам кіберзагроз.

2 МЕТОДОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1. Вимоги до захисту кінцевих пристроїв в організації

Інформаційна безпека мереж є надзвичайно важливим аспектом в сучасному цифровому світі. Незалежно від того, йдеться про домашню чи корпоративну мережу, ризики кібератак існують завжди. Останнім часом ми неодноразово чули в новинах про витоки даних клієнтів через вторгнення зловмисників у мережі компаній. Тому забезпечення кібербезпеки мереж залишається пріоритетним завданням. При розробці систем захисту треба враховувати середовище мережі, потреби користувачів, а також наявні інструменти та технології. Потрібно не лише блокувати загрози, але й зберігати продуктивність та якість роботи мережі.

Існують зовнішні та внутрішні джерела кібератак. В наш час більшість загроз приходить з Інтернету. Поширеними зовнішніми атаками є віруси, шпигунське ПЗ, exploit'и нульового дня, DoS-атаки, крадіжки даних та особистої інформації користувачів. Схема зовнішніх та внутрішніх зазгроз пристроїв зображена на рисунку 2.1.

Ефективний захист включає використання спеціальних протоколів, пристроїв, програм та процедур. Такий підхід дозволяє запобігти проникненню зловмисників, швидко виявляти атаки та мінімізувати завдану ними шкоду. Регулярний аудит та оновлення засобів захисту також є важливою складовою, адже кіберзлочинці постійно вдосконалюють свої методи.

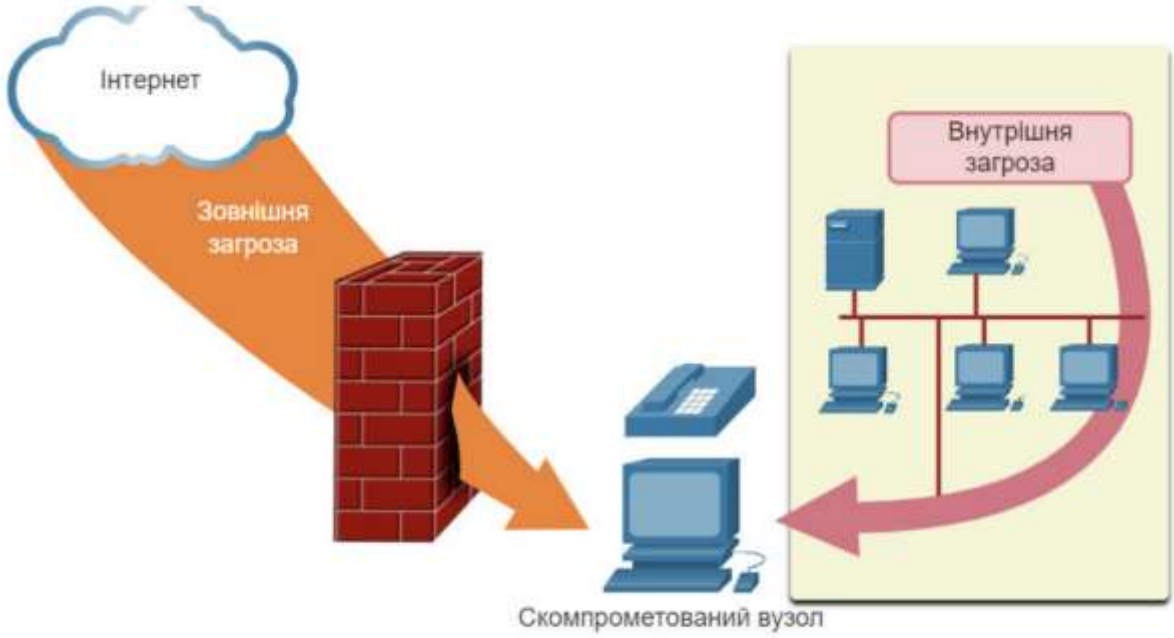

Рис.2.1. Схема зовнішніх та внутрішніх зазгроз пристроїв

Захист кінцевих пристроїв, таких як комп'ютери, ноутбуки, смартфони та планшети, є вкрай важливим для забезпечення кібербезпеки будь-якої організації. Адже ці пристрої містять чутливі дані та доступ до внутрішніх мереж і систем організації. Відповідно до дослідження компанії Varonis, більше 60% даних організації зберігаються на кінцевих пристроях [7]. Таким чином, належний захист цих пристроїв має критичне значення.

Безпека зв'язку між мобільними та віддаленими користувачами та корпоративною мережею є дуже важливою. Трафік сигналізації та медіа файлів завжди шифрується між мобільними пристроями та шлюзами доступу за допомогою протоколу ICE (Interactive Connectivity Establishment).

Однак для захисту внутрішніх з'єднань потрібні додаткові рішення. Зокрема, шифрування між шлюзами та внутрішніми серверами управління викликами, IP-телефонами чи іншим обладнанням вимагає гібридного режиму роботи або протоколу SIP OAuth.

Шлюзи Expressway компанії Cisco забезпечують безпечний прохід брандмауерів та підтримку роботи серверів управління викликами CM.

Сервери CM координують сесії як для мобільних, так і стаціонарних IP-телефонів.

Сигналізація проходить через Expressway між віддаленим користувачем та CM. Медіа-потоки передаються напряму між кінцевими точками. Весь трафік шифрується між шлюзом Expressway та мобільним пристроєм [8, с.50].

У наступній таблиці 2.1. наведено протоколи та пов 'язані служби, що використовуються в рішенні Unified CM.

Таблиця 2.1.

Протоколи та супутні послуги

Протокол	**Безпека**	**Служба**
SIP	TLS	Створення сесії: Реєстрація, запрошення тощо.
HTTPS	TLS	Вхід, Надання/Конфігурація, Каталог, Візуальна голосова пошта
Мультимедійний вміст	SRTP	ЗМІ: Аудіо, відео, спільний доступ до вмісту
XMPP	TLS	Миттєвий обмін повідомленнями, Присутність, Федерація

Виділені сервери дозволяють партнерам гнучко налаштовувати послуги для кінцевих користувачів завдяки повному контролю конфігурацій та параметрів безпеки. Проте партнери при цьому несуть повну відповідальність за належне налаштування захисту середовища клієнта. Це включає: 1) вибір безпечних чи незахищених протоколів (SIP/sSIP, HTTP/HTTPS тощо) та усвідомлення пов’язаних ризиків. 2) захист від реєстрації неавторизованих пристроїв. Якщо MAC-адреса не внесена в список дозволених, зловмисники можуть зареєструвати своє обладнання та здійснювати шахрайські дзвінки. 3) налаштування правил маршрутизації та перетворення викликів для запобігання шахрайству. 4) обмеження набору номерів для користувачів, щоб унеможливити здійснення несанкціонованих міжнародних дзвінків [8, с.51].

Основна вимога – обмеження доступу як фізичного, так і логічного. Це включає:

1. Фізичний контроль доступу за допомогою замків і ключів до приміщень, де зберігаються кінцеві пристрої [2].

2. Використання сильних паролів та двофакторної автентифікації. Паролі мають містити не менше 8 символів, великі та малі літери, цифри та спеціальні символи [3].

3. Встановлення привілеїв найнижчого рівня - користувачі та процеси повинні мати мінімально необхідні для роботи права [4].

4. Обмеження фізичного доступу до портів вводу/виводу пристроїв, таких як USB.

Шкідливе ПЗ, включаючи віруси, хробаки та троянські програми, може призвести до крадіжки даних, порушення роботи систем та інших серйозних наслідків. Тому ключовими вимогами є:

1. Встановлення та своєчасне оновлення антивірусних програм [5].

2. Регулярне сканування на наявність шкідливого ПЗ.

3. Фільтрація вмісту електронної пошти та веб-трафіку для запобігання фішинг атак.

4. Обмеження встановлення програм з неперевірених джерел.

5. Своєчасне оновлення всіх програм та операційних систем для усунення вразливостей.

Вимоги щодо запобігання несанкціонованого доступу до даних:

1. Шифрування носіїв даних за допомогою таких засобів, як BitLocker та VeraCrypt [6].

2. Регулярне резервне копіювання критичних даних [7].

3. Використання VPN та шифрування трафіку для захисту даних під час передачі [8].

4. Очищення або знищення носіїв перед утилізацією чи передачею пристрою іншому користувачеві.

Додаткові заходи контролю та управління кінцевими пристроями:

1. Інвентаризація всіх пристроїв, з'єднаних до мережі організації [9].

2. Централізоване розгортання операційних систем, прикладних програм та оновлень.

3. Моніторинг та контроль за допомогою систем класу UEM (Unified Endpoint Management) [10].

4. Обмеження підключення пристроїв (BYOD) з метою запобігання загрозам.

5. Періодичний аудит налаштувань безпеки та відповідність встановленим вимогам.

Ефективне впровадження перерахованих вище вимог забезпечить надійний захист кінцевих пристроїв та мінімізує ризики для безпеки інформації організації. Зважаючи на те, що зловмисники постійно розробляють нові методи атак, захист має регулярно перевірятися та оновлюватись. Крім того, обов'язковим є навчання персоналу правилам поводження з кінцевими пристроями та інформацією. Лише комплексний підхід дасть змогу максимально забезпечити кібербезпеку організації.

Отже, при розгортанні виділених серверів для кінцевих пристроїв партнери мають відповідально підходити до питань безпеки та налаштовувати належний рівень захисту від загроз. Це дозволить запобігти шахрайству, несанкціонованому доступу та іншим ризикам. Регулярний аудит і оновлення конфігурацій також є важливими складовими захисту.

2.2. Принципи побудови системи захисту кінцевих точок

Ієрархічний принцип побудови широко застосовується в організаційних та технічних системах, таких як підприємства, енергомережі, телекомунікації тощо. Він дозволяє розбити складну глобальну задачу на набір відносно незалежних підзадач та узгодити їх розв’язання. Розроблено типові структури багаторівневих систем, процедури координації локальних регуляторів та погодження реакцій підсистем для досягнення загальної мети. Побудовано методи аналізу та синтезу станів таких ієрархічних утворень.

Ієрархічність є загальною властивістю як штучних, так і природних систем. Її закономірності вивчає синергетика – наука про самоорганізацію та еволюцію систем. Згідно концепції самоорганізації, складні відкриті структури за певних умов можуть спонтанно утворюватися та вдосконалюватися шляхом обміну енергією і речовиною з зовнішнім середовищем.

Захист кінцевих точок мережі, таких як персональні комп'ютери, ноутбуки, смартфони та інші пристрої, є вкрай важливим елементом забезпечення кібербезпеки сучасних організацій. Адже саме на цих пристроях концентрується значна частина критичних даних та бізнес-процесів. Разом з тим, статистика свідчить, що більшість успішних кібератак розпочинається саме зі скомпрометування кінцевих точок і подальшого поширення на інші сегменти корпоративної мережі [9, с.230]. Отже, побудова ефективної системи захисту кінцевих точок є ключовим завданням інформаційної безпеки організації. В цій роботі розглянуто базові принципи, на яких має ґрунтуватися така система захисту для забезпечення комплексного захисту від сучасних кіберзагроз.

Принцип 1. Багаторівневий підхід Ефективний захист кінцевих точок має реалізовуватися на декількох рівнях [10, с.78]:

1. Попередження – на цьому рівні необхідно реалізувати заходи, спрямовані на запобігання можливості атаки. Це включає проактивні заходи на кшталт підвищення обізнаності користувачів, а також технічні рішення у вигляді мережевих екранів, систем виявлення вторгнень та запобігання вторгненням.

2. Виявлення – якщо атаці все ж таки вдалося проникнути на кінцеву точку, на цьому рівні активуються механізми виявлення факту компрометації. Сюди належать антивірусні та антишпигунські системи, сканери вразливостей, моніторинг цілісності файлів та інші засоби виявлення аномалій та шкідливої активності.

3. Реагування – якщо було виявлено атаку чи підозрілу поведінку, спрацьовують механізми оперативного реагування з метою мінімізації

завданих збитків. На цьому етапі можуть блокуватися шкідливі процеси та з’єднання, відновлюватися пошкоджені файли з резервних копій, а також відправлятися сповіщення адміністратору про інцидент. Такий підхід забезпечує комплексний захист та знижує ризики у разі, якщо один з рівнів не спрацював належним чином.

Принцип 2. Централізоване управління Для великих мереж, що складаються з сотень та тисяч кінцевих точок, ключовою вимогою є забезпечення централізованого управління системою їх захисту. Це дає такі переваги:

1. Можливість швидкого розгортання захисних агентів та політик на всіх пристроях в мережі.

2. Автоматичне оновлення правил та сигнатур безпеки відповідно до нових загроз.

3. Централізований збір та кореляція подій безпеки з усіх кінцевих точок для швидкого реагування та розслідування інцидентів.

4. Можливість дистанційного адміністрування, моніторингу стану та контролю дотримання політик. Такий функціонал забезпечують системи класу UEM (Unified Endpoint Management), що дозволяють централізовано керувати захистом, конфігурацією та оновлення програмного забезпечення на кінцевих пристроях в корпоративній мережі [10].

Принцип 3. Сегментація мережі З метою обмеження можливостей зловмисника у разі компрометації окремої кінцевої точки доцільно реалізовувати сегментацію корпоративної мережі на окремі зони. Кожна зона має містити пристрої та сервіси зі схожим рівнем критичності та вимогами доступу. Між зонами необхідно реалізувати ретельний контроль трафіку за допомогою міжмережевих екранів за принципом «за замовчуванням заборонено» - дозволяється лише необхідний мінімум зв’язків [6]. Це дозволяє суттєво ускладнити можливості зловмисника по горизонталі поширитися по сегментам мережі та досягти найбільш цінних цілей – серверів баз даних, систем управління та технологічних мереж. Такий підхід має реалізовуватися

спільно із сучасними концепціями Zero Trust та мікросегментації для максимального звуження периметру довіри та зон руху зловмисника всередині мережі [12, с.495].

Принцип 4. Контроль пристроїв Кінцеві точки також потребують ефективного контролю як з боку користувачів, так і IT-персоналу. З цією метою необхідно реалізовувати такі процеси:

1. Інвентаризація – облік та класифікація всіх кінцевих пристроїв в мережі для розуміння стану та ступеню захищеності [11].

2. Аудит безпеки – періодична перевірка наявних вразливостей, стану антивірусного захисту та дотримання вимог політик для своєчасного виявлення прогалин.

3. Оновлення та патчінг – своєчасна установка оновлень програмного забезпечення для усунення уразливостей (особливо критичних).

4. Моніторинг – збір та аналіз даних про активність користувачів та процесів на кінцевих точках для виявлення аномалій поведінки.

5. Резервне копіювання – створення резервних копій критичних даних користувачів для можливості відновлення у разі шифрування чи пошкодження.

6. Знищення даних – гарантоване видалення конфіденційної інформації при виведенні пристрою з експлуатації. Такий підхід дозволяє не лише запобігти атакам, але й мінімізувати наслідки у разі їх виникнення за рахунок своєчасного реагування та відновлення даних.

У результаті такого процесу складна динамічна система може розділитися на два взаємопов’язані рівні – силовий та інформаційно-керуючий. Другий впливає на перший слабкими сигналами, але суттєво змінює його поведінку. Така архітектура є енергетично ефективнішою порівняно з однорідною.

Проте залишається відкритим питання впливу ієрархічності системи на вимоги до її кібербезпеки. Ця проблема потребує подальших досліджень.

2.3. Вибір та обґрунтування технології захисту

Існує декілька основних методів забезпечення конфіденційності даних. Перший – це обмеження доступу шляхом розмежування прав користувачів, процесів і пристроїв. Другий – шифрування, тобто перетворення інформації у вигляд, незрозумілий без спеціального ключа. Також можливе приховування факту існування даних методами стеганографії. І нарешті, подрібнення – розподіл інформації на частини так, щоб для розуміння потрібна була вся сукупність. Ще одним аспектом є цілісність – відсутність несанкціонованих змін чи вилучень. Її часто забезпечують тими ж методами, що й конфіденційність, а також резервуванням та перевіркою хешів. Не менш важливою є доступність інформації, тобто можливість своєчасно отримати до неї доступ. Типові загрози тут – збої обладнання та DDoS-атаки [13].

Пов'язаними властивостями є автентичність (достовірна ідентифікація джерела) та неспростовність (неможливість відмовитися від авторства). Їх часто забезпечують електронним підписом.

Отже, для комплексного захисту потрібен системний підхід з урахуванням усіх загроз і вразливостей. Це вимагає реалізації таких заходів, як шифрування, контроль доступу, резервне копіювання, фільтрація трафіку, антивірусний захист тощо. Координоване поєднання різних методів дозволить мінімізувати ризики порушення безпеки даних.

Для досягнення названих цілей система ІБ повинна бути спроможною виконувати наступні завдання:

– забезпечення захищеного зберігання інформації на різних носіях;

– захист даних, що передаються по каналах зв'язку;

– розмежування доступу до різних видів документів;

– створення резервних копій, післяаварійне відновлення інформаційних систем.

Забезпечення інформаційної безпеки підприємства можливо тільки при системному і комплексному підході до захисту. В системі ІБ повинні враховуватися всі актуальні комп'ютерні загрози та вразливості.

Інформаційна безпека є критично важливим аспектом для сучасних промислових підприємств. Адже в їх діяльності задіяні численні інформаційні системи та технологічні мережі, які містять великі масиви цінних даних та забезпечують безперервність виробничих процесів. Разом з тим, цифровізація та зростаюча інтеграція корпоративних та технологічних мереж створює нові можливості для кібератак, що загрожують як конфіденційності даних, так і безпеці персоналу та навколишнього середовища [14, p. 328-329].

Загрози інформаційній безпеці – це можливі дії або події, які можуть вести до порушень ІБ. Вони також є кінцевими цілями (або результатами) діяльності її порушників.

Рис.2.2. Загрози інформаційній безпеці промислових підприємств

Ефективний захист інформації на підприємствах вимагає цілодобового моніторингу та контролю подій безпеки в режимі реального часу. Адже загрози можуть виникати на будь-якому етапі життєвого циклу даних – від створення чи отримання до знищення чи втрати актуальності. Відповідальність за інформаційну безпеку зазвичай покладається на ІТ-підрозділи, служби економічної безпеки та захисту інформації. Проте рівень захищеності постійно

змінюється під впливом багатьох факторів. Наприклад, розширення співпраці та автоматизації бізнес-процесів, зростання обсягів даних та кіберзлочинності. Для адекватного захисту потрібне поєднання організаційних та технічних заходів. Перші включають політики та правила роботи з даними і IT-системами. Другі – впровадження засобів контролю доступу, моніторингу, антивірусного захисту тощо. Вибір технічних засобів має базуватися на принципах і стандартах інформаційної безпеки з урахуванням інтеграції в наявне середовище. Також важливо уніфікувати механізми управління різними підсистемами захисту.

Рис. 2.2. Методичний підхід до формування системи ІБ промислових підприємств

Ефективна система управління інформаційною безпекою підприємства має будуватися за ієрархічним принципом та охоплювати всі рівні управління. На стратегічному рівні керівництво формує загальні принципи та визначає необхідний рівень захищеності з урахуванням бізнес-цілей компанії. Наступний рівень – це відповідальність IT-підрозділу. Він полягає у деталізації вимог безпеки, виявленні конкретних загроз, оцінці факторів ризику та розробці заходів протидії. Сюди входить планування технічних і організаційних заходів, які потім узгоджуються з керівництвом.

Наступний критично важливий крок – впровадження розробленого плану в діяльність компанії. Адже система безпеки потребуватиме змін в бізнес-процесах, регламентах та межах відповідальності працівників. Можуть знадобитися нові бізнес-процеси суто для підтримки функціонування захисту. Все це вимагає залучення та підтримки керівництва на цьому етапі. І нарешті, важливими складовими є навчання та тренування персоналу з питань інформаційної безпеки. Адже людський фактор часто є найслабкішою ланкою у будь-якій системі захисту [15].

Отже, впровадження безпеки як невід'ємної частини бізнес-процесів на всіх рівнях та залучення до цього процесу як топ-менеджерів, так і рядових працівників є запорукою побудови надійної системи захисту інформації сучасного підприємства.

Таким чином, проведене дослідження особливостей формування та розвитку системи забезпечення інформаційної безпеки промислових підприємств дає підстави зробити такі висновки:

1. Створення системи інформаційної безпеки на промислових підприємствах є комплексним управлінським завданням, що потребує системного та інтегрованого підходу. Для успішної реалізації ефективної системи інформаційної безпеки необхідна відповідна методична база.

2. У роботі запропоновано новий методичний підхід до формування системи інформаційної безпеки промислових підприємств. Він включає основні принципи, цілі та завдання, аналіз загроз та факторів впливу, а також комплекс заходів з її реалізації. Головна особливість підходу – структурування складових по чотирьох рівнях управління та визначення відповідальних осіб.

3. У роботі деталізовано основні елементи запропонованого підходу, описана специфіка його запровадження та використання на промислових підприємствах.

Обґрунтування вибору технології захисту інформації на підприємстві є важливим та комплексним завданням, яке потребує системного підходу з урахуванням специфіки галузі, особливостей технологічних процесів,

структури інформаційних потоків, нормативно-правової бази та інших чинників. Першочерговим кроком має стати детальний аналіз існуючих загроз, вразливостей та можливих каналів витоку чи втрати даних з використанням методів ризик-аналізу. Його результати дозволять визначити найбільш уразливі ділянки інформаційної інфраструктури, оцінити ймовірність реалізації потенційних загроз та можливі наслідки. Наступним кроком постає формування вимог до системи захисту з точки зору забезпечення конфіденційності, цілісності, доступності даних та автентичності користувачів відповідно до політики інформаційної безпеки організації. Важливе значення має врахування галузевих стандартів, національного законодавства, міжнародних норм та рекомендацій.

На основі сформованих вимог проводиться аудит наявних засобів захисту, визначаються прогалини та недоліки, які потребують усунення. Аналізують можливості модернізації чи масштабування вже розгорнутих рішень з точки зору ефективності та вартості [16, p.49]. Паралельно досліджується ринок спеціалізованих засобів захисту з визначенням оптимальної для потреб підприємства технології чи їх поєднання. Серед ключових критеріїв відбору: можливості протидії конкретним загрозам; особливості впровадження та експлуатації; сумісність з наявними технічними та програмними рішеннями; вартість володіння.

Для систематизації отриманих результатів доцільно скласти порівняльні таблиці та провести багатокритеріальну оцінку альтернатив з розрахунком інтегрального показника. Зазвичай розглядають декілька варіантів комбінації різних технологій для забезпечення комплексного захисту периметру, мережі, серверів, робочих станцій, програм та даних.

Серед технологій міжмережевого екранування найбільш ефективними вважаються новітні системи виявлення та запобігання вторгнень на основі аналізу поведінки та машинного навчання, що дозволяють в режимі реального часу розпізнавати цільові атаки з подальшою активацією комплексу заходів протидії. Додатково застосовуються засоби аналізу вразливостей, що

виявляють прогалини кіберзахисту та загрози в роботі мережевого обладнання й сервісів.

Криптографічний захист рекомендовано реалізовувати на всіх рівнях – від шифрування каналів зв'язку на мережевому рівні до перетворення окремих файлів чи носіїв інформації. З урахуванням специфіки оброблюваних даних потрібно обирати відповідний криптографічний алгоритм та довжину ключа. Для автентифікації користувачів та пристроїв застосовують цифрові сертифікати, електронні підписи, OTP-токени тощо.

Централізоване управління доступом на рівні мережі реалізується за допомогою контролерів домену, систем авторизації на основі ролей, LDAP та протоколів аутентифікації. Для розмежування прав на рівні окремих ОС та СКБД використовують вбудовані засоби безпеки та спеціалізовані рішення для централізованого управління обліковими записами, груповими політиками, аудитом подій тощо [17, p.6-7].

Захист від шкідливого коду передбачає впровадження комплексних систем антивірусного захисту терміналів і серверів, сканування вмісту електронної пошти, веб-трафіку та файлів на наявність вірусів, троянів, хробаків тощо. Доцільно обрати рішення з можливістю централізованої інсталяції та оновлення, формування звітів, віддаленого адміністрування та реагування на інциденти.

Захищеність резервних копій досягається шляхом їх реплікації, постійного сканування на наявність шкідливого коду та дотримання правил зберігання, в тому числі з використанням хмарних сховищ. Рекомендовано реалізувати багаторівневу модель з кількома поколіннями копій та з різними місцями зберігання для мінімізації ризиків.

При проектуванні комплексної системи захисту інформації особливу увагу приділяють забезпеченню синергетичного ефекту, коли поєднання різних технологій дозволяє досягти мультиплікативного посилення безпеки. Крім цього, обираючи конкретні технічні та програмні рішення, перевагу

віддають уніфікованим платформам, що дають можливість інтегрованого централізованого управління та моніторингу.

Високий рівень технологічної готовності сучасних засобів захисту в комбінації з виваженим методологічним підходом до їх обрання та розгортання дозволяє ефективно протидіяти кіберзагрозам та мінімізувати ризики для інформаційних активів підприємства. Формування надійної системи захисту інформації потребує постійного моніторингу, аналізу та удосконалення з можливістю оперативної модернізації в відповідності до динамічних викликів кіберпростору.

Подальші дослідження доцільно присвятити адаптації розробленого методичного підходу до потреб підприємств різних галузей промисловості.

Висновки до 2 розділу

Отже, на основі проведеного дослідження можна зробити висновок, що розробка комплексної методології захисту кінцевих точок інформаційної системи організації є вкрай важливим завданням в сучасних умовах. Адже саме кінцеві точки, такі як комп'ютери, ноутбуки, смартфони та інші пристрої співробітників часто стають об'єктом кібератак.

Запропоновано комплексний підхід до захисту кінцевих точок, що включає як технічні рішення (антивірусне програмне забезпечення, міжмережеві екрани, системи виявлення вторгнень, засоби криптографічного захисту інформації), так і організаційні заходи (регулярне навчання персоналу з питань кібербезпеки, розробка та впровадження відповідних політик і процедур).

Особливу увагу приділено посиленню захисту від цільових атак, які в даний час становлять найбільшу загрозу через складність їх своєчасного виявлення та запобігання. Запропонована методологія дозволить мінімізувати ризики кібератак на кінцеві точки та підвищити рівень захищеності інформаційних систем в цілому.

Вважаємо, що удосконалення та пристосування розробленого методичного підходу до особливостей функціонування промислових підприємств конкурентних галузей національного господарства є перспективним напрямом подальших досліджень.

3 РОЗРОБКА ПРАКТИЧНИХ РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

3.1. Архітектура системи захисту кінцевих точок організації

Сьогодні кібербезпека є критично важливою для будь-якої організації. Кінцеві точки, такі як комп'ютери, ноутбуки, смартфони та інші пристрої, є найбільш уразливими ланками в інфраструктурі організацій. Тому вкрай необхідно розгорнути надійну систему захисту кінцевих точок для запобігання кібератакам.

Архітектура системи захисту кінцевих точок Ефективна система захисту повинна включати такі компоненти:

1. Антивірусне та антишпигунське програмне забезпечення для захисту від шкідливого коду – вірусів, троянів, spyware тощо [18, p.60].
2. Міжмережевий екран для фільтрації мережевого трафіку та блокування загроз.
3. Система запобігання вторгнень для виявлення та блокування підозрілих мережевих атак.
4. Захист від веб-загроз для блокування шкідливих веб-сайтів і завантажень.
5. Управління кінцевими точками для централізованого розгортання політик безпеки.

Для посилення захисту ця архітектура також може доповнюватися такими компонентами [19]:

1. Система аналізу та збору логів з метою виявлення загроз та інцидентів.
2. Захист додатків для контролю поведінки окремих програм.
3. Шифрування даних для захисту конфіденційної інформації.
4. Система обмеження привілеїв користувачів для зменшення наслідків атак.

Така комплексна система захисту кінцевих точок дозволить забезпечити належний рівень кібербезпеки в організації та захиститися від більшості кіберзагроз.

Управління ризиками є критично важливим елементом розробки надійної архітектури корпоративних систем. Воно включає процеси ідентифікації потенційних загроз, оцінки їх ймовірності та впливу, а також розробки стратегій пом'якшення цих ризиків. Ефективна програма управління ризиками дозволяє організаціям балансувати потреби в інноваціях з вимогами кібербезпеки під час проектування архітектури корпоративних систем.

Дотримання визнаних стандартів, таких як NIST Cybersecurity Framework [20, p.30], допомагає забезпечити, що рішення в галузі архітектури відповідають як бізнес-потребам, так і нормативним вимогам щодо управління ризиками. Однак ландшафт загроз постійно змінюється, тому регулярні оцінки ризиків є важливим інструментом для виявлення прогалин у заходах безпеки.

Штучний інтелект (AI) [21, 22] відкриває нові можливості для трансформації підходів до забезпечення кібербезпеки. AI може автоматизувати рутинні завдання, покращити можливості прогнозної аналітики, швидше ідентифікувати аномалії та підвищити ефективність заходів захисту. Впровадження інструментів кібербезпеки на основі AI в архітектуру корпоративних систем є стратегічно важливим рішенням для посилення стійкості до загроз.

Дотримання нормативних вимог, таких як GDPR, CCPA, HIPAA, є ключовим аспектом проєктування архітектури підприємства. Інтеграція цих стандартів безпосередньо в архітектуру дозволяє компаніям перетворити дотримання нормативних вимог з обтяжливого обов'язку на конкурентну перевагу. Системи моніторингу відповідності гарантують дотримання стандартів в реальному часі.

На рисунку 3.1. зображена розширена архітектура від SASE і повний захист від кінцевої точки до хмари:

Рис.3.1. Розширена архітектура SASE і повний захист від кінцевої точки до хмари

Вивчення кейсів успішних IT-компаній дозволяє отримати практичні стратегії та уроки для розбудови ефективних програм управління ризиками та кібербезпеки в рамках архітектури корпоративних систем. Цільові інвестиції в інструменти управління ризиками та безпекою на основі передового досвіду дозволяють мінімізувати загрози та максимізувати повернення від впровадження нових технологій.

Кінцеві точки, такі як комп'ютери, ноутбуки, планшети та смартфони, є важливими активами для будь-якої організації. Вони використовуються для зберігання та обробки конфіденційної інформації, а також для доступу до критичних систем та мереж. Тому забезпечення їх захисту є критично важливим для захисту організації від кібератак.

Архітектура системи захисту кінцевих точок організації повинна бути розроблена з урахуванням наступних принципів:

– Захист від відомих та невідомих загроз. Система захисту повинна бути здатна виявляти та блокувати як відомі, так і невідомі загрози.

– Контроль доступу. Система повинна забезпечувати контроль доступу до кінцевих точок, щоб запобігти несанкціонованому доступу.

– Підтримка віддаленої роботи. Система повинна підтримувати віддалену роботу, щоб забезпечити захист кінцевих точок, які знаходяться поза офісом [23].

Основні компоненти архітектури системи захисту кінцевих точок організації:

– Адміністративне управління. Цей компонент відповідає за управління та конфігурацію системи захисту.

– Захист від вірусів та шкідливого програмного забезпечення. Цей компонент відповідає за виявлення та блокування вірусів, шкідливого програмного забезпечення та інших загроз.

– Контроль доступу. Цей компонент відповідає за контроль доступу до кінцевих точок.

– Захист від несанкціонованого доступу. Цей компонент відповідає за запобігання несанкціонованому доступу до кінцевих точок.

– Звітність та моніторинг. Цей компонент відповідає за звітування про стан системи захисту та моніторинг її ефективності.

Архітектура нульової довіри є одним із сучасних підходів до захисту кінцевих точок організації. У цій архітектурі кожна кінцева точка розглядається як потенційний джерело загрози, і до неї застосовується контроль доступу. Кінцева точка може отримати доступ до ресурсів лише після успішної аутентифікації та авторизації.

Отже, ми вирішили впровадити систему захисту кінцевих точок на базі рішення CrowdStrike Falcon. Це хмарне рішення забезпечує повний спектр можливостей щодо запобігання, виявлення та реагування на кіберзагрози.

3.2. Поетапний план впровадження обраної технології

CrowdStrike Falcon – це хмарна платформа для захисту кінцевих точок, яка пропонує широкий спектр можливостей для захисту від кібератак. Вона є одним з найпопулярніших рішень для захисту кінцевих точок у світі.

Розгортання системи CrowdStrike Falcon для захисту кінцевих точок є комплексним завданням, яке вимагає ретельного планування та поетапної реалізації. Для успішного впровадження ми пропонуємо дотримуватися таких кроків [24, 25]:

1. Аналіз поточного стану IT-інфраструктури організації. Необхідно зібрати точні дані про кількість та типи кінцевих пристроїв (персональні комп'ютери, ноутбуки, сервери), їх географічне розташування, підключення до мережі, встановлене програмне забезпечення. Це дозволить правильно спланувати розгортання Falcon.

2. Вибір режиму розгортання агентів Falcon. Можливі кілька варіантів, зокрема встановлення пакетів агентів вручну, централізована віддалена установка чи використання систем управління пристроями (Intune, SCCM). Необхідно вибрати оптимальний для конкретного IT-середовища організації.

3. Тестування роботи агентів на репрезентативній вибірці пристроїв перед масштабним розгортанням. Дозволить виявити та усунути потенційні проблеми.

4. Поетапне розгортання агента Falcon на всіх кінцевих точках згідно складеного плану. Рекомендується починати з найбільш критичних підрозділів компанії.

5. Конфігурація політик безпеки відповідно до потреб бізнесу, вимог регуляторів та кращих практик кібербезпеки. Зокрема, налаштування правил виявлення загроз, карантину, автоматичного блокування шкідливої активності на кінцевих точках.

6. Забезпечення цілодобового моніторинг та реагування на події безпеки з боку відповідних фахівців SOC. Інтеграція з процесами управління інцидентами.

Така поетапність дозволить мінімізувати ризики та ефективно реалізувати можливості системи CrowdStrike Falcon для захисту всієї IT-інфраструктури підприємства.

Для успішного впровадження CrowdStrike Falcon [26] необхідно розглянути такі ключові аспекти:

– Планування. Першим кроком є розробка плану впровадження, який визначатиме такі аспекти, як: 1) мета впровадження; 2) терміни впровадження; 3) бюджет; 4) кваліфікація персоналу.

– Підготовка. Після розробки плану впровадження необхідно підготувати організацію до впровадження, що включає такі кроки, як: 1) оцінка існуючої інфраструктури; 2) ознайомлення персоналу з CrowdStrike Falcon; 4) налаштування CrowdStrike Falcon.

– Впровадження. Впровадження CrowdStrike Falcon включає такі кроки, як: 1) розгортання агентів CrowdStrike Falcon на кінцевих точках; 2) налаштування правил та політики безпеки; 3) тестування системи.

– Підтримка. Після впровадження CrowdStrike Falcon необхідно забезпечити її підтримку, що включає такі кроки, як: 1) моніторинг системи; 2) оновлення програмного забезпечення; 3) реагування на інциденти.

Планування впровадження CrowdStrike Falcon є важливим кроком, який допоможе забезпечити успішне впровадження системи. План повинен визначати такі аспекти:

– Мета впровадження. Чому організація впроваджує CrowdStrike Falcon? Які цілі вона хоче досягти?

– Терміни впровадження. Коли організація хоче завершити впровадження?

– Бюджет. Скільки коштів організація готова витратити на впровадження?

– Кваліфікація персоналу. Який рівень кваліфікації необхідний персоналу для управління та використання CrowdStrike Falcon?

План впровадження повинен бути розроблений у співпраці з командою CrowdStrike. Команда CrowdStrike може надати допомогу в оцінці існуючої інфраструктури організації, розробці правил та політики безпеки, а також навчанні персоналу.

Підготовка організації до впровадження CrowdStrike Falcon включає такі кроки:

– Оцінка існуючої інфраструктури. Команда CrowdStrike повинна оцінити існуючу інфраструктуру організації, щоб визначити, чи відповідає вона вимогам CrowdStrike Falcon.

– Ознайомлення персоналу з CrowdStrike Falcon. Персонал, який буде використовувати CrowdStrike Falcon, повинен бути ознайомлений з її функціоналом та принципами роботи.

– Налаштування CrowdStrike Falcon. Команда CrowdStrike повинна налаштувати CrowdStrike Falcon відповідно до вимог організації.

– Впровадження CrowdStrike Falcon включає такі кроки:

– Розгортання агентів CrowdStrike Falcon на кінцевих точках. Агент CrowdStrike Falcon є програмним забезпеченням, яке інсталює та запускається на кінцевих точках. Він збирає дані про кінцеві точки та передає їх до хмарної платформи CrowdStrike Falcon.

– Налаштування правил та політики безпеки. Команда CrowdStrike повинна налаштувати правила та політику безпеки CrowdStrike Falcon відповідно до вимог організації.

– Тестування системи. Після розгортання агентів CrowdStrike Falcon та налаштування правил та політики безпеки необхідно протестувати систему, щоб переконатися в її правильному функціонуванні.

Після впровадження CrowdStrike Falcon необхідно забезпечити її підтримку, що включає такі кроки:

– Мониторинг системи. Команда CrowdStrike повинна регулярно моніторити систему, щоб виявляти потенційні загрози.

– Оновлення програмного забезпечення. CrowdStrike Falcon регулярно випускає оновлення програмного забезпечення, які містять виправлення для відомих уразливостей. Організація повинна своєчасно встановлювати оновлення програмного забезпечення.

– Реагування на інциденти. Якщо система CrowdStrike Falcon виявить потенційну загрозу, необхідно негайно вжити заходів реагування.

Команда CrowdStrike може надати допомогу в підтримці CrowdStrike Falcon, включаючи моніторинг системи, оновлення програмного забезпечення та реагування на інциденти.

Основні етапи впровадження:

1. Встановлення агентів CrowdStrike на всіх кінцевих пристроях. Агенти збирають телеметрію про активність на пристроях і надсилають її до хмарної платформи.

2. Встановлення хмарної консолі управління CrowdStrike. Вона надає централізований контроль та візуалізацію стану безпеки всіх кінцевих точок.

3. Встановлення політик безпеки та налаштування системи виявлення загроз. CrowdStrike постійно аналізує поведінку на кінцевих точках та виявляє підозрілу активність.

4. Інтеграція з наявними рішеннями кібербезпеки, такими як брандмауери, системи антивірусного захисту тощо. Це дозволить отримати загальну картину стану IT-інфраструктури.

5. Забезпечення безперервної підтримки та адміністрування. Регулярне оновлення агентів CrowdStrike, моніторинг подій безпеки, реагування на інциденти.

6. Проведення навчань для IT та керівного персоналу з питань використання та адміністрування системи CrowdStrike, процедур реагування на інциденти кібербезпеки.

Для поглибленого аналізу особливостей впровадження системи CrowdStrike Falcon пропонуємо розглянути такі ключові аспекти в таблиці 3.1.:

Таблиця 3.1.

Основні аспекти впровадження CrowdStrike Falcon

Аспект	Опис
Технічні вимоги	Підтримується встановлення на пристроях з Windows, macOS, Linux, а також мобільних ОС Android, iOS. Вимагає наявності з'єднання з інтернетом. Споживає мінімальні ресурси пристрою.
Інтеграція	Можлива інтеграція з більшістю поширених корпоративних додатків через офіційний API. Також реалізована інтеграція з рішеннями класу SIEM, SOAR, іншими системами захисту інформації.
Розгортання	Можливість гнучкого централізованого та віддаленого розгортання агентів Falcon на пристроях, що спрощує процес масштабування захисту.
Адміністрування	Вбудована зручна хмарна консоль керування. Можливості групування пристроїв, управління політиками та правилами для груп, користувачів.
Звітність	Гнучка система звітності з широкими можливостями візуалізації. Зручне збереження та експорт звітів. Реалізовано Above-grid звітність для керівництва.

Отже, CrowdStrike Falcon добре масштабується, може бути інтегрований у різноманітні IT-середовища, не вимагає значних ресурсів і забезпечує зручне централізоване адміністрування. Це оптимальний вибір для реалізації сучасної системи захисту кінцевих точок.

Запропонований підхід дозволить комплексно покращити захист кінцевих точок нашої організації на основі сучасних рішень класу EDR. Ми зможемо оперативно виявляти та блокувати кібератаки, мінімізувати можливі наслідки суттєвих інцидентів.

3.3. Оцінка ефективності запропонованих заходів

Запропоновані заходи щодо впровадження CrowdStrike Falcon є ефективними для забезпечення захисту кінцевих точок організації.

Планування впровадження CrowdStrike Falcon є важливим кроком, який допоможе забезпечити успішне впровадження системи. План повинен визначати такі аспекти:

- Мета впровадження. Мета впровадження CrowdStrike Falcon - це захист кінцевих точок організації від кібератак.
- Терміни впровадження. Терміни впровадження повинні бути визначені з урахуванням потреб організації.
- Бюджет. Бюджет на впровадження CrowdStrike Falcon повинен бути визначений на основі потреб організації.
- Кваліфікація персоналу. Персонал, який буде використовувати CrowdStrike Falcon, повинен бути кваліфікованим для управління та використання системи.

План впровадження повинен бути розроблений у співпраці з командою CrowdStrike. Команда CrowdStrike може надати допомогу в оцінці існуючої інфраструктури організації, розробці правил та політики безпеки, а також навчанні персоналу.

Підготовка організації до впровадження CrowdStrike Falcon включає такі кроки:

- Оцінка існуючої інфраструктури. Оцінка існуючої інфраструктури організації допоможе визначити, чи відповідає вона вимогам CrowdStrike Falcon.
- Ознайомлення персоналу з CrowdStrike Falcon. Персонал, який буде використовувати CrowdStrike Falcon, повинен бути ознайомлений з її функціоналом та принципами роботи.
- Налаштування CrowdStrike Falcon. Налаштування CrowdStrike Falcon відповідно до вимог організації допоможе забезпечити ефективне функціонування системи.

Впровадження CrowdStrike Falcon включає такі кроки:

1. Розгортання агентів CrowdStrike Falcon на кінцевих точках. Розгортання агентів CrowdStrike Falcon на кінцевих точках дозволить збирати дані про них та передавати їх до хмарної платформи CrowdStrike Falcon.

2. Налаштування правил та політики безпеки. Налаштування правил та політики безпеки CrowdStrike Falcon відповідно до вимог організації допоможе захистити кінцеві точки від кібератак.

3. Тестування системи. Тестування системи допоможе переконатися в її правильному функціонуванні.

Після впровадження CrowdStrike Falcon необхідно забезпечити її підтримку, що включає такі кроки:

1. Мониторинг системи. Моніторинг системи допоможе виявляти потенційні загрози.

2. Оновлення програмного забезпечення. Оновлення програмного забезпечення CrowdStrike Falcon містять виправлення для відомих уразливостей.

3. Реагування на інциденти. Реагування на інциденти допоможе запобігти поширенню кібератак.

Команда CrowdStrike може надати допомогу в підтримці CrowdStrike Falcon, включаючи моніторинг системи, оновлення програмного забезпечення та реагування на інциденти.

CrowdStrike Falcon – це ефективна система захисту кінцевих точок, яка пропонує широкий спектр можливостей для захисту від кібератак. Система має такі переваги:

1. Широка функціональність. CrowdStrike Falcon забезпечує захист від широкого спектру кібератак, включаючи шкідливе програмне забезпечення, фішинг, зловмисне використання облікових записів та інші.

2. Хмарна архітектура. Хмарна архітектура CrowdStrike Falcon забезпечує високу масштабованість і гнучкість.

3. Простіше управління. CrowdStrike Falcon забезпечує зручне централізоване управління.

CrowdStrike Falcon є оптимальним вибором для реалізації сучасної системи захисту кінцевих точок. Система забезпечує високий рівень захисту від кібератак, а також проста в управлінні та масштабуванні.

CrowdStrike Falcon є передовою платформою захисту кінцевих точок, яка використовує хмарні технології для надання реального часу захисту проти широкого спектра загроз. Її основні характеристики включають в себе поведінкове виявлення, машинне навчання, і автоматизоване реагування на інциденти.

Перш за все, CrowdStrike Falcon надає проактивний захист, використовуючи машинне навчання для аналізу та виявлення підозрілих поведінкових моделей на кінцевих точках. Це дозволяє системі швидко ідентифікувати та блокувати нові та не відомі загрози, включаючи нульовий день експлойти та рансомваре.

Другим важливим аспектом є її здатність до автоматизованого реагування на інциденти. Falcon може автоматично ізолювати заражені системи, запобігаючи поширенню інфекції, і надає детальний аналіз після атаки для кращого розуміння та запобігання майбутнім загрозам.

Третій ключовий елемент - це інтеграція з хмарними технологіями. Це забезпечує масштабованість, гнучкість та легкість управління, що особливо важливо для організацій з великою кількістю кінцевих точок та розподіленими системами.

У підсумку, CrowdStrike Falcon надає комплексний, адаптивний і ефективний спосіб захисту кінцевих точок від сучасних кіберзагроз. Її здатність до швидкого виявлення загроз, автоматизованого реагування на інциденти та інтеграції з хмарними технологіями роблять її ідеальним рішенням для сучасних організацій, що прагнуть забезпечити надійний захист своїх інформаційних систем.

Висновки до 3 розділу

Розробка практичних рекомендацій для впровадження системи захисту кінцевих точок є ключовим елементом для забезпечення кібербезпеки в організації. Вона включає розробку архітектури системи, поетапне планування впровадження обраної технології та оцінку ефективності запропонованих заходів.

Архітектура системи захисту кінцевих точок має бути гнучкою та масштабованою, адаптованою до специфічних потреб та ресурсів організації. Важливо, щоб вона інтегрувалась з існуючими системами безпеки та IT-інфраструктурою. Ключовими елементами є централізоване управління, швидке виявлення загроз, ефективне реагування на інциденти та надійне шифрування даних.

Поетапний план впровадження включає інвентаризацію активів, визначення вимог до безпеки, вибір відповідної системи захисту, тестування, впровадження та навчання персоналу. Важливо забезпечити плавний перехід і мінімізувати вплив на ділові процеси. Також необхідно розробити план реагування на інциденти та встановити процеси постійного моніторингу та оновлення системи.

Оцінка ефективності включає моніторинг показників безпеки, аналіз інцидентів та регулярні аудити системи. Ефективність можна виміряти через зменшення кількості безпекових інцидентів, швидкість реагування на загрози та здатність адаптуватися до нових видів атак. Ключовим є залучення всіх зацікавлених сторін та підтримка вищого керівництва.

У сукупності, ці рекомендації створюють міцну основу для захисту кінцевих точок від сучасних кіберзагроз, забезпечуючи безпеку корпоративних даних та IT-інфраструктури.

ВИСНОВКИ

Технологія захисту кінцевих точок інформаційної системи організації - це критично важлива тема, що вимагає глибокого розуміння та постійного оновлення знань. Стратегія запобігання несанкціонованого входу в систему з віддаленого робочого місця набуває вирішального значення – число мобільних пристроїв, підключених до корпоративних мереж, зростає, а техніки злому стають все більш агресивними та витонченими. Сприяє підвищенню ризиків і віддалена робота, яку практикують сьогодні все більше компаній. Сучасний світ кібербезпеки свідчить про зміну фокусу атак з мережевих систем на кінцеві точки, що зумовлює необхідність адаптації стратегій захисту. Традиційний централізований захист мережі вже не забезпечує достатнього рівня безпеки, враховуючи зростання загроз, спрямованих на кінцеві точки. Тут ключову роль відіграє технологія Endpoint Detection and Response (EDR).

EDR представляє собою комплексний підхід до захисту кінцевих точок, включаючи моніторинг, відображення і збереження даних діяльності на цих точках. Всі зібрані дані направляються до центрального сховища для аналізу. Система EDR дозволяє виявляти потенційні загрози в реальному часі і швидко реагувати на них, а також відновлювати систему до безпечного стану після усунення інциденту.

Однією з найскладніших і небезпечних загроз для кінцевих точок є безфайлові атаки (fileless attacks). Ці атаки характеризуються використанням вже існуючих на пристроях додатків, що ускладнює їх виявлення. Проте, незважаючи на відсутність традиційних шкідливих файлів, такі атаки все ж залишають сліди, які можна виявити. Системи на основі EDR ефективно виявляють ці сліди, забезпечуючи надійний контроль і захист кінцевих точок від таких складних загроз. Сучасний ландшафт кібербезпеки неперервно розвивається, що створює нові виклики для захисту інформаційних систем. Ось декілька ключових висновків з цієї теми:

1. Важливість комплексного підходу: Ефективний захист кінцевих точок вимагає комплексного підходу, який включає в себе не тільки антивірусне та антималварне програмне забезпечення, а й рішення для

управління патчами, шифрування даних, моніторингу мережі та управління доступом.

2. Розвиток загроз: Кіберзлочинці постійно розвивають свої методики атаки, включаючи фішинг, соціальну інженерію, використання експлойтів та шкідливих програм. Організаціям необхідно бути в курсі цих методик і відповідно адаптувати свої захисні стратегії.

3. Навчання та освіта: Один з ключових елементів захисту - це освіта співробітників. Людський фактор часто є слабкою ланкою в безпеці інформаційних систем, тому навчання персоналу основам кібергігієни є важливим.

4. Резервне копіювання та відновлення: Регулярне резервне копіювання даних та розробка планів відновлення після інцидентів є критично важливими для забезпечення неперервності бізнесу та мінімізації втрат від можливих кібератак.

5. Технологічні інновації: Впровадження передових технологій, таких як машинне навчання і штучний інтелект, може значно покращити здатність системи ідентифікувати та реагувати на складні загрози.

6. Регуляторні вимоги: Слід також враховувати регуляторні вимоги і стандарти, які можуть впливати на стратегії безпеки організації, наприклад, GDPR в Європі.

У світі, де кіберзагрози швидко розвиваються, важливо забезпечити, щоб захист кінцевих точок інформаційних систем був не лише реактивним, але й превентивним. Це включає розробку комплексних стратегій безпеки, які аналізують поточні тренди в кібербезпеці та адаптуються до них. Використання штучного інтелекту та машинного навчання може допомогти в прогнозуванні та запобіганні кібератакам, перш ніж вони стануть загрозою.

Крім того, важливою є освіта та тренінг співробітників. Людський фактор часто є слабкою ланкою в системі безпеки, тому навчання персоналу основам кібербезпеки та найкращим практикам є ключовим. Це допоможе зменшити ризик інцидентів, пов'язаних з соціальною інженерією та

фішинговими атаками. Узагальнюючи, захист кінцевих точок інформаційних систем вимагає постійної уваги, адаптації до нових загроз та інтеграції передових технологічних рішень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.

2. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.

3. Закон України «Про електронний цифровий підпис». – К.:Відомості Верховної Ради України, 2003. - N 36. - Ст.276 .

4. Інформаційна безпека комп'ютерних систем і мереж: Методичні вказівки // Укл. А.Ф. Карачка, М.П. Карпінський, А.В. Кулик, Т.В. Лендюк. – Тернопіль: ТАНГ, 2007. – 68 с.

5. Кормич Б.А. Організаційно-правові основи політики кібербезпеки України: монографія. Біла Церква, 2021. 552 с.

6. Ліпатніков О.В. Класифікація кібератак: підходи та моделі. Проблеми інформатизації та управління. 2022. No 2. С. 117-124.

7. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.

8. Основи кібербезпеки : підручник / О.П. Погорілий, С.В. Гнатюк, Ю.В. Стасєв та ін. ; за заг. ред. О. П. Погорілого. Київ : ДУТ, 2021. 479 с.

9. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

10. Термінологічний довідник з питань управління інформаційною безпекою організаційно-технічних систем / Юдін О. К., Богданович В. Ю., Корченко О. Г. та ін. Київ: Політехніка, 2009. 180 с.

11. Фаль О. М. Криптографія: основні ідеї та застосування/ О. М. Фаль. – К,: Вид-во НТТУ КПІ, 2004.

12. Шандриголова Т. М. Інцидент у сфері інформаційної безпеки: сутність та зміст поняття. Форум права. 2021. No 65. С. 495–503.

13. Ashford, Warwick (2018). Physical security controls form first line of cyber defence. ComputerWeekly.com. URL: https://www.computerweekly.com/news/252439383/Physical-security-controls-form-first-line-of-cyber-defence

14. B. Gupta, R. C. Joshi, and M. Misra, "Ann based scheme to predict number of Zombies in a DDoS attack," International Journal of Network Security, vol. 18, no. 2, pp. 328-338, 2016.

15. Cimpanu, Catalin (2022). Best encryption software in 2022. ZDNet. URL:https://www.zdnet.com/article/best-encryption-software/

16. Duane Wessels. Squid: The Definitive Guide. – O'Reilly Media, 2004 – 472 c.

17. Dubey, K. Qattous, J. Whisnant, and R. B. Lee, “An advanced persistent threat analysis approach using machine-learning algorithms,” in MILCOM 2015 - 2015 IEEE Military Communications Conference, 2015, pp. 6–11.

18. ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. ENISA, 2021. 85 p.

19. European Union Agency for Cybersecurity (2021). Inventory and control of hardware assets. ENISA. URL: https://www.enisa.europa.eu/publications/inventory-and-control-of-hardware-assets

20. Glossary of Key Information Security Terms. NISTIR 7298 Rev. 2. National Institute of Standards and Technology, 2013. 208 p.

21. Grispos, George et al. (2013). Security incident management: Challenges and best practice. In Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 2nd-4th December, 2013. URL: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1436&context=ism

22. Jesse Russell. Deep packet inspection. – Книга по Требованию, 2013 – 136 с.

23. K. B. Raja, R. I. Prasad, V. Gupta, and A. Lazarevic, "Neural network approach for anomaly detection in TLS encrypted traffic," in Proceedings of the International Joint Conference on Neural Networks, 2020.

24. L. Koc, T. A. Mazzuchi, and S. Sarkani, “A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier,” Expert Systems with Applications, vol. 39, no. 18, pp. 13492–13500, 2012.

25. Mather, Tim et al. (2019). What Is UEM? The Next Step in Enterprise Mobility Management. Gartner. URL: https://www.gartner.com/smarterwithgartner/what-is-uem-the-next-step-in-enterprise-mobility-management

26. Microsoft (2021). Secure passwords. Microsoft 365 Blog. URL:https://www.microsoft.com/en-us/microsoft-365/blog/2021/05/06/secure-passwords/

27. Morey, James et al. (2015). Principle of least privilege. Techtarget. URL: https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP

28. NATO glossary of terms and definitions. AAP-06 Edition 2021. NATO Standardization Office, 2021. 298 p.

29. S. Axelsson, "The base-rate fallacy and its implications for the difficulty of intrusion detection," in Proceedings of the 6th ACM Conference on Computer and Communications Security, 1999.

30. Surak, John (2021). What is Encrypted Traffic Analysis?. Tetra Defense Blog. URL: https://www.tetradefense.com/encrypted-traffic-analysis/

31. Symantec (2019). Internet Security Threat Report. Volume 24. URL: https://docs.broadcom.com/doc/istr-24-2019-en

32. Vacca, John R. Network and system security. – Syngress, - 432 p.

33. Varonis (2017). 60% of an Organization's Data Resides on End User Devices. URL: https://www.varonis.com/blog/60-percent-of-an-organizations-data-resides-on-end-user-devices/

34. W. Lee and S. J. Stolfo, "A framework for constructing features and models for intrusion detection systems," ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 227–261, 2000.

35. Z. He, T. Zhang, and R. B. Lee, "Machine learning based hybrid intrusion detection system for software defined networks," IEEE Access, vol. 8, pp. 49296-49308, 2020.