ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА
ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

ВСЕУКРАЇНСЬКА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ»

Дата проведення:
03 листопад 2024 року.

Початок о 10:00.

Київ 2024

УДК 004.89:621.39(043.2)

Організатори:

Іванченко Євгенія Вікторівна кандидат технічних наук, професор, Директор навчально-наукового інституту кібербезпеки та захисту інформації ДУІКТ;

Туровський Олександр Леонідович, доктор технічних наук, професор, завідувач кафедри Технічних систем кіберзахисту ДУІКТ;

Хлапонін Юрій Іванович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури.;

Пепа Юрій Володимирович, професор кафедри Технічних систем кіберзахисту ДУІКТ, кандидат технічних наук, доцент.

Комп’ютерна верстка та редагування:
Поночовний Петро Михайлович, старший викладач
кафедри технічних систем кіберзахисту ДУІКТ.

Рекомендовано до друку Вченою радою Навчально-наукового інституту телекомунікацій Державного університет інформаційно-комунікаційних технологій (протокол № 9 від 24.05.2024 р.).

Актуальні проблеми безпеки інформаційно-телекомунікаційних систем: збірник тез всеукраїнської науково-практичної конференції (м. Київ, 03 листопада 2024 року), Київ: РВЦ ДУІКТ. – 2024. – 110 с.

Збірник тез призначений для аспірантів, науковців, викладачів та інших зацікавлених осіб.

О.С. Ветлицька,
аспірантка кафедри управління інформаційною
та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, м. Київ

ЗАХИСТ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА В КОНТЕКСТІ ДЕРЖАВНОГО УПРАВЛІННЯ

У роботі розглянуто питання безпеки цифрової держави з акцентом на захист інформації та кібербезпеки в контексті державного управління. Проаналізовано сучасні виклики, пов'язані з використанням інформаційних технологій у державному управлінні, та запропоновано певні заходи спрямовані на забезпечення безпеки цифрового простору держави.

Ключові слова: безпека цифрової держави; інформаційні технології; кібербезпека; захист інформації.

Цифровізація та застосування інформаційних технологій у державному управлінні стали невід'ємною частиною сучасного суспільного життя. Однак, зі зростанням використання цифрових технологій виникає низка загроз для безпеки цифрової держави, включно з витоком і несанкціонованим доступом до конфіденційної інформації, кібератаками та іншими видами кіберзлочинності [1].

Важливим кроком є розробка та впровадження стандартів безпеки для державних органів. Це має включати встановлення правил для доступу до конфіденційної інформації, шифрування даних, регулярне оновлення програмного забезпечення та апаратного забезпечення, а також моніторинг та аналіз подій безпеки. Навчання персоналу державних органів основам кібербезпеки є критичним кроком. Співробітники мають бути проінформовані про можливі загрози, знати, як розпізнавати фішингові листи, використовувати складні паролі та звертатися по допомогу в разі виникнення підозрілих подій [1]. Регулярні тренінги та оновлення знань є невід'ємною частиною процесу навчання.

Посилення заходів щодо захисту від несанкціонованого доступу до інформації також є важливим аспектом безпеки. Це може включати двофакторну автентифікацію, використання біометричних даних, контроль доступу на основі ролей та інші методи захисту. Співпраця з міжнародними організаціями щодо обміну інформацією про кіберзагрози є необхідним кроком для забезпечення безпеки цифрового простору. Це дає змогу отримувати інформацію про нові загрози та обмінюватися досвідом з іншими державами в боротьбі з кіберзлочинністю. Колективні зусилля, включно зі спільними навчаннями та регулярними зустрічами, сприяють підвищенню ефективності боротьби з кіберзагрозами [2].

Розвиток криптографічних методів захисту персональної інформації громадян також є важливим аспектом безпеки цифрової держави. Механізми шифрування та автентифікації допомагають захистити особисті дані громадян від несанкціонованого доступу та використання [3]. Захист інтересів громадян у цифровому просторі також є важливим завданням. Державні органи повинні забезпечити безпеку інформаційних систем громадських служб, таких як охорона здоров'я, освіта та соціальне обслуговування.

Важливим аспектом кібербезпеки цифрової держави є розробка сильних систем захисту даних. Це включає в себе використання сучасних технологій для виявлення та запобігання атакам, таких як системи штучного інтелекту та машинного навчання [2]. Ці технології дають змогу автоматизувати процеси виявлення та реагування на загрози, що підвищує ефективність захисту. Розвиток систем моніторингу та аналізу даних також має важливе значення для забезпечення безпеки.

Приватні компанії можуть надавати спеціалізовані послуги з кібербезпеки, проводити аудити та тестування вразливостей систем, а також пропонувати інноваційні рішення для

захисту даних. Партнерство з приватним сектором дає змогу використовувати найкращі практики та досвід у сфері кібербезпеки. Впровадження стандартів і сертифікації в галузі кібербезпеки також важливе для забезпечення безпеки цифрової держави. Це може охоплювати сертифікацію інформаційних систем, мереж та обладнання, а також стандарти шифрування та автентифікації [3]. Дотримання цих стандартів допомагає забезпечити відповідність систем і послуг вимогам безпеки.

Забезпечення безпеки цифрової держави потребує комплексного підходу та посилених зусиль з боку державних органів. Розроблення та впровадження політик і стандартів безпеки, навчання персоналу, розвиток кібербезпеки, співпраця з іншими країнами та громадськістю, а також підвищення поінформованості громадян щодо кібербезпеки - все це необхідно для ефективного захисту інформації та гарантування безпеки державних органів і громадян.

Список використаних джерел:

1. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 16.02.2024).
2. Сратегія інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення: 20.04.2022).
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 No 2163-VII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.02.2024).

Н.П. Яцкова
Державний університет інформаційно-комунікаційних технологій, м. Київ

ВАЖЛИВІСТЬ КІБЕРБЕЗПЕКИ НА ОБ’ЄКТІ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

У сучасному ландшафті світових фінансів банківська галузь дедалі більше покладається на цифрові технології, що відкриває безпрецедентні рівні ефективності та зв'язку. Однак ця оцифровка також породила безліч загроз кібербезпеці, зробивши фінансові установи головними мішенями для зловмисників, які прагнуть отримати несанкціонований доступ, фінансову вигоду або підірвати їхню роботу. У цьому контексті неможливо переоцінити необхідність надійних заходів кібербезпеки в банківській сфері.

У сучасну цифрову епоху кібербезпека має першорядне значення для банківської галузі. Зі зростанням залежності від онлайн-банкінгу та цифрових фінансових послуг захист даних клієнтів, фінансових активів і критично важливих систем від кібератак має вирішальне значення.

Банкам довіряють величезні обсяги конфіденційної інформації про клієнтів, включаючи фінансові дані, персональні дані та облікові дані для входу в систему. Захист цих даних необхідний для того, щоб захистити клієнтів від крадіжки персональних даних, шахрайства та іншої фінансової шкоди. Кібератаки можуть призвести до значних фінансових втрат для банків та їхніх клієнтів.

Наприклад, шахрайство з банкоматами коштувало одному банку близько $7,3 млн, а успішний злом системи онлайн-банкінгу іншого банку - $10 млн [1]. У 2003 році бізнес втратив майже $666 млн. від кібератак, і це не враховуючи випадкових збитків від крадіжки майна та особистих даних [2].

Захист від кіберзагроз має важливе значення для забезпечення цілісності фінансових систем та збереження довіри до банківського сектору [3]. Збої, спричинені кібератаками, можуть завдати шкоди банківським операціям і серйозно вплинути на якість обслуговування клієнтів.

Кіберзлочинці постійно вдосконалюють свою тактику, розробляючи нові атаки, такі як фішингові кампанії, зараження шкідливим програмним забезпеченням та атаки з вимогою викупу. Зростаюча залежність від онлайн-банкінгу та взаємопов'язаних систем розширює можливості для атак і створює нові вразливості. Спрямованість атак вразливості в ланцюжках постачання програмного забезпечення можуть мати широкі наслідки для банківської індустрії. Глобальний дефіцит кадрів у сфері кібербезпеки створює значні труднощі для банків у пошуку та утриманні кваліфікованих фахівців.

Надійна автентифікація та контроль доступу шляхом впровадження багатофакторної автентифікації, безпечних паролів та контролю доступу на основі принципу найменших привілеїв допомагає запобігти несанкціонованому доступу. Шифрування конфіденційних даних у стані спокою та під час передачі захищає їх від несанкціонованого доступу, навіть якщо вони перехоплені. Управління вразливостями та виправлення шляхом регулярного сканування систем на наявність вразливостей та оперативного застосування патчів має вирішальне значення для усунення відомих вразливостей у системі безпеки. Підвищення обізнаності та навчання з питань безпеки шляхом інформування працівників і клієнтів про ризики та найкращі практики кібербезпеки допомагає запобігти атакам соціальної інженерії та спробам фішингу. Планування реагування на інциденти кібербезпеки - наявність добре підготовленого плану реагування на кібератаки мінімізує збитки та прискорює процес відновлення. Співпраця з правоохоронними органами та галузевими партнерами шляхом обміну розвідданими про загрози та співпраці з іншими організаціями в банківському секторі та за його межами допомагає ефективніше боротися з кіберзлочинністю.

Впровадження надійних заходів кібербезпеки має важливе значення для забезпечення безперервності бізнесу та мінімізації простоїв. Банки повинні дотримуватися різних правил і стандартів щодо безпеки даних та запобігання фінансовим злочинам. Впровадження ефективних заходів кібербезпеки має вирішальне значення для дотримання нормативних вимог та уникнення штрафних санкцій з боку регулятора.

У постійно мінливому ландшафті кібербезпеки шлях до захисту національної інфраструктури, особливо в банківському секторі, є динамічним і багатогранним. Оскільки технологічні інновації продовжують змінювати ландшафт загроз, стійкий і спільний підхід буде ключовим для забезпечення цілісності, конфіденційності та доступності критично важливих фінансових систем. Щоб орієнтуватися в майбутніх тенденціях, потрібна проактивна позиція, співпраця між різними галузями, а також прихильність до безперервної освіти та розвитку навичок.

Список використаних джерел:

1. Johnson, A.L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. NC Banking Inst., 20, 277.

2. Bada, M., & Nurse, J.R. (2020). The social and psychological impact of cyberattacks. In Emerging cyber threats and cognitive vulnerabilities (pp. 73-92). Academic Press.

3. Horna, C.J., Toro, L., & Regalado-Pezua, O. (2022). Silver bank: vulnerability and risks during cyberattacks. Emerald Emerging Markets Case Studies, 12(1), 1-33.

Д.В. Бойко
Студент групи ТСДМ-62,
Державний університет інформаційно-комунікаційних технологій, м. Київ

АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕТОДИ ЗАХИСТУ WI-FI МЕРЕЖ

У роботі розглядаються актуальні проблеми безпеки інформаційно-телекомунікаційних систем з акцентом на захист Wi-Fi мереж. Проаналізовано сучасні загрози, такі як атаки "Man-in-the-Middle", несанкціонований доступ, використання слабких точок доступу та соціальна інженерія. Пропонуються ефективні методи захисту, включаючи шифрування даних, багатофакторну автентифікацію та виявлення підроблених точок доступу. Окрема увага приділяється важливості своєчасного виявлення вразливостей і моніторингу мереж для підвищення загального рівня безпеки.

Ключові слова: Wi-Fi мережі, інформаційна безпека, кібератаки, шифрування, несанкціонований доступ.

Сучасні інформаційно-телекомунікаційні системи, в тому числі мережі Wi-Fi, є невід'ємною частиною повсякденного життя. Вони забезпечують швидкий та зручний доступ до інформації, сприяють розвитку бізнесу, науки, освіти та комунікацій. Однак разом з розвитком технологій зростає і кількість загроз та вразливостей, які можуть негативно вплинути на безпеку даних. Мережі Wi-Fi стають привабливою мішенню для кібератак, зокрема через їхню широку доступність і часто недостатній рівень захисту. Це вимагає розробки та впровадження нових методів виявлення та захисту від несанкціонованих вторгнень.

Актуальність проблеми безпеки мереж Wi-Fi зумовлена стрімким зростанням обсягів передачі даних та їх чутливості, що підвищує інтерес кіберзлочинців до таких систем. Особливу загрозу становлять атаки типу «зловмисник посередині», фейкові точки доступу та використання застарілих методів шифрування, що дозволяють перехоплювати дані користувачів. З огляду на постійне вдосконалення методів злому, виникає потреба в нових підходах до виявлення потенційних загроз і забезпечення надійного захисту Wi-Fi мереж. Особливо актуальним це питання є для корпоративних та державних структур, де відсутність належного рівня безпеки може призвести до значних фінансових та інформаційних втрат [1].

1. **Зростаюча загроза кібератак на Wi-Fi мережі**. У сучасних умовах широке використання мереж Wi-Fi для передачі конфіденційної інформації робить їх мішенню для зловмисників. Кібератаки на мережі Wi-Fi можуть приймати різні форми, від простих несанкціонованих підключень до більш складних методів, таких як перехоплення і модифікація трафіку. Відсутність належного захисту створює ризик витоку конфіденційної інформації. Актуальність цієї проблеми постійно зростає через постійне збільшення кількості підключених пристроїв та мобільного трафіку. Необхідність виявлення вразливостей і впровадження ефективних механізмів захисту, таких як регулярний аудит безпеки, стає нагальним завданням для всіх учасників мережі.

2. Проблема безпечного шифрування даних. Одним з ключових аспектів безпеки Wi-Fi мережі є захист даних під час передачі. Використання застарілих протоколів шифрування, таких як WEP або навіть WPA, не забезпечує достатнього рівня безпеки, оскільки ці протоколи вразливі до ряду атак, включаючи швидке розшифрування трафіку. Новітній протокол WPA3 забезпечує кращий рівень захисту завдяки використанню індивідуальних сеансових ключів та більш надійних методів аутентифікації. Впровадження сучасних стандартів шифрування є необхідною умовою для запобігання витоку даних в мережах Wi-Fi, особливо в корпоративних середовищах.

3. **Атаки типу «людина посередині» (MitM)**. Однією з найсерйозніших загроз безпеці мереж Wi-Fi є MitM-атаки, коли зловмисник перехоплює трафік між користувачем і точкою

доступу, не будучи виявленим. Це дозволяє хакерам перехоплювати конфіденційні дані, такі як паролі, банківські реквізити або особисту інформацію, і змінювати їх на свій розсуд. MitM-атаки можуть бути реалізовані через використання фальшивих точок доступу або вразливостей шифрування. Ефективними методами запобігання таким атакам є впровадження багатофакторної автентифікації, використання сучасних протоколів шифрування та регулярний моніторинг мережі на предмет підозрілої активності, а також впровадження технологій розпізнавання аномалій у мережевому трафіку [2].

4. Захист від атак через слабкі точки доступу (Rogue Access Points). Однією з найнебезпечніших загроз для безпеки Wi-Fi мереж є атаки з використанням фейкових точок доступу, які зловмисники створюють для імітації легітимних мереж. Такі точки доступу дозволяють користувачам перехоплювати дані, коли вони помилково підключаються до фальшивої мережі. Шахрайські точки доступу можуть бути використані для крадіжки персональних даних, фінансової інформації або навіть для отримання повного контролю над пристроями жертви [3, с. 41].

Загальні питання безпеки інформаційно-телекомунікаційних систем, у тому числі мереж Wi-Fi, є однією з ключових загроз у сучасному цифровому світі. Поширення кіберзлочинності, використання застарілих методів шифрування, таких як WEP і WPA, а також атаки «зловмисника посередині» і фальшивих точок доступу Rogue Access Points створюють значні ризики для конфіденційності та безпеки даних. Вразливості в мережах Wi-Fi стають все більш серйозними через зростання кількості мобільних пристроїв і користувачів, що підключаються до мереж. Важливим аспектом захисту є впровадження багатофакторної автентифікації, яка значно ускладнює зловмисникам отримання доступу, навіть якщо пароль був скомпрометований. Також необхідно впроваджувати сучасні протоколи шифрування, такі як WPA3, для забезпечення надійного захисту трафіку.

Список використаних джерел:

1. Аналіз механізмів захисту та вразливостей бездротових Wi-Fi мереж. [Електронний ресурс]. — Режим доступу: http://ir.nmu.org.ua/butstream/handle

2. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. — Режим доступу: http://zakon5.rada.gov.ua/laws/show/1126–97–%D0%BF

3. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). [Електронне видання]. Київ: Нац. акад. СБУ, 2019. 384 с.

С.Р. Кулініч
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЛЬ ШИФРУВАННЯ В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ЗАКРИТИХ ЛІНІЙ ПЕРЕДАЧІ ДАНИХ

У сучасному світі зростаюча кількість кіберзагроз ставить питання захисту інформації на перше місце, особливо коли йдеться про передачу даних в інформаційно-телекомунікаційних системах. Використання закритих каналів передачі даних є важливим засобом забезпечення конфіденційності та цілісності інформації, що передається. Такі канали забезпечують захист від несанкціонованого доступу та перехоплення, що є особливо актуальним для критичних інфраструктур, урядових організацій та бізнесу. Впровадження ефективних засобів захищеної передачі даних, таких як фізично захищені лінії, лінії з шифруванням даних, VPN, супутникові та мобільні мережі, дозволяє значно підвищити безпеку передачі даних і знизити ризик витоку конфіденційної інформації.

Основні загрози захисту закритих ліній передачі даних включають перехоплення, коли зловмисники можуть отримати доступ до конфіденційної інформації під час її передачі, і модифікацію повідомлень, що може призвести до зміни даних або їх фальсифікації. Також поширені атаки на конфіденційність, які використовують вразливості в шифруванні або реалізації протоколів, що дозволяє розкрити зашифровану інформацію або отримати ключі. Для протидії цим загрозам необхідно застосовувати надійні методи шифрування та актуальні протоколи безпеки.

Основні загрози для закритих ліній передачі даних включають перехоплення інформації, коли зловмисники можуть отримати доступ до конфіденційних даних під час їх передачі. Також серйозною загрозою є модифікація повідомлень, що може призвести до зміни переданих даних або їх фальсифікації. Ще однією небезпекою є атаки на конфіденційність, які використовують слабкі місця у протоколах шифрування або їх реалізації. Такі загрози особливо актуальні для супутникових і мобільних мереж, де можливі атаки типу "людина посередині". Для захисту від цих загроз важливо застосовувати сучасні методи шифрування та надійні протоколи безпеки.

Алгоритм шифрування AES (Advanced Encryption Standard) є одним із найпоширеніших методів захисту даних у закритих лініях передачі. Його перевагою є висока швидкість шифрування та стійкість до зламу, що забезпечує надійний захист від атак на конфіденційність. AES підтримує різні довжини ключів (128, 192, 256 біт), що дозволяє налаштувати рівень безпеки відповідно до вимог.

Основним недоліком є те, що AES є симетричним алгоритмом, тобто для шифрування та розшифрування використовується один і той самий ключ. Це вимагає безпечного обміну ключами, що може бути складним завданням. Крім того, у разі витоку ключа зловмисник може отримати доступ до всієї зашифрованої інформації.

Як приклад для одного з видів закритих каналів передачі даних, фізично захищеного каналу передачі: оптоволокна, складність отримання інформації можна оцінити через вирази, що враховують фізичні та криптографічні фактори. У цьому контексті розглянемо два аспекти: перехоплення сигналу з оптоволокна та злам шифрування[1].

Перехоплення сигналу з оптоволокна (без шифрування)

Без шифрування складність отримання інформації пов'язана з можливістю незаконного підключення до оптоволокна. Цю складність можна визначити за наступною формулою(1) [2]:

$$S_{\text{перехоплення}} = P_{\text{виявлення}} \times T_{\text{фізичне підключення}} \quad (1),$$

де $P_{\text{виявлення}}$ — ймовірність виявлення перехоплення, що залежить від використання технологій моніторингу каналу (наприклад, детекторів згасання сигналу), а$T_{\text{фізичне підключення}}$ — час, необхідний для підключення до оптоволокна.

Чим складніше фізично отримати доступ до кабелю (наприклад, через його розташування чи наявність системи моніторингу), тим вище складність перехоплення. Однак, якщо зловмисник успішно підключиться, дані передаються у відкритому вигляді, і їхнє отримання є прямим.

Перехоплення з шифруванням (AES)

Коли дані в оптоволокні захищені шифруванням, складність отримання інформації визначається як комбінація складності фізичного перехоплення та складності зламу шифрування, яку можна визначити за формулою (2)[2]:

$$S_{\text{загальне}} = S_{\text{перехоплення}} + T_{AES} \quad (2),$$

де $S_{\text{перехоплення}}$ — складність фізичного підключення до оптоволокна, як описано вище, а T_{AES} — це час, необхідний для зламу шифрування, який можна визначити за формулою (3):

$$T_{AES} = \frac{2^n}{R} \quad (3),$$

де n — довжина ключа в бітах (наприклад, 128 для AES-128), а R — кількість операцій в секунду.

Висновок

Дослідження показало, що шифрування є критично важливим елементом для захисту інформації в закритих лініях передачі даних, таких як оптоволокно. Без шифрування зловмисники можуть легко отримати доступ до інформації після фізичного підключення до каналу. Однак впровадження сучасних алгоритмів, таких як AES, значно підвищує рівень захисту, роблячи несанкціонований доступ практично неможливим через величезну кількість обчислень, необхідних для злому.

Таким чином, використання шифрування в поєднанні з фізично захищеними каналами, VPN та іншими технологіями дозволяє значно знизити ризики перехоплення й модифікації даних. У фізично захищених каналах, таких як оптоволокно, шифрування не є обов'язковим, а виконує функцію додаткового рівня захисту, який значно ускладнює перехоплення та доступ до інформації. У таких каналах основний захист забезпечується фізичною безпекою інфраструктури, тоді як шифрування підвищує загальну стійкість до загроз. Порівняно з цим, для інших типів каналів, таких як мобільні мережі, супутникові зв'язки або VPN, шифрування є обов'язковою та невід'ємною частиною захисту, без якої забезпечення конфіденційності та цілісності інформації стає неможливим. Це обумовлено високим ризиком перехоплення даних та наявністю більшої кількості потенційних точок атаки в таких середовищах.

Отримані результати можуть бути застосовані для вдосконалення безпеки в інформаційно-телекомунікаційних системах, особливо в критично важливих інфраструктурах, де гарантування конфіденційності та цілісності інформації має вирішальне значення[3].

Список використаних джерел:

1. Stallings W. *Cryptography and Network Security: Principles and Practice.* 7th ed. Boston: Pearson, 2017. 840 p.

2. Palais J. C. *Fiber Optic Communications.* 5th ed. Upper Saddle River: Prentice Hall, 2005. 550 p.

3. Конрад Е., Фельдман Дж. *Навчальний посібник CISSP.* 2-ге видання. Бостон: Syngress, 2012. 638 с.

А.О. Хоменко
Державний університет інформаційно-комунікаційних технологій, м. Київ

ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ ПРИВІЛЕЙОВАНОГО ДОСТУПУ (PRIVILEGED ACCESS MANAGEMENT)

Один із найбільш делікатних аспектів інформаційних технологій являється привілейований доступ. Саме, за допомогою привілейованих облікових даних вносяться значні зміни в пристроях та програмах, які встановлені в інфраструктурі, що в більшості впливає на безперервність бізнесу. Використовуючи у зловмисний спосіб привілегійовані облікові записи, призведуть до порушення пунктів відповідності, що в результаті буде інцидентом інформаційної безпеки.

Саме, Privileged Access Management дає можливість зменшити внутрішні та зовнішні кіберзагрози в організації. За допомогою, PAM можна контролювати доступ до такої інформації, як фінанси, комерційна таємниця та особисті дані клієнтів. Аналіз кіберзагроз за останні роки найбільш пов'язаний із компрометацією привілейованих облікових даних, тобто записи адміністраторів та інших користувачів із підвищими правами були скомпрометованими. Зловмисник, отримавши доступ до облікових даних, які мають підвищені має пряму вразливість для організації.

На даний момент, найбільше порушень безпеки пов'язане із компрометацією паролів користувачів і привілейованих облікових записів. Отримавши доступ до даних записів зловмисники можуть приховувати власну діяльність під виглядом адміністратора. Деякі порушення кібербезпеки залишилася непоміченими більше 200 днів. Найопопулярніші приклади, отримання доступу зловмисниками:

1. Зловмисники використовують шкідливе програмне забезпечення або соціальну інженерію, щоб отримати доступ до комп'ютерів, ноутбуків або серверів. Користувачам надсилають фішингові листи, в яких просять натиснути посилання, в подальшому завантажить програмне забезпечення із зловмисним програмним забезпеченням прихованим усередині, або ввести паролі від облікових даних на підроблених веб-сайтах.
2. Використання атаки «Man in the Middle or Pass the Hash attacks».

Прикладами порушення безпеки, є наступні систуації:

- У 2019 році інформація про понад 30 000 співробітників Міністерства внутрішньої безпеки було зламано. Зловмисник, отримав доступ до даних через електронну пошту співробітника.
- У 2016 році компанія з хмарних сховищ Dropbox виявила, що була зламана ще в 2012 році, що призвело до втрати електронної пошти 68 мільйонів користувачів та паролі, що розкриваються в Інтернеті.

Адміністратор – це вбудований обліковий запис, який налаштовує компоненти Windows, такі як каталог, файлова система та мережеві компоненти. «Root» - це обліковий запис суперкористувача в системах Unix та Linux. Будь-який користувач знаючи пароль від даних користувачів може увійти в систему.

OWASP характеризує доступ до привілегійованих облікових записів, як критичний та відносить до списку 10 найпопулярніших ризиків. Під контролем доступу, мається на увазі дотримання політик, щоб користувачі не могли діяти поза межами виділених дозволів. *Поширеними вразливостями є:*

- Порушення принципу привілеїв, де доступ мав надаватися для певних дій, але доступний всім.
- Обхід перевірок контролю доступом шляхом підміни URL-адреси.
- Підвищувати власні привілеї, ввійшовши як користувач.

Прикладом атак на основі визначених вразливостей, наведено:

1. Програма використовує неперевірені SQL дані, яка отримує доступ до інформації облікового запису:

pstmt.setString(1, request.getParameter("acct"));

ResultSet results = pstmt.executeQuery( );

При використанні, зловмисник змінює «acct» браузера, щоб надіслати будь-який номер облікового запису. Якщо перевірка буде неправильна, то зловмисник отримує доступ до облікового запису користувача:

https://example.com/app/accountInfo?acct=notmyacct

2. Зловмисник змусить переглянути цільові URL-адрес. Для доступу до сторінки адміністратора потрібні права адміністратора.

https://example.com/app/getappInfo

https://example.com/app/admin_getappInfo

Отже, компанії, які не мають управління привілегійованими обіліковими записами стикаються із важливими проблемами, які включають:

- Працівники мають надмірні привілеї, що перевищують вимоги до їх ролей.
- Спільний доступ до облікових записів, наприклад: кілька осіб спільно використовують привілейовані облікові запис. Організації буде складно ідентифікувати, хто саме використовує даного користувача.
- Зловмисники можуть отримати несанціонований доступ до критично важливих систем і даних, якщо вони скомпрометовані.
- Довірені співробітники можуть стати внутрішньою загрозою, якщо їхній привілейований доступ зловживається зловмисно.

Отже, дана технологія надзвичайно поширена та вимагає надійного захисту. Заходи безпеки, які необхідно вжити слід ретельно розглянути. Якщо враховувати, відповідні правила, то ризик від атак, який спрямований на організацію буде мінімальний.

Список використаних джерел:

1. OWASP 2024 Top 10: https://github.com/OWASP/Top10/tree/master/2024/Data»
2. Bago (Editor), E. & Glazer, I., (2023) "Introduction to Identity - Part 1: Admin-time (v2)", IDPro Body of Knowledge 1(5). doi: https://doi.org/10.55621/idpro.27

А.М. Котенко,
Доцент каф. Технічних систем кіберзахисту,
В.В. Каліш,
студент групи СЗДМ 61,
Державний університет інформаційно-комунікаційних технологій м. Київ

ПОРІВНЯННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМИ ХЕШУВАННЯ SHA-3 ТА SHA-256

SHA-3 і SHA-256 два криптографічних алгоритми хешування, які відіграють важливу роль в безпеці інформаційних систем. Обидва алгоритми генерують хеш-значення для подібних цілей, але є важливі відмінності, які професіонали безпеки повинні враховувати при виборі того, який з них використовувати.

Однією з головних відмінностей між SHA-3 і SHA-256 є їх архітектура: SHA-256 належить до сімейства SHA-2 і базується на класичній структурі Меркла-Демгарда. Навпаки, SHA-3 базується на алгоритмі Keccak і використовує структуру губки для обробки даних. Ця архітектурна відмінність робить SHA-3 більш стійкими до певних типів атак, таких як атаки розширення довжини, які використовують вразливості в структурі Merkle-Damgård. Продуктивність є ще одним важливим фактором при виборі між цими алгоритмами: SHA-256 старіший, більш широко прийнятий, і вигоди від апаратної підтримки на багатьох системах; SHA-3 новіший і пропонує поліпшену криптографічну надійність, але без апаратної оптимізації. Однак його продуктивність може змінюватися в залежності від конкретних вимог безпеки та швидкості виконання даного завдання.

З точки зору безпеки обидва алгоритми надійні: SHA-256 широко використовується в різних галузях, де потрібна висока безпека, таких як блокчейн і цифрові підписи; SHA-3 була розроблена як альтернатива SHA-2 на випадок виявлення вразливості в SHA-2; SHA-256 був розроблений як альтернатива SHA-2 на випадок виявлення вразливості в SHA-2. Це підходящий варіант для проектів, які вимагають додаткової безпеки і довгострокової стійкості від майбутніх атак на SHA-256.

З точки зору додатків, SHA-256 найкраще підходить для сценаріїв, які вимагають швидкості і широкої сумісності, таких як блокчейн-системи (наприклад, Bitcoin) або інтеграції з існуючими криптографічними протоколами. Навпаки, SHA-3 підходить для нових проектів, де довгострокова стійкість до криптографічних атак є пріоритетною.

На закінчення, як SHA-3, так і SHA-256 є надійними алгоритмами хешування і можуть бути застосовані до широкого спектру систем. Вибір між ними залежить від таких факторів, як відмовостійкість архітектури, продуктивність і специфічні вимоги безпеки. Обидва алгоритми забезпечують високий рівень захисту. Тому рішення повинно ґрунтуватися на конкретних потребах системи або проекту.

Список використаних джерел:

1. SHA-3 Algorithms - [Електронний ресурс]. – Режим доступу :https://xilinx.github.io/Vitis_Libraries/security/2019.2/guide_L1/internals/sha3.html

2. The cryptographic hash function SHA-256 - [Електронний ресурс]. – Режим доступу :https://helix.stormhub.org/papers/SHA-256.pdf

3. What is the difference between SHA-3 and SHA-256 - [Електронний ресурс].–Режим доступу :https://crypto.stackexchange.com/questions/68307/what-is-the-difference-between-sha-3-and-sha-256

А.В. Кобець,
Студент групи СЗДМ 61
Державний університет інформаційно-комунікаційних технологій м. Київ

ЗАХИСТ ІНФОРМАЦІЇ У МЕРЕЖАХ МОБІЛЬНИХ ОПЕРАТОРІВ СТАНДАРТУ GSM.

Сучасні засоби мобільного зв’язку дають суспільству великі можливості для обміну інформацією. Але разом з цим вони також є небезпечним інструментом для несанкціонованого отримання інформації сторонніми особами. Перепрограмування мобільного телефону, підміна або подарунок модифікованого пристрою, впровадження вірусу у комунікатор дають можливість отримувати доступ к даним на мобільному телефоні, а також прослуховувати всі розмови, що ведуться поблизу нього.

Для забезпечення конфіденційності телефонних розмов, що здійснюються незахищеним GSM каналом, необхідно використовувати системи безпеки на основі шифрування даних. Наприклад використанням другої версії алгоритму A5/2 [1]. Алгоритм заснований на регістрах зсуву з лінійної зворотним зв'язком певної довжини (19, 22, 23 біта). Початкові заповнення регістрів визначаються секретним і відкритим ключами. Відкритий ключ відомий і різний для кожного нового сеансу. Але цей алгоритм не є гарантією приватності розмови

Також можливе використання стандарту GSM SAFE – це акустичний сейф, призначений для захисту від прослуховування через мобільні пристрої. Автоматичне спрацьовування GSM SAFE відбувається під час несанкціонованої віддаленої активації мобільного пристрою зв'язку. Він починає генерувати шуми в чутному діапазоні акустичних частот, що маскують мову

Не є зайвим й метод застосування криптофонів. Криптофони - це звичайні смартфони з додатковим програмним забезпеченням. Першими такі пристрої розробила німецька компанія Cryptophone, звідки і їх назва. Принцип дії криптофонів, як і скремблерів, полягає у наступному: сигнали з мікрофону оцифровуються, кодуються і відправляються в мережу стільникового зв'язку в зашифрованому вигляді. Вся різниця між криптофонами і скремблерами полягає у способі 2 реалізації цієї методики. Головною перевагою криптофона є використання двох алгоритмів шифрування AES і Twofish з ключами довжиною 256 біт, розподіленими за системою Діффі-Хелмана (з власним ключем завдовжки 4096 біт). Також існують криптографічні картки SECUSMART, які встановлюються у телефон і перетворюють його у повноцінний криптофон.

Також використовуються додатки для шифрування за алгоритмом AES [2]:

- клас Aes Encription відповідає безпосередньо зазашифрування сигналу;
- клас Audiorecorder відповідає за захоплення звуку з мікрофону;
- клас Cripto Exception обробляє можливі помилки при роботі крипто алгоритму і виводить коди помилок;
- клас Decription Form відповідає користувацький інтерфейс для процесу розшифрування;
- клас Encription Form відповідає за користувацький інтерфейс для процесу зашифрування;
- клас Sound Capture відповідає за обробку захопленого звуку.

Проведений аналіз криптоалгоритмів, що використовуються в мережах GSM та можуть бути використані додатково, дозволяє розробити додаток на мові програмування JAVA що використовує додаткові засоби для обробки сигналу. Це, у свою чергу, дозволяє зменшити кількість викривлень сигналу.

Список використаних джерел:
1. С. Панасенко, “Алгоритмы шифрования” :BHI,2009.-213с.
2. С.Г. Баричев, Р.Е. Серов “Основы Современной Криптографии”: WILEY,2007.-145с.

Д.О. Козеренко, А.Е. Опалько,
Державний університет інформаційно-комунікаційних технологій м. Київ

АДАПТИВНИЙ ЗАХИСТ АКУСТИЧНОЇ ІНФОРМАЦІЇ.

Захист мовної інформації це процес спрямований на запобігання витоку інформації акустичним канало.

Залежно від середовища поширення сигналів і способів їх перехоплення технічні канали витоку мовної інформації можна розділити на [2, с. 134]:

- безпосередньо акустичні - поширення акустичних коливань у вільному повітряному просторі;
- вібраційні (віброакутсичні) - за рахунок впливу звукових коливань на елементи і конструкції будівель, що викликає вібрації конструкцій (труби водопостачання, опалення, кондиціонування тощо) [1];
- акустоелектричні - вплив звукових коливань на допоміжні технічні засоби ОІД (за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу та виникнення електрорушійної сили, або до модуляції струмів, що протікають по цим елементам, за рахунок «мікрофонного ефекту», за рахунок використання «високочастотного електромагнітного нав'язування»);
- оптико-електронні канали - за рахунок приймання та демодуляції відбитого від вібруючих під дією акустичного сигналу поверхонь приміщень (шибок, дзеркал тощо) випромінювання;
- параметричні - вплив звукових коливань на основні та допоміжні технічні засоби (модуляція сигналів у пристроях, які перебувають у приміщеннях де ведуться конфіденційні переговори за рахунок утворення вторинних радіохвиль, «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких змінюються під дією мовного сигналу);

При проведенні робіт із захисту акустичної інформації, на ОІД створюється комплекс технічного захисту інформації від витоку акустичним каналом [2].

Виходячи з цього роботи з технічного захисту інформації доцільно проводити за наступними напрямками:

- захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами;
- захист інформації від витоку акустоелектричними та параметричними каналами;
- захист інформації від витоку через закладні пристрої.

При цьому необхідно враховувати частотний розподіл мови. Це означає, що кожна форманта повідомлення вносить свій конкретний вплив на загальну характеристику мовленевого повідомлення [3] (табл. 1).

Активні системи захисту акустичної інформації повинні бути адаптовані до такого частотного розподілу.

В цьому і полягає сутність побудови адаптивної системи захисту акустичної інформації.

Таблиця 1 Вклад -ой частотної смуги в сумарну розбірливість

Середньогеометричні частоти октавних смуг, Гц	Вклад -ой частотної смуги в сумарну розбірливість	Середньогеометричні частоти (ключових смуг)	Вклад -ой частотної смуги в сумарну розбірливість
125	0.023	113	0.023
250	0.076	230	0.038
500	0.175	330	0.058
1000	0.220	439	0.071
2000	0.234	559	0.064
4000	0.197	692	0.064
8000	0.075	839	0.060
		1002	0.051
		1184	0.053
		1392	0.054
		1634	0.061
		1918	0.056
		2253	0.051
		2652	0.047
		3132	0.045
		3714	0.042
		4437	0.045
		5360	0.044
		6549	0.039
		8079	0.025
		10140	0.008

Список використаних джерел:

1. Методи та засоби захисту інформації. В 2-х томах / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко, Під ред. В.А.Хорошко. – К.: Арий, 2008.– Том ІІ. Інформаційна безпека. – 344 с.

2. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

3. Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами: НД ТЗІ 2.3-017-08. – К.: ДССЗЗІ України, 2008. – 18 с.

Б.В. Чабан, А.В. Інюшев
Державний університет інформаційно-комунікаційних технологій м. Київ

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ НА ОСНОВІ КОМПЛЕКСУВАННЯ ДАНИХ.

Виток інформації технічними каналами є основною загрозою інформації на об’єктах інформаційної діяльності. Одним з таких технічних каналів є матеріально-речовий канал. Дослідження чинників, що сприяють витоку інформації матеріально-речовим каналом, є підґрунтям для організації надійної протидії таким загрозам інформації.

Матеріально-речовий канал витоку інформації є специфічним. Це пов’язано зі специфікою джерел і носіїв інформації у порівнянні з іншими технічними каналами. Джерелами і носіями інформації в ньому є суб'єкти (люди) і матеріальні об'єкти (макро і мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Витік інформації в цих каналах супроводжується фізичним переміщенням людей та матеріальних тіл з інформацією за межами контрольованої зони[1]. Перенесення інформації в цьому каналі за межі контрольованої зони можливо наступними суб'єктами і об'єктами:

- співробітниками організації;
- сторонніми особами (злочинцями);
- повітряними масами атмосфери;

Ці носії можуть переносити всі види інформації: семантичну, ознакову а також демаскуючі речовини. Приймачі інформації цього каналу досить різноманітні. Це експерти зарубіжної розвідки або конкурента, прилади для фізичного та хімічного аналізу, засоби обчислювальної техніки, приймачі радіоактивних випромінювань та ін. Втрати носіїв з цінною інформацією можливі при відсутності в організації чіткої системи обліку її носіїв.

Для добування інформації матеріально-речовим каналом зловмисник, як правило, використовує кілька шляхів її витоку. Комплексне використання каналів витоку інформації грунтується на наступних принципах:

- комплексируємі канали доповнюють один одного за своїми можливостями;
- ефективність комлексування підвищується при зменшенні залежності між джерелами інформації та демаскуючими ознаками в різних каналах.

Комплексування каналів витоку інформації забезпечує [1]:

- збільшення ймовірності виявлення і розпізнавання об'єктів за рахунок розширення їх поточних ознакових структур;
- підвищення достовірності семантичної інформації і точності вимірювання ознак, особливо у разі добування інформації з недостатньо надійних джерел.

Пропонується для запобігання витоку інформації матеріально-речовим каналом використовувати такий же принцип комплексування різних технічних систем. Це буде сприяти отриманню більшої кількості інформації про стан ОІД де зберігаються матеріальні носії секретної інформації. Відповідно підвищиться ефективність її захисту ніж при використанні, як традиційно, однієї системи захисту.

Так відомо, що для протидії витоку інформації матеріально-речовим каналом використовуються технічні системи охорони, системи відео спостереження, системи контролю та управління доступом на ОІД.

Система відеоспостереження представляє собою програмно-апаратний комплекс, призначений для запису відеоінформації та передачі її до місця перегляду або зберігання [2]. Система контролю і управління доступом призначена для виконання комплексу заходів, спрямованих на обмеження і санкціонування доступу співробітників на територію підприємства, в приміщення і зони обмеженого доступу. Технічна система охорони встановлена на об'єктах охорони, повинна в комплексі з силами фізичної охорони і системою

інженерних споруджень задовольняти сучасним (виходячи з криміногенної обстановки) вимогам по охороні об`єктів охорони від устремлінь потенційного порушника.

Для оцінки усієї комплексної системи захисту пропонується використовувати метод динамічного програмування [3]. Цей метод застосовується до завдань з оптимальною підструктурою, і виглядає як набір підзадач, що перетинаються, складність яких трохи менше вихідної.

У математичному вигляді постановка завдання на вибір оптимального варіанту системи буде виглядати наступним чином (показник ефективність/вартість):

Дано: (*X1* – система відеоспостереження; *X2* – технічна система охорони; *X3* – СКУД) – система ***M.***

Знайти*: К→* *optim* за критерієм (цільова функція):

$$\max\left(\frac{F}{I}\right) = \max\left(\frac{\sum_i f_i}{\sum_i I_i}\right)$$

де:

f – показний корисності *i* – ої реалізації кожної з систем;

I – вартість *i* – ої реалізації системи.

Далі методом повного перебору варіантів систем знайдемо оптимальний склад системи захисту інформації на ОІД від витоку матеріально-речовим каналом. що задовольняє критерію якості виконання функцій при мінімальній вартості системи.

Список використаних джерел:

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.:, 2010. –465 с.

2. Котенко А.М. Запобігання витоку інформації матеріально-речовим каналом за рахунок використання систем відеоспостереження. Сучасний захист інформації. Київ: ДУТ, 2017. № 1. – С. 48 – 52..

3. Котенко А.М., Кітіченко Н.С. Застосування методу динамічного програмування для побудови ефективної системи відеоспостереження. Сучасний захист інформації. Київ: ДУТ, 2020. №1(41) 2020.

Є.О. Куліш,
Державний університет інформаційно-комунікаційних технологій м. Київ

ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМ РАННЬОГО ВИЯВЛЕННЯ DDOS-АТАК

У сучасному бізнес-середовищі стабільність роботи інформаційних систем є критичним фактором успіху. DDoS-атаки (Distributed Denial of Service) є одними з найнебезпечніших кіберзагроз, що можуть спричинити серйозні порушення в роботі підприємств. Вони націлені на перевантаження серверів і мережевої інфраструктури, що призводить до значних фінансових збитків, втрати клієнтів і репутації. Протягом останніх років такі атаки стають все більш складними та важко виявлюваними, що вимагає впровадження новітніх технологій для їх раннього виявлення та нейтралізації. Ця робота спрямована на аналіз методів виявлення DDoS-атак та оцінку їхньої ефективності в різних мережевих середовищах.

DDoS-атаки є однією з найбільш поширених форм кібератак, що націлені на порушення доступності сервісів. Основна мета таких атак — вивести з ладу сервер або мережеву інфраструктуру, шляхом перевантаження її запитами. DDoS-атака здійснюється через велику кількість скоординованих запитів з різних пристроїв (часто скомпрометованих) на один або кілька ресурсів, що призводить до виснаження їхніх обчислювальних або пропускних

можливостей. Це може повністю паралізувати роботу системи, залишивши клієнтів без доступу до сервісів, що призводить до фінансових втрат і пошкодження репутації компанії. Кількість DDoS-атак у першому півріччі 2024 року зросла на 46% порівняно з аналогічним періодом минулого року, досягнувши 445 тисяч у другому кварталі 2024 року. Порівняно з даними за попередні шість місяців (3–4 квартали 2023 року) вона зросла на 34% [1].
Основні типи DDoS-атак включають:

1. **Атаки на рівні мережі:** Вони спрямовані на перевантаження мережевого трафіку великим обсягом запитів.
2. **Атаки на рівні додатків:** Ці атаки націлені на конкретні додатки або сервіси, викликаючи їхню нестабільність або збій.
3. **Атаки протоколів:** Вони використовують вразливості мережевих протоколів для блокування ресурсів.

Ці атаки небезпечні тим, що їх часто важко виявити через великий обсяг легітимного трафіку або віртуалізовані джерела атак, що змушує підприємства інвестувати в спеціалізовані системи для їх виявлення та нейтралізації. Кількість DDoS-атак у першому півріччі 2024 року зросла на 46% порівняно з аналогічним періодом минулого року, досягнувши 445 тисяч у другому кварталі 2024 року. Порівняно з даними за попередні шість місяців (3–4 квартали 2023 року) вона зросла на 34%.

Методи виявлення DDoS-атак:

1. Методи на основі аналізу трафіку

1.1 Фільтрація трафіку (Traffic Filtering)

Цей метод захищає від DDoS-атак через блокування IP-адрес. Система ідентифікує атакуючі адреси та блокує їх, запобігаючи доступу до цілі. Фільтрація підходить для базових атак, коли джерело шкідливого трафіку відоме[3].

Точність виявлення: Висока для відомих атак. Проте, атаки з використанням динамічних IP-адрес (наприклад, ботнети) можуть обходити цю фільтрацію.

Швидкість реагування: Миттєва (від кількох мілісекунд до 1 секунди), оскільки фільтрація відбувається на рівні маршрутизатора.

Переваги: Простота реалізації та швидке блокування відомих джерел атак.

Недоліки: Не ефективний проти складних розподілених атак або нових видів атак, які не зафіксовані у списках фільтрації

1.2 Метод на основі сигнатур (Signature-based detection)

Цей підхід використовує базу даних сигнатур відомих атак. Коли трафік відповідає сигнатурі атаки, система блокує його. Це швидкий метод для виявлення атак, які вже відомі системі[2].

Точність виявлення: Висока для відомих атак, але неефективна проти нових або змінених варіантів атак, для яких немає відповідних сигнатур.

Швидкість реагування: Миттєва (від кількох мілісекунд до 1 секунди), якщо сигнатура вже відома.

Переваги: Швидка реакція на відомі атаки без потреби в додатковому аналізі трафіку.

Недоліки: Потребує постійного оновлення бази даних сигнатур і не працює проти нових атак

1.3 Аналіз аномалій (Anomaly-based detection)

Цей метод виявляє аномалії в мережевому трафіку шляхом статистичного аналізу. Він може виявляти нові типи атак, які не зафіксовані в базі даних сигнатур, але може мати хибні спрацьовування при легітимних змінах трафіку, таких як під час рекламних кампаній[2].

Точність виявлення: Висока, але можливі хибні спрацьовування при легітимних сплесках трафіку.

Швидкість реагування: Від 1 до 2 хвилин, оскільки потрібен час для аналізу даних.

Переваги: Добре виявляє нові типи атак, не потребує оновлення сигнатур.

Недоліки: Може мати хибні спрацьовування при значних коливаннях у нормальному трафіку.

2. Методи на основі алгоритмів навчання

2.1 Машинне навчання (ML)

Методи машинного навчання використовують алгоритми для класифікації мережевого трафіку на основі великих даних. Моделі можуть розпізнавати патерни атак і постійно вдосконалюватися, вивчаючи нові загрози[2].

Точність виявлення: Дуже висока для добре навчених моделей, але можливі помилки при несподіваних змінах у трафіку.

Швидкість реагування: Від 5 до 30 секунд, залежно від складності моделі та обчислювальних ресурсів.

Переваги: Ефективний проти нових та складних атак, автоматично вдосконалюється.

Недоліки: Потребує значних обчислювальних ресурсів та великих наборів навчальних даних.

2.2 Глибоке навчання (DL)

Глибоке навчання є підгрупою машинного навчання, яке використовує складні нейронні мережі для виявлення атак. Цей метод може автоматично виявляти складні патерни в даних та забезпечує вищу точність[2].

Точність виявлення: Висока, особливо для складних сценаріїв.

Швидкість реагування: Залежить від обчислювальної потужності, може варіюватися від кількох секунд до декількох хвилин.

Переваги: Може автоматично навчатися на нових даних та адаптуватися до змін у поведінці трафіку.

Недоліки: Вимагає великої кількості даних для навчання та суттєвих обчислювальних ресурсів.

3. Методи на основі поведінки

3.1 Аналіз трафіку (Traffic Pattern Analysis)

Цей метод ґрунтується на спостереженні за нормальною поведінкою мережевих пристроїв та порівнянні її з поточною активністю. Будь-які відхилення можуть сигналізувати про атаку[2].

Точність виявлення: Висока для повільних або складних атак, але може пропустити швидкі атаки.

Швидкість реагування: Від 1 до 3 хвилин, оскільки аналіз вимагає тривалого спостереження.

Переваги: Добре підходить для виявлення повільних або малопомітних атак.

Недоліки: Повільна реакція на атаки і можливі хибні спрацьовування при атипових змінах у поведінці.

3.2 Аналіз ентропії (Entropy-Based Detection Method)

Цей метод обчислює ентропію, аналізуючи розподіл функцій у пакетах трафіку, як-от IP-адреса джерела, IP-адреса призначення, кількість потоків і номери портів. Наявність аномалій у цих функціях потім локалізується шляхом порівняння значень ентропії із заздалегідь визначеним порогом[2].

Точність виявлення: Висока для атак із великим обсягом трафіку, але низька для малих атак.

Швидкість реагування: Від 1 до 5 секунд — швидка реакція на значні зміни.

Переваги: Легкий у реалізації, швидко реагує на великі атаки.

Недоліки: Не ефективний проти малих атак, що не викликають значних змін у трафіку.

В заключенні можна сказати, що кожен із розглянутих методів виявлення DDoS-атак має свої суттєві недоліки. Хоча вони можуть бути ефективними в деяких випадках, при професійних і комплексних атаках їх індивідуальні результати можуть бути незадовільними. Тому важливо в подальшому розвивати інтеграцію різних методів в єдину систему, що дозволить підвищити ефективність виявлення загроз та зменшити ймовірність пропуску атак.

Перспективи розвитку включають використання штучного інтелекту як для автоматизації процесів виявлення та реагування на атаки, так і для розробки нових алгоритмів аналізу трафіку, здатних виявляти нові патерни атак.

Список використаних джерел:

1. The Hacker News: DDoS Attacks Surge 46% in First Half of 2024, Gcore Report Reveals. [Електронний ресурс]. – Режим доступу: https://thehackernews.com/2024/08/ddos-attacks-surge-46-in-first-half-of.html (дата звернення: 16.10.2024)

2. MDPI : DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges by Kazeem B. Adedeji, Adnan M. Abu-Mahfouz and Anish M. Kurien . [Електронний ресурс]. – Режим доступу: https://www.mdpi.com/2224-2708/12/4/51 (дата звернення: 16.10.2024)

3. DDoS-Guard : Popular Traffic Filtering Methods. [Електронний ресурс]. – Режим доступу: https://ddos-guard.net/blog/traffic-filtering-methods (дата звернення: 15.10.2024)

О.С. Меркулов
Державний університет інформаційно-комунікаційних технологій м. Київ

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ ПРИ ПЕРЕДАЧІ ІНФОРМАЦІЇ СТЕГАНОГРАФІЧНИМИ МЕТОДАМИ

Актуальність теми

Із розвитком цифрових технологій зростає потреба в надійних системах захисту інформації. Стеганографічні методи, які передбачають приховування інформації в різних носіях, таких як зображення, аудіо- та відеофайли, дозволяють забезпечити високий рівень конфіденційності. Однак існуючі методи мають свої недоліки, які можуть бути використані зловмисниками для виявлення та викриття схованих даних. Це викликає необхідність удосконалення систем захисту, що включає оптимізацію алгоритмів приховування, підвищення стійкості до атак та зменшення можливості виявлення стеганографічних сигналів.

Проблематика стеганографії

Стеганографія, як метод приховування інформації, розвивається з метою забезпечення конфіденційності та таємності передачі даних. Однак, незважаючи на її переваги, цей метод має ряд проблем і обмежень, які впливають на ефективність і надійність використання.

1. Низька пропускна здатність

Одна з головних проблем стеганографії — це обмежена кількість інформації, яку можна приховати у носії, не змінюючи його візуальні чи аудіальні властивості. Приховані дані не повинні помітно впливати на якість зображення, відео чи звуку.

2. Стійкість до атак

Стеганографічні методи можуть бути вразливими до різних атак, таких як стегоаналіз, який спеціалізується на виявленні прихованих даних. Зловмисники можуть використовувати алгоритми для аналізу файлів на наявність аномалій або модифікацій, що дозволяють виявити стеганографічну інформацію.

3. Обмеження на носії інформації

Стеганографія залежить від типу носія інформації. Наприклад, зображення, аудіо чи відео мають різні можливості для приховування даних. Вибір носія впливає на кількість інформації, яку можна приховати, і на рівень захищеності.

4. Помітність змін

Ефективність стеганографії залежить від здатності зберігати вигляд чи звучання носія незмінним для людського сприйняття після вбудовування інформації. Якщо зміни стають помітними, це може викликати підозри і спонукати до подальшого аналізу носія, що підвищує ризик виявлення.

5. Криптографічна складність

Стеганографія зазвичай використовується разом із криптографією для підвищення рівня безпеки. Однак використання складних криптографічних алгоритмів може збільшити обсяг даних, які потрібно приховати, що створює додаткові проблеми щодо пропускної здатності носія. Крім того, некоректне поєднання криптографії та стеганографії може призвести до зниження загального рівня захисту, що відкриває шлях для атак.

Результати дослідження

В рамках магістерського дослідження було проведено експеримент для оцінки стійкості запропонованого стеганографічного алгоритму до виявлення та модифікацій. Алгоритм був розроблений для приховування текстових повідомлень у зображеннях у форматі PNG за допомогою методу LSB (Least Significant Bit) із додатковим шифруванням за алгоритмом AES перед вбудовуванням.

Результати експерименту:

Непомітність: Візуальний аналіз показав, що зміни у зображеннях після вбудовування інформації були непомітні для людського ока. Показник PSNR для всіх зображень був вище 40 дБ, що свідчить про високу якість зображень після стеганографічних змін.

Стійкість до стегоаналізу: Алгоритми на основі гістограмного аналізу та частотного аналізу не змогли виявити приховані повідомлення у тестових зображеннях. Це підтвердило стійкість розробленого методу до базових технік виявлення стеганографії.

Стійкість до стиснення та фільтрації:

Після стиснення зображень у форматі JPEG із якістю 90%, приховані дані були відновлені успішно у 85% випадків.

Після фільтрації середнім фільтром приховані повідомлення залишилися доступними для відновлення у 80% зображень, що свідчить про відносну стійкість до обробки.

Висновок

Експеримент показав, що запропонований стеганографічний алгоритм має високу стійкість до виявлення за допомогою стандартних методів стегоаналізу. Алгоритм також показав добрі результати при тестуванні на стійкість до компресії зображень і фільтрації. Таким чином, він може бути рекомендований для використання в системах, де необхідно забезпечити приховану передачу конфіденційної інформації без значної втрати якості носія та з високим рівнем захисту від виявлення.

Список використаних джерел:

1. Johnson, N. F., Duric, Z., & Jajodia, S. "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures". Springer, 2022.

2. Katzenbeisser, S., & Petitcolas, F. A. P. "Information Hiding Techniques for Steganography and Digital Watermarking". Artech House, 2021.

М.В. Марченко, Д.І. Назаренко,
Національний авіаційний університет , м.Київ

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ КАНАЛІВ НА ОСНОВІ ТЕХНОЛОГІЇ WI-FI

Побудова гнучких інформаційно-комунікаційних мереж збирання та керування даними є завданням, яке постійно актуальне в різних галузях науки та промисловості. Одним з видів таких мереж є мережі, засновані на бездротових технологіях передачі даних.

Бездротові технології містять в собі величезний потенціал розвитку, що впливає на підвищення стабільності та ефективності функціонування всіх системи країни, що в сукупності визначає соціально-технічну базу модернізації. Основне завдання при проектуванні бездротових локально обчислювальних мереж - рішення проблем

завадостійкості, енергозабезпечення, а також забезпечення належного рівня швидкості передачі і безпеки даних.

Система захисту безпроводової мережі передачі даних на основі технології Wi-Fi.

Захист безпроводової мережі передачі даних на основі технології Wi-Fi заснований на використанні протоколу WPA2. Протокол WPA2 з кодуванням на основі криптоалгоритму AES є обов'язковим у всіх Wi-Fi-пристроях, починаючи з 2006 року і на сьогоднішній день, не показав нічого схожого на подібні уразливості. Для забезпечення належного рівня захисту рекомендується виставляти такі настройки безпеки мережі [1,2]:

- назва SSID має бути унікальним для виключення злому способом словникового перебору;
- в якості методу аутентифікації вибирати режим WPA2-PSK;
- методом шифрування вказувати AES;

Перераховані критерії забезпечують найбільш високий рівень безпеки від злому.

Механізм автентифікації WPA2

WPA2 - це програма сертифікації бездротового зв'язку. Перевагами WPA є підвищений захист даних та контроль бездротових мереж. Суттєвою особливістю є сумісність безлічі бездротових пристроїв на апаратному та на програмному рівнях. Низький рівень безпеки, безсумнівно, довго залишався головних недоліком мережі W-Fi [1,2]. Здійснений на рівні 2 протокол WPA2 оберігає бездротову мережу набагато краще. Управління доступом за цим протоколом в поєднанні з реалізованим протоколом автентифікації IEEE 802.1X на портах, дає змогу зменшити безліч проблем захисту [1,2].

Протокол WPA2 застосовує метод кодування, заснований на більш сильному, алгоритмі шифрування AES, ніж RC4. WPA і WPA2 мають 2 режими автентифікації [1,2]:

- корпоративному (Enterprise);
- персональному (Personal).

У персональному режимі WPA2 із парольної фрази введеної відкритим текстом, генерується 256-розрядний ключ., Ідентифікатор SSID та ключ PSK і довжина останнього разом визначають математичний базис для створення головного парного ключа PMK, який потрібен для ініціалізації чотиристороннього квантування зв'язку та генерації сеансового ключа PTK, для взаємодії клієнтського пристрою з точкою доступу.

Протокол WPA2-Enterprise добре усуває проблеми з розподілом статичних ключів та адміністрування цих ключів. Інтеграція даного протоколу з багатьма корпоративними сервісами аутентифікації дає змогу здійснювати контроль доступу на базі облікових записів.

Автентифікація відбувається між робочою станцією і центральним сервером автентифікації. Точка доступу або бездротового контролер здійснюють моніторинг з'єднання.

Стандарт 802.1X служить базою для режиму WPA2-Enterprise. До основних компонентів аутентифікації 802.1X відносяться клієнтський запит, автентифікатор і сервер автентифікації. Згідно зі специфікацією 802.1X, призначений для користувача запит вважається пристрій, що вимагає доступ до мережі.

Протокол EAP є контейнерним, отже, фактично механізм авторизації виповнюється внутрішніми протоколами.

Сьогодні найбільшу кількість застосувань налічують наступні типи протоколів[1,3]:

- EAP-FAST - дозволяє проводити автентифікацію за логіном-паролем, трансльованого всередині TLS тунелю між відправником і RADIUS- сервером;
- EAP-FAST EAP-TLS - використовує інфраструктуру відкритих ключів (PKI) для автентифікації користувача і сервера (відправника і RADIUS-сервера) через сертифікати, видані довіреним підтверджуючий центр (CA). Вимагає видачі та 32 установки клієнтських сертифікатів на кожен пристрій, тому підходить тільки для керованої корпоративного середовища;
- EAP-TTLS - схожий з EAP-TLS, але при налагодженні тунелю не потрібен клієнтський сертифікат. В такому тунелі, аналогічному SSL-з'єднання браузера, відбувається повторна авторизація;

• PEAP-MSCHAPv2 - схожий на EAP-TTLS в питанні первинного налагодження шифрованого TLS тунелю між користувачем і сервером, що вимагає серверного сертифіката. Далі в такому тунелі здійснюється автентифікація по протоколу MSCHAPv2;

Механізм шифрування WPA2

Протокол WPA2 здійснюється на базі шифрування AES. Потребує апаратної підтримки та характеризується необхідністю величезного обсягу обчислень, які іноді відсутній в старому обладнанні. Для авторизації і підтримки цілісності даних WPA2 застосовує протокол CBC-MAC, а для шифрування даних - режим лічильника CTR.

Повідомлення (MIC) коду цілісності протоколу WPA2 є контрольною сумою і на відміну від WEP і WPA надає цілісність даних для заголовка 802.11. Це дозволяє усунути нападу типу «Packet replay» з метою розшифрування пакетів або компрометації криптографічного інформації. Для розрахунку MIC використовується 128-розрядний вектор ініціалізації IV, для шифрування IV - метод AES і часовий ключ, а на виході маємо 128 розрядний підсумок [1,3]. За допомогою AES і TK шифрується її результат, а потім над останнім результатом і наступними 128 бітами даних знову виконується операція - виключає АБО. Процедура повторюється до вичерпання всій корисного навантаження.

Використовуючи AES і TK шифруються перші 128 біт даних, а тоді понад 128-біт, де результатом шифрування виступає операція - включення АБО. Перші 128 біт даних дають перший 128-розрядний зашифрований блок. Процедура повторюється до повного шифрування всього 128-розрядного блоку даних

Висновок:

Проведено аналіз безпеки бездротових інформаційно-комунікаційних каналів на основі технології WI-FI.

Проаналізована система захисту безпроводової мережі передачі даних. Подано результати огляду механізм автентифікації та шифрування даних в безпроводових мережах..

Список використаних джерел:

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К.: Консум. — 2005. — 576 с.

2. Романова А.І. Телекомунікаційні мережі та управління. – Київ: ВПЦ “Київський університет”, 2003. 247 с.

3. Стандарты Wi-Fi [электронный ресурс] – Режим доступу: http://viconnect.ru/

Р.М. Вільчинський

Державний університет інформаційно-комунікаційних технологій, м. Київ

ВПЛИВ АНОМАЛІЙ НА МЕРЕЖЕВИЙ ТРАФІК

Вступ.

Аномалії в мережевому трафіку можуть викликати значні проблеми. Загалом, аномалія — це щось, що суперечить очікуванням. Наприклад, пошкоджений комутатор може створити несподіваний трафік в іншій частині мережі, або нові коди помилок можуть почати з'являтися, коли сервіс не працює. Виправлення проблем у мережі базується на аномаліях мережі.

Постановка задачі.

В контексті постійного розвитку інформаційних технологій та збільшення трафіку, виникає потреба в кращих методах аналіу трафіку. Існує багато різних причин і методів боротьби з аномаліями. Однак, необхідно провести дослідження з метою визначення першочергових дій для виявлення та усунення аномалій в трафіку

Мета дослідження.

Метою дослідження є аналіз процесу виникнення аномалій в мережовому трафіку та методи боротьби з ними, визначення способів які допоможуть в боротьбі з ними.

Результати дослідження.

В результаті дослідження було встановлено декілька джерел виникнення аномалій, а також описано практики як можна з ними боротись:

- Кіберзагрози. DDoS-атаки, які викликають різке зростання трафіку; спроби несакціонованого доступу, соціальна інженерія.
- Технічні проблеми. Збої в програмному забезпечені; випадкові помилки.
- Інші причини. Людський фактор, який може проявлятись в не правильно налаштованій конфігурації обладнання; різке зростання кількості користувачів або пристроїв.

Кіберзахист в мережевому трафіку є критично важливим аспектом забезпечення безпеки інформаційних систем. Однією з основних стратегій є шифрування, яке забезпечує захист даних під час їх передачі. Використання протоколів шифрування, таких як TLS або SSL, допомагає запобігти перехопленню інформації та несанкціонованому доступу.

Не менш важливими є фаєрволи, які контролюють вхідний і вихідний трафік. Вони дозволяють блокувати шкідливі запити, що може значно знизити ризик витоків даних або атак на мережу. Ще одним важливим аспектом є сегментація мережі. Розділення мережі на окремі сегменти обмежує доступ до критичних ресурсів та зменшує ризик поширення атак.

Окрім технічних засобів, навчання користувачів є важливим елементом кіберзахисту. Освіта співробітників щодо кібербезпеки, а також методів виявлення фішингових атак допомагає запобігти багатьом загрозам ще до того, як вони можуть реалізуватися.

Уникати технічних помилок в обладнанні в мережевому трафіку можна за допомогою ряду стратегій і практик. По-перше, важливо регулярно проводити моніторинг та діагностику мережі, що дозволяє виявляти потенційні проблеми на ранніх стадіях. Це може включати використання систем моніторингу продуктивності та аналізу трафіку, що допомагають виявити аномалії. По-друге, необхідно дотримуватися правильних процедур налаштування обладнання. Застосування стандартних конфігурацій і документування всіх налаштувань допоможе уникнути помилок при оновленні або зміні конфігурації.

Крім того, важливо забезпечити навчання персоналу, відповідального за обслуговування мережі. Регулярні тренінги щодо нових технологій і методів управління обладнанням можуть зменшити ризик технічних помилок.

Висновок.

Кіберзахист у мережевому трафіку та управлінні обладнанням є критично важливими для забезпечення безпеки інформаційних систем. Застосування шифрування, моніторингу трафіку, фаєрволів і сегментації мережі створює багатоетапний захист, що допомагає виявляти та запобігати атакам. Регулярне оновлення програмного забезпечення і навчання персоналу також є важливими елементами для підтримки високого рівня безпеки. Крім того, для уникнення технічних помилок в обладнанні необхідно проводити моніторинг, дотримуватися процедур налаштування та здійснювати регулярні перевірки і обслуговування. Впровадження резервування та відмовостійкості допомагає зберегти безперервність роботи мережі. У сукупності, ці заходи сприяють створенню стабільного та безпечного середовища для передачі даних, що є ключовим для ефективної роботи сучасних інформаційних систем.

Список використаних джерел:

1. Petr Pecha. Science of Network Anomalies. 05.2021. Режим доступу до ресурсу: https://www.progress.com/blogs/science-of-network-anomalies

2. Louis F. DeKoven, Audrey Randall, Ariana Mirian, Gautam Akiwate, Ansel Blume, Lawrence K. Saul, Aaron Schulman, Geoffrey M. Voelker, and Stefan Savage. Measuring security practices and how they impact security. In ACM Internet Measurement Conference, 2019.

В.С. Клівак
Національний авіаційний університет, м. Київ

КІБЕРЗАГРОЗИ ДЛЯ ПРИСТРОЇВ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ ТА МЕТОДИ ЇХ ВИЯВЛЕННЯ

Пристрої віртуальної реальності (VR) набувають все більшого поширення та застосування в різних сферах людського життя: розваги, освіта, промисловість та інші. Однак враховуючи таке широке розповсюдження даної технології це також призводить до зростання занепокоєння щодо ризиків кібербезпеки, пов'язаних з пристроями віртуальної реальності. Відповідно до цього необхідно здійснити огляд загроз, що спрямовані на пристрої віртуальної реальності, та дослідити існуючі способи виявлення несанкціонованого доступу та інших потенційних порушень безпеки.

Пристрої віртуальної реальності стикаються з рядом загроз кібербезпеки, що можуть поставити під загрозу безпеку дані та конфіденційність користувачів. Унікальні особливості систем віртуальної реальності, такі як імерсивне середовище, широке використання датчиків і безперервна передача даних, роблять їх вразливими до певних типів атак. Однією з головних проблем є ризик несанкціонованого доступу до даних користувачів VR, включаючи особисту та біометричну інформацію.

Пристрої віртуальної реальності збирають значний обсяг даних користувачів. Це може бути рух, голос, емоційні реакції, місцезнаходження пристрою та багато іншого. Такі дані є дуже чутливими, і їх компрометація може мати серйозні наслідки для конфіденційності користувача. Наприклад, шкідливе програмне забезпечення може використовуватися для перехоплення компонентів пристрою віртуальної реальності, маніпулюючи віртуальним середовищем, щоб спричинити психологічний або фізичний дискомфорт користувачам. Також атаки «людина посередині» можуть бути спрямовані на мережеві дані VR-гарнітур, що дозволяє зловмисникам перехоплювати або змінювати передану інформацію [1].

Ще однією помітною загрозою є відсутність стандартизованих заходів безпеки для VR-обладнання. Багато з них побудовані таким чином, що користувацький досвід є важливішим за безпеку і це призводить до слабких механізмів контролю доступу та обмеженого шифрування. Зловмисники можуть використовувати ці вразливості для дистанційного керування пристроями або навіть для вбудовування шкідливого контенту. Такі атаки можуть призвести до маніпулювання сенсорним датчиками, що в свою чергу може завдати користувачам шкоди як психологічної так і фізичної.

Виявлення кіберзагроз, спрямованих на VR-пристрої, є складним завданням через відмінності в архітектурі та способах взаємодії цих систем. Одним з ефективних підходів до виявлення загроз є використання систем виявлення вторгнень (IDS), розроблених спеціально для середовищ віртуальної реальності. Ці системи відстежують мережевий трафік і активність пристроїв, виявляючи незвичайні патерни, що вказують на кібератаки [2].

Іншим важливим методом виявлення аномалій у реальному часі можна здійснювати за допомогою моніторингу різних датчиків, таких як камери, гіроскопи, акселерометрами. Моніторинг цих датчиків може допомогти виявити відхилення від очікуваної поведінки, що може свідчити про потенційне втручання або несанкціоноване використання. Останні досягнення в галузі машинного навчання ще більше розширили можливості таких систем виявлення, дозволяючи краще ідентифікувати складні вектори атак.

Методи машинного навчання, особливо глибокого навчання, продемонстрували значний потенціал у виявленні складних кіберзагроз, що можуть бути спрямовані на пристрої віртуальної реальності. Використовуючи великі масиви даних про взаємодію і поведінку користувачів, моделі машинного навчання можна навчити розпізнавати навіть незначні відхилення від нормальної роботи, що в свою чергу дозволяє ефективніше виявляти як існуючі відомі загрози, так і загрози «нульового дня». Для підвищення точності виявлення загроз віртуальної реальності використовуються підходи навчання під наглядом, навчання без

нагляду та навчання з підкріпленням [3].

Інший метод передбачає інтеграцію технології блокчейн для захисту даних віртуальної реальності та забезпечення цілісності. Його можна використовувати для створення незмінного журналу всіх взаємодій і передачі даних у середовищах віртуальної реальності, що ускладнює зловмисникам зміну інформації, не будучи виявленими. Цей метод також забезпечує прозорість і допомагає в аудиті діяльності, що відбувається в програмних системах для віртуальної реальності [4].

Крім того, все більш помітним стає використання рішень для виявлення та реагування на кінцеві точки (EDR), пристосованих для пристроїв віртуальної реальності. Ці рішення забезпечують безперервний моніторинг і аналіз дій кінцевих точок, пропонуючи розуміння потенційних інцидентів безпеки в реальному часі. Інструменти EDR можуть швидко реагувати на виявлені аномалії, допомагаючи зменшити загрози до того, як вони можуть завдати значної шкоди [5].

Використання надійних механізмів автентифікації також відіграє вирішальну роль у зменшенні ризиків безпеки VR. Багатофакторна автентифікація з використанням біометричних даних все частіше досліджується як засіб підвищення безпеки пристроїв віртуальної реальності. Однак, хоча біометрична автентифікація додає додатковий рівень безпеки, вона також викликає занепокоєння щодо зберігання та потенційного зловживання конфіденційними даними користувачів, що підкреслює необхідність ретельного впровадження.

Ще одним перспективним підходом до виявлення загроз у VR-середовищі є застосування поведінкової біометрії. Цей метод передбачає аналіз специфічної для користувача поведінки, такої як патерни рухів, відстеження голови і рук, а також стилі взаємодії, для створення унікального профілю користувача. Будь-яке відхилення від цієї встановленої поведінки може сигналізувати про несанкціонований доступ або зловмисну діяльність. Поведінкова біометрія особливо ефективна в контексті VR, оскільки методи взаємодії настільки індивідуалізовані, що ускладнюють імітацію [6].

Іншими методами, які можна адаптувати для виявлення загроз віртуальної реальності, є «медові токени» та «медові горщики». Токени - це приманкові дані, які здаються цінними, але слугують приманкою для зловмисників. Якщо отримати доступ до токена, він може спровокувати тривогу, сигналізуючи про потенційне порушення. Аналогічним чином, системи, навмисно зроблені вразливими, щоб привабити зловмисників, можуть бути розгорнуті в мережах VR для вивчення поведінки та методів зловмисників, надаючи інформацію, яка може допомогти посилити загальні заходи безпеки [7].

Стрімке поширення технологій віртуальної реальності принесло нові можливості для взаємодії та інновацій, але також створило значні проблеми з кібербезпекою. Пристрої віртуальної реальності є унікально вразливими до кіберзагроз через їхню імерсивну та інтенсивну передачу даних. Протидія цим загрозам вимагає впровадження спеціальних систем виявлення вторгнень, виявлення аномалій за допомогою моніторингу датчиків, передових методів машинного навчання, інтеграції технології блокчейн, поведінкової біометрії, сегментації мережі та стратегій «медового горщика», а також посилених заходів автентифікації. Надаючи пріоритет кібербезпеці при розробці систем віртуальної реальності, можна забезпечити безпечне і надійне впровадження цих технологій у різних секторах.

Список використаних джерел:

1. Krivenko, S.; Rotaniova, N.; Lazarevska, Y.; Karpenko, U. Дослідження системи на уразливість до MITM – атаки за допомогою створення FAKE AP. *Кібербезпека: освіта, наука, техніка.* 2021, №1, С. 29-38.

2. О.С. Ріпний, О.О. Дьяченко, С.В. Малахов, «Особливості функціонування систем IDS та IPS при реалізації спроб несан-кціонованого доступу до корпоративних ресурсів», Матеріали IX міжнародної НТК. 11-12.04.2019, Харків: НТУ «ХПІ», 2019, С. 95.

3. Що таке машинне навчання (Machine learning, ML)? URL: https://thetransmitted.com/adlucem/shho-take-mashynne-navchannya-machine-learning-ml/ (дата звернення: 25.10.2024).

4. AR, Virtual Reality (VR) & Blockchain Technology: Crafting the Future of Immersive Experiences. URL: https://vanarchain.com/en/blog/ar-virtual-reality-blockchain-technology-crafting-the-future-of-immersive-experiences.html (дата звернення: 25.10.2024).

5. Що таке протидія загрозам у кінцевих точках (EDR)? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-edr-endpoint-detection-response (дата звернення: 26.10.2024).

6. M. Chyzhevska, N. Romanovska, A. Ramskyi, V. Venger, M. Obushnyi Behavioral Biometry as a Cyber Security Toolю CEUR Workshop Proceedings. – 2022. – Vol. 3188, Iss. 2, Kyiv, Ukraine. – P. 88–97.

7. Honeypot: поглиблене дослідження. URL: https://proxyelite.info/uk/glossary/honeypot/ (дата звернення: 27.10.2024).

О.О. Шимчук, Н.В. Дем'янов,
Київський національний університет будівництва і архітектури, м. Київ

АНАЛІЗ ТА ЗАХИСТ ВРАЗЛИВОСТЕЙ У ВЕБ-РОЗРОБЦІ

Веб-розробка є критичною складовою сучасних інформаційно-телекомунікаційних систем, однак через широке розповсюдження вона є також вразливою до численних типів атак. Уразливості в архітектурі та коді веб-додатків, зокрема на клієнтській та серверній частинах, відкривають можливості для зловмисників отримати доступ до даних або порушити цілісність роботи сервісу.

SQL-Ін'єкції (SQLi)

SQL-ін'єкція є одним з основних векторів атак на базу даних веб-додатків. Вразливість виникає, коли користувацький вхід некоректно обробляється в SQL-запитах, що дозволяє зловмисникам додавати додаткові SQL-команди в запит до бази даних. Наприклад, рядок username='admin' OR '1'='1' у некоректно захищеному SQL-запиті може привести до отримання всіх даних таблиці Users.

Для захисту від SQL-ін'єкцій рекомендується використовувати підготовлені запити (prepared statements) та ORM (Object-Relational Mapping), які автоматично здійснюють обробку введених даних, виключаючи небезпечні символи. ORM, такі як Sequelize (Node.js) чи Hibernate (Java), дозволяють безпечно взаємодіяти з базою даних, а також мінімізують необхідність писати власні SQL-запити, що знижує ризики помилок, що призводять до SQL-ін'єкцій.

Cross-Site Scripting (XSS)

XSS-атаки використовують можливість виконання зловмисного JavaScript-коду на стороні користувача через введення небезпечних даних у веб-форму, коментарі чи інші елементи вводу. Класичний приклад XSS-атаки: користувач вводить <script>alert('XSS')</script>, і браузер виконує цей код, якщо не використано механізмів захисту.

Для захисту від XSS необхідно застосовувати автоматичне екранування (escaping) HTML-контенту на сервері та на стороні клієнта. Використання бібліотек, як-от DOMPurify, допомагає видаляти небезпечний контент, не порушуючи структуру даних. Також важливе впровадження Content Security Policy (CSP), яка обмежує виконання коду лише із дозволених джерел, і це може запобігти виконанню вбудованих чи небезпечних скриптів.

Cross-Site Request Forgery (CSRF)

CSRF-атаки здійснюються, коли зловмисник змушує користувача виконати небажані дії в системі, де він вже авторизований. Наприклад, запит на зміну паролю може бути

відправлений без відома користувача шляхом підробленої форми або скрипту, що виконується на іншому сайті.

Захист від CSRF передбачає впровадження CSRF-токенів, які генеруються сервером для кожної сесії і додаються до кожного запиту. Такі токени мають бути динамічними та унікальними для кожного користувача, що ускладнює підробку запитів. Більшість веб-фреймворків, включно з Django, ASP.NET, мають вбудовану підтримку CSRF-токенів, що полегшує реалізацію цього захисту.

Захист API

Розширення API стало основою для інтеграції веб-додатків з іншими сервісами, однак публічні API піддаються ризику несанкціонованого доступу, особливо при використанні у відкритих мережах. Однією з основних уразливостей є недостатнє обмеження доступу або слабка аутентифікація. Наприклад, API-ключі, які зберігаються на стороні клієнта, можуть бути перехоплені та використані для масових атак або зловживань.

Щоб мінімізувати ризики, для API-захисту слід використовувати:

- OAuth 2.0 з токенами оновлення, що обмежує час життя кожного токена.
- Технологію API Gateway, яка здійснює аутентифікацію та авторизацію кожного запиту, а також реалізує ліміт запитів (rate limiting), що запобігає спробам перевантаження.
- Використання HTTPS для захищеного з'єднання, щоб уникнути перехоплення даних

Багатофакторна аутентифікація (MFA)

Багатофакторна аутентифікація є важливим елементом захисту авторизаційних систем. Використання лише паролів стало недостатньо безпечним через ризики фішингу та витоку паролів. MFA забезпечує додатковий рівень захисту, вимагаючи підтвердження особистості за допомогою одноразового пароля (OTP) або біометричних даних.

Реалізація MFA на практиці вимагає інтеграції з провайдерами, як-от Google Authenticator, Authy або SMS-провайдерами. Також важливо налаштувати механізми аварійного відновлення доступу, оскільки втрата пристрою для MFA може призвести до блокування користувача.

Шифрування і захист конфіденційних даних

Шифрування є критичним для забезпечення конфіденційності, особливо при зберіганні чутливої інформації, такої як паролі. Один з оптимальних методів – використання алгоритмів хешування (bcrypt, Argon2) для зберігання, які забезпечують високу стійкість до атак підбору.

Також необхідно впровадити шифрування на стороні бази даних, наприклад, за допомогою Transparent Data Encryption (TDE) або через сервіси шифрування в хмарних базах даних. Цей підхід запобігає витоку даних навіть у разі отримання доступу до фізичного сервера чи витоку з бекапу.

Висновки

Безпека веб-додатків є комплексним завданням, що потребує системного підходу та впровадження сучасних захисних технологій. Реалізація методів захисту, таких як підготовлені SQL-запити, CSP, CSRF-токени, багатофакторна аутентифікація та регулярний аудит безпеки, є критично важливими для захисту сучасних веб-додатків від атак. Адаптація до нових методів атак та підтримка актуальності системи захисту – необхідний підхід у сфері інформаційно-телекомунікаційних технологій, що забезпечує надійність та довіру користувачів.

Список використаних джерел:

1. Офіційний посібник OWASP Foundation, Google Developers. Content Security Policy (CSP), Стандарт ISO/IEC 27001:2022, Mitre Corporation. Common Vulnerabilities and Exposures (CVE)

Ю.М. Якименко, Д.А. Поляков,
Державний університет інформаційно-комунікаційних технологій, м. Київ

МЕТОДИЧНІ ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД СУЧАСНИХ ЗАГРОЗ

У сучасному світі інформаційні ресурси стають дедалі більш уразливими до різноманітних загроз, таких як кібератаки, витоки даних та зловмисне програмне забезпечення. Захист інформаційних систем вимагає комплексного підходу, який поєднує технологічні, організаційні та людські аспекти. Метою даного дослідження є аналіз сучасних методичних підходів до захисту інформаційних ресурсів і оцінка їх ефективності.

Серед сучасних загроз інформаційній безпеці і особливо до інформаційних ресурсів будь-якої організації наукові дослідники визначають:

- Кібератаки, коли зловмисники використовують різноманітні техніки, такі як фішинг, зловмисні програми та DDoS-атаки, щоб отримати доступ до інформаційних ресурсів.
- Витоки даних, які часто пов'язані з недотриманням політик безпеки або недостатнім контролем доступу.
- Внутрішні загрози: можуть бути як навмисними (зловмисні співробітники), так і ненавмисними (помилки при обробці даних).

Для захисту інформаційних ресурсів використовуються різні методичні підходи, які приводять до технологічних і організаційних рішень.

Серед основних технологічних рішень для захисту інформаційних ресурсів можна виділити:

- Системи виявлення та запобігання вторгнень (IDS/IPS): ці системи аналізують трафік та можуть виявляти та блокувати підозрілі дії [1].
- Шифрування даних: використання шифрування для захисту конфіденційної інформації як під час зберігання, так і при передачі [2].

Організаційні аспекти захисту інформаційних ресурсів включають:

- Політики безпеки: розробка чітких політик щодо обробки та зберігання інформації, а також навчання співробітників (відповідно до вимог ДСТУ ISO/IEC 27001).
- Моніторинг та аудит: регулярний моніторинг систем та проведення аудитів для виявлення вразливостей.

Слід відзначити, що незважаючи на технологічні рішення, людський фактор залишається ключовим аспектом в питаннях захисту інформації. Як показує практика, вплив людини на захист інформації від різних загроз становить до 75% з усіх наступних випадків: несанкціонований доступ – 2%; — укорінення вірусів – 3%; — технічні відмови апаратури мережі – 20%; — цілеспрямовані дії персоналу – 20%; — помилки персоналу (недостатній рівень кваліфікації) – 55%. Навчання співробітників, усвідомлення ризиків і культура безпеки є критично важливими для забезпечення захисту інформаційних ресурсів [3].

Таким чином, захист інформаційних ресурсів є складним і багатогранним процесом, що вимагає інтеграції технологічних, організаційних і людських факторів. Сучасні загрози вимагають постійного вдосконалення методичних підходів і адаптації до нових викликів. Перспективи дослідження включають розвиток нових технологій захисту, таких як штучний інтелект для виявлення загроз, а також удосконалення навчальних програм для співробітників.

Список використаних джерел:

1. Stallings, W., & Brown, L. (2012). Computer Security: Principles and Practice. Pearson.
2. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
3. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.

М.О. Дроголо,
Державний університет інформаційно-комунікаційних технологій, м. Київ

ЛІТІЄВІ БАТАРЕЇ ФІРМИ ZTE, ЯК НАЙКРАЩЕ РІШЕННЯ ДЛЯ ПІДТРИМКИ ПРАЦЕЗДАТНОСТІ БАЗОВИХ СТАНЦІЙ ПІД ЧАС ДОВГОТРИВАЛОГО ВІДКЛЮЧЕННЯ ЖИВЛЕННЯ

Анотація

У цій тезі розглядається застосування літієвих батарей виробництва ZTE для забезпечення стабільної роботи базових станцій стільникового зв'язку під час тривалих відключень електроенергії. Відмічено переваги літієвих батарей порівняно з іншими типами акумуляторів, такі як тривалий термін служби, енергоефективність, швидкість заряджання та стійкість до умов високих і низьких температур. Аналізуються також можливості зниження витрат на обслуговування базових станцій і підвищення надійності мобільного зв’язку за рахунок впровадження рішень від ZTE.

Мета і завдання

Мета – визначити ефективність використання літієвих батарей ZTE як резервного джерела живлення для базових станцій мобільного зв’язку під час тривалих відключень електроенергії.

Завдання:

1. Проаналізувати основні технічні переваги літієвих батарей ZTE.
2. Дослідити особливості використання літієвих батарей у контексті експлуатації базових станцій.
3. Визначити економічні вигоди від застосування літієвих батарей ZTE у порівнянні з іншими рішеннями для резервного живлення.
4. Оцінити перспективи застосування таких рішень в умовах української інфраструктури.

Виклад основного матеріалу

Переваги літієвих батарей ZTE для базових станцій

1. Тривалий термін служби і циклічність Літієві батареї ZTE відомі своєю довговічністю та великою кількістю циклів зарядки-розрядки, що забезпечує ефективну роботу упродовж 10–15 років. Це значно перевищує тривалість роботи традиційних свинцево-кислотних акумуляторів, що мають меншу циклічність і швидше втрачають ємність. У випадку з базовими станціями, де резервне живлення може часто використовуватися, довговічність літієвих батарей ZTE є вагомою перевагою.

2. Швидкість заряджання Літієві батареї ZTE забезпечують швидкий процес заряджання, що є критично важливим для базових станцій у періоди нестабільного енергопостачання. Завдяки цьому батареї можуть швидше набрати потрібний рівень заряду для повторного використання під час наступного блекауту, знижуючи ризик відключення станцій через недостатній заряд.

3. Широкий температурний діапазон Літієві батареї ZTE мають високу стійкість до змін температури, що дозволяє використовувати їх в екстремальних умовах, характерних для українського клімату. Вони зберігають працездатність як при низьких зимових температурах, так і в умовах літньої спеки, що забезпечує надійність роботи базових станцій у різних регіонах країни.

4. Менша потреба в обслуговуванні Літієві батареї мають менші вимоги до обслуговування у порівнянні зі свинцево-кислотними акумуляторами. Вони не потребують регулярного доливання електроліту та мають систему управління батареями (BMS), яка автоматично контролює стан акумулятора, знижуючи витрати на технічне обслуговування базових станцій.

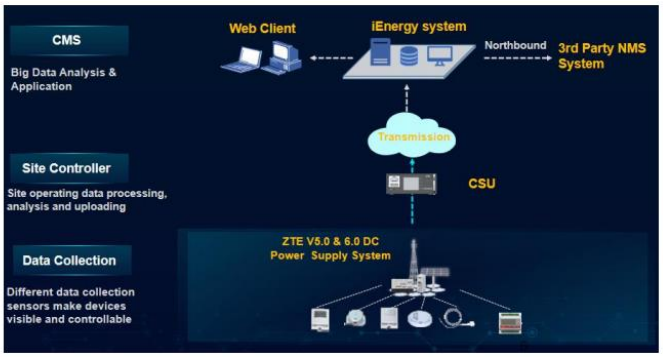

Рис 1. Архітектура системи моніторингу

5. Екологічність та безпека Батареї ZTE виготовлені з екологічно безпечних матеріалів і мають мінімальні шкідливі викиди в процесі експлуатації. Також вони менш схильні до витоку електроліту та загоряння, що забезпечує безпечні умови експлуатації для персоналу.

Недоліки та обмеження

1. Висока початкова вартість Літієві батареї є більш дорогими у порівнянні з традиційними акумуляторами, що може вимагати значних інвестицій на початковому етапі впровадження. Однак, з огляду на тривалість експлуатації та низькі витрати на обслуговування, літієві батареї часто є вигіднішими у довгостроковій перспективі.

2. Необхідність у належній системі вентиляції Для оптимальної роботи літієвих батарей потрібна хороша вентиляція, що забезпечує розсіювання тепла під час зарядки та розрядки. Це вимагає додаткових заходів щодо облаштування місць їх розміщення, особливо у випадку використання на великих базових станціях.

Економічна вигода та ефективність

Хоча літієві батареї ZTE є дорожчими на етапі придбання, їхні технічні характеристики дозволяють значно знизити витрати на експлуатацію та обслуговування. У разі довготривалого відключення електроенергії, такі батареї забезпечують більшу стабільність зв’язку і зменшують ризики відключення, що особливо важливо в умовах критичної інфраструктури. За рахунок довговічності та низьких експлуатаційних витрат ці батареї є економічно вигідним рішенням для телекомунікаційних компаній, які прагнуть мінімізувати ризики збоїв у роботі мережі.

Висновок

Літієві батареї ZTE є ефективним рішенням для підтримки працездатності базових станцій стільникового зв’язку під час тривалих відключень електроенергії. Їхні переваги включають високу циклічність, швидке заряджання, стійкість до температурних коливань і низькі витрати на обслуговування. Хоча вартість літієвих батарей вища порівняно з іншими типами акумуляторів, вони є економічно обґрунтованими у довгостроковій перспективі, що робить їх найкращим вибором для телекомунікаційних операторів. Успішне впровадження таких батарей сприятиме стабільній роботі мобільної інфраструктури України в умовах нестабільного енергопостачання.

Список використаних джерел:

1. Офіційний сайт ZTE Corporation: https://zte.com.

2. Дослідження ринку резервного живлення для телекомунікаційної інфраструктури (2023).https://pro-consulting.ua/base/analiz-rynka-ukrainy?level1=tele&level2=params&page=3&stat=1

3. Аналітичні матеріали щодо енергоефективності та впливу літієвих батарей на безперебійність мобільного зв’язку.

4. Звіт Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації за 2023 рік. https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=2972&language=uk

Б.М. Зерницький
Державний університет інформаційно-комунікаційних технологій м. Київ

МЕТОДИ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

У сучасних умовах, системи електронного документообігу (СЕДО) стали основою бізнес-процесів багатьох організацій, забезпечуючи швидкість, ефективність та зручність в управлінні документами. Однак зростаючий обсяг електронних даних вимагає підвищеної уваги до питань безпеки. Від вразливостей СЕДО залежить як конфіденційність інформації, так і цілісність бізнес-процесів.

Проблематика захисту СЕДО

Система електронного документообігу — це програмне забезпечення, яке дозволяє автоматизувати процес створення, зберігання, обробки, передачі та пошуку документів в електронному форматі. Системи електронного документообігу підлягають різноманітним кіберзагрозам. Серед найбільш поширених можна виділити:

1) Неавторизований доступ до систем електронного документообігу. Даний тип загроз несе велику небезпеку, оскільки вона може мати руйнівні наслідки для організації. Зловмисники можуть отримати доступ до чутливих документів і даних через різноманітні методи, включаючи фішинг, де використовуються підроблені електронні листи для збору облікових даних користувачів. Також часто застосовуються атаки "грубої сили", при яких зловмисники намагаються вгадати паролі, використовуючи автоматизовані інструменти. Крім того, вразливості в програмному забезпеченні можуть бути використані для отримання доступу до системи без необхідних облікових даних.

2) Загроза цілісності документів. Це є серйозною загрозою для СЕДО, оскільки будь-яка несанкціонована зміна чи модифікація інформації може призвести до серйозних наслідків, включаючи втрату довіри з боку клієнтів і партнерів, юридичні наслідки та фінансові збитки. Зловмисники можуть використовувати різноманітні методи, такі як шкідливе ПЗ, для зміни вмісту документів, а також маніпулювати електронними підписами, щоб зробити підроблені документи виглядати легітимними. Це може включати як навмисні дії, так і випадкові помилки співробітників, які без належної підготовки можуть втрутитися в критичні документи.

3) Внутрішні загрози. Загрози в системах електронного документообігу становлять серйозну небезпеку, оскільки вони можуть виникати від співробітників, які мають законний доступ до інформації та системи. Це може включати як умисні дії, такі як крадіжка даних або саботаж, так і неумисні помилки, які можуть призвести до компрометації важливих документів. Наприклад, співробітник може випадково надіслати конфіденційний документ сторонній особі або помилково видалити важливу інформацію.

Методи захисту СЕДО від неавторизованого доступу

Для входу в систему електронного документообігу користувач обов’язково має пройти процес аутентифікації, який підтверджує його право доступу до даних. Найпростішим способом аутентифікації є пароль, однак використовуються також фізичні ключі на зразок USB-токенів чи біометричні дані, як-от відбиток пальця. Кожен із цих методів забезпечує певний рівень безпеки, але має власні ризики: наприклад, паролі можуть бути вразливі до підбору, а фізичні ключі — загублені чи викрадені.

Найбільш надійним методом аутентифікації вважається біометрична перевірка, яка базується на унікальних фізичних характеристиках користувача, таких як відбиток пальця, сітківка ока або голос. Вона надає високий рівень безпеки, адже біометричні дані майже неможливо підробити. Однак такий підхід потребує технічного забезпечення, яке підтримує зчитування біометричних показників, що може підвищити вартість впровадження та експлуатації СЕДО.

Для підвищення захисту використовуються багатоетапні методи аутентифікації, які об’єднують кілька кроків, наприклад, комбінацію пароля з USB-ключем або пароля з біометричним параметром. Такий підхід значно ускладнює несанкціонований доступ,

оскільки навіть при компрометації одного способу залишається ще один бар'єр для входу. Користувач проходить кожен етап по черзі, що дозволяє системі максимально надійно перевірити особу. Використання кількох етапів підвищує захищеність, але може ускладнити процес входу для співробітників і потребує надійного зберігання ключів і управління доступом.

Біометрична перевірка на основі відбитків пальців пальців є унікальною і важко підроблюються. Для зчитування або копіювання відбитку потрібне обладнання високої точності. Просте сканування чи фото відбитка недостатнє – потрібно створити об'ємну структуру поверхні пальця. Однак для обходу цього, зловмисники намагатимуться створити муляж пальця, наприклад, використовуючи відбитки, залишені на поверхні, але для успішного обходу потрібно мати доступ до складного процесу створення силіконових чи гелевих форм, що може бути невиправдано складним або неточним. Але в той же час, сучасні сканери використовують не лише рельєф поверхні пальця, але й інші фізичні показники, такі як вологість чи температура шкіри, які складно імітувати, що додає рівень захисту.

Розпізнавання обличчя включає аналіз багатьох точок на обличчі, таких як форма носа, відстань між очима, контури підборіддя, що робить його складним для підробки. Для введення в оману системи розпізнавання обличчя зловмисникам знадобилося б високоякісне зображення користувача в 3D-форматі. Створення 3D-маски є дорогим і потребує точного доступу до рис обличчя. Навіть у такому випадку система може додатково перевіряти незначні рухи обличчя, що ускладнює використання статичних зображень чи муляжів.

Сканування райдужної оболонки і сітківки вважається ефективним, оскільки сітківка і райдужна оболонка мають дуже детальні й унікальні структури, які важко підробити. Для їхнього зчитування потрібне інфрачервоне освітлення і спеціальне обладнання, яке може фіксувати тонкі деталі очного яблука. Відтворення такої структури потребувало б доступу до оригінальних зображень ока користувача з високою роздільною здатністю та спеціальних пристроїв, що здатні імітувати структуру сітківки. Сучасні системи здатні використовувати ідентифікацію в умовах низької освітленості, що додатково ускладнює створення точних копій.

Висновок:

Таким чином, для захисту СЕДО для від неавторизованого доступу можна застосовувати різноманітні методи аутентифікації, включно з паролями, фізичними ключами (USB-токени), а також біометричними даними (відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки). Біометрична аутентифікація є найнадійнішою, оскільки базується на унікальних фізичних характеристиках користувача, що значно ускладнює підробку. Однак для посилення захисту краще застосовувати багатоетапну аутентифікацію, яка поєднує декілька методів, створюючи додаткові бар'єри для зловмисників. Такий підхід забезпечує високий рівень безпеки, але може вимагати додаткових технічних ресурсів та впливати на зручність використання.

Список використаних джерел:

1. Кукарін О. Б. Електронний документообіг та захист інформації: навч. посіб. / Н. В. Грицяк. – К.: НАДУ, 2015. – 84 с.

2. Wayman J. Biometric Systems: Technology, Design and Performance Evaluation. / A. Jain, D. Maltoni, D. Maio – UK: Springer London, 2005. – P. 370

3. Зибін С.В. Захист інформації від несанкціонованого доступу в системах обробки інформації // Інформаційна безпека. – 2011. – №1.

В.А. Разваляєв
Державний університет інформаційно-комунікаційних технологій, м. Київ

ЗАХИСТ ДАНИХ ВІДЕОСПОСТЕРЕЖЕННЯ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Актуальність. Захист даних, що надходять із систем відеоспостереження, є одним із ключових аспектів забезпечення безпеки в організаціях і критичній інфраструктурі. Несанкціонований доступ до таких даних може призвести до серйозних наслідків, включаючи витік конфіденційної інформації та порушення безпеки фізичних об'єктів. В умовах зростаючої кількості кіберзагроз і хакерських атак, надійний захист даних відеоспостереження є обов'язковим компонентом комплексної системи безпеки.

Метою даної роботи є розгляд основних підходів до захисту даних, що генеруються системами відеоспостереження та оцінка ефективності існуючих методів.

Основні положення. Основні підходи до захисту даних відеоспостереження

1. Шифрування відеопотоку. Одним з основних методів захисту є шифрування даних відеоспостереження як під час їх передачі, так і при зберіганні. Сучасні протоколи шифрування, такі як AES-256, дозволяють надійно захищати дані від перехоплення під час передачі по мережі.

2. Багатофакторна автентифікація (MFA). Забезпечення доступу до системи відеоспостереження лише уповноваженим особам через багатофакторну автентифікацію допомагає значно знизити ризик несанкціонованого доступу. Це може включати поєднання паролів, смс-кодів, біометричних даних та інших факторів.

3. Контроль доступу та управління правами користувачів. Впровадження обмежень доступу до відеоданих є критично важливим. Це означає встановлення чітких ролей і прав доступу для різних категорій користувачів, що мінімізує ймовірність несанкціонованого перегляду або копіювання інформації.

4. Аудит та моніторинг доступу до відеоданих. Запровадження інструментів аудиту та журналів записів доступу до відеоархівів дозволяє відслідковувати кожну дію користувачів і миттєво реагувати на підозрілі дії. Системи моніторингу можуть автоматично сповіщати про аномалії, що вказують на можливі спроби несанкціонованого доступу.

Попри численні методи захисту, системи відеоспостереження залишаються вразливими до кібератак, особливо якщо їхня інфраструктура недостатньо захищена або якщо не використовуються останні оновлення програмного забезпечення. Крім того, інтеграція систем відеоспостереження з іншими інструментами кібербезпеки, такими як штучний інтелект для розпізнавання аномалій, забезпечує нові можливості для ефективнішого захисту.

Висновок. Захист даних відеоспостереження є важливою складовою комплексної інформаційної безпеки. Впровадження шифрування, багатофакторної автентифікації, управління доступом і моніторингу допомагає суттєво знизити ризик несанкціонованого доступу та підвищити безпеку даних. Інтеграція цих методів у комплексну систему кібербезпеки стане основою для побудови надійної і захищеної інфраструктури відеоспостереження.

Список використаних джерел:

1. Відеокамери види та різниця [Електронний ресурс]. – Режим доступу: World Wide Web. – URL:http://www.bezpekacity.com.ua

2. Відеоспостереження і охоронні системи.[Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.install.in.ua

3. Kruegle H. CCTV Surveillance: Video Practices and Technology 2nd Edition — UK: Butterworth-Heinemann 2006, — P. 672

Є.С. Герасименко,
Державний університет інформаційно-комунікаційних технологій, м. Київ

ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ШЛЯХОМ ВИКОРИСТАННЯ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Захист інформації в умовах швидкого розвитку цифрових технологій і зростання обсягів обробки даних на об'єктах інформаційної діяльності є нагальним питанням. Збільшення кількості кіберзагроз і випадків несанкціонованого доступу до конфіденційної інформації ставить перед організаціями завдання вибору ефективних механізмів безпеки. Одним із ключових напрямів забезпечення безпеки є впровадження сучасних систем контролю доступу (СКД), які забезпечують багаторівневий захист інформаційних активів від витоку, зловживання та кібератак.

Складові сучасних систем контролю доступу:

1. Аутентифікація як основа захисту. У сучасних системах контролю доступу використовується багатофакторна аутентифікація (MFA), яка передбачає застосування двох або більше факторів аутентифікації: «те, що знає користувач» (пароль або ПІН-код), «те, що має користувач» (смартфон або смарт-картка) і «те, чим є користувач» (біометричні дані). Зокрема, біометричні системи на основі відбитків пальців, розпізнавання обличчя або сканування райдужної оболонки ока значно підвищують рівень безпеки, оскільки такі характеристики важко підробити чи передати іншій особі.

2. Авторизація та диференціація прав доступу. Важливою складовою СКД є розмежування прав доступу на основі принципу мінімальних привілеїв. Користувачі отримують доступ лише до тих ресурсів, що необхідні для виконання їхніх завдань, а це зменшує ризики витоку інформації та несанкціонованих дій. У більш просунутих системах використовують рольові моделі контролю доступу (RBAC), які надають права доступу залежно від ролі користувача в організації, або моделі на основі атрибутів (ABAC), які враховують додаткові умови, такі як час, місцезнаходження або тип пристрою.

3. Моніторинг активності та управління інцидентами. Сучасні СКД інтегровані із системами моніторингу активності, що дозволяє відстежувати поведінку користувачів у реальному часі. Це допомагає виявляти та реагувати на підозрілі дії, що можуть бути свідченням компрометації облікового запису або внутрішньої загрози. Використання поведінкової аналітики (UBA) дозволяє розпізнавати аномалії, що відхиляються від типових дій користувачів. Наприклад, спроба доступу до системи з нових місць або незвичний час входу можуть свідчити про можливе зловживання обліковими даними.

4. Інтеграція з системами штучного інтелекту (ШІ). Інтеграція СКД із ШІ дозволяє використовувати алгоритми машинного навчання для адаптивного підходу до безпеки, які вдосконалюються з досвідом і стають точнішими у виявленні загроз. Такі системи можуть автоматично коригувати налаштування контролю доступу, блокувати підозрілі спроби входу та оптимізувати механізми моніторингу на основі даних про поведінкові патерни користувачів. Використання ШІ у СКД знижує навантаження на адміністраторів систем, підвищуючи точність і швидкість реагування на інциденти.

5. Інтеграція із засобами кібергігієни. Поряд із впровадженням СКД, важливим аспектом є навчання користувачів і підтримка кібергігієни. Більшість витоків даних виникають через людський фактор, тому навчання співробітників базовим правилам безпеки, як-от розпізнавання фішингових атак або безпечне управління паролями, є ключовим елементом у забезпеченні захисту інформаційних об'єктів.

Виклики та перспективи розвитку СКД

Інформаційна безпека залишається сферою, що постійно змінюється під впливом нових загроз та технологій. Сучасні СКД стикаються з викликами, як-от необхідність обробки великих обсягів даних, забезпечення сумісності з різними IT-системами, а також дотриманням норм конфіденційності. З розвитком технологій штучного інтелекту і поведінкової аналітики

очікується, що майбутні СКД стануть ще більш адаптивними та інтелектуальними, забезпечуючи ефективніший захист інформаційних активів.

Висновок

Сучасні системи контролю доступу є невід'ємною частиною забезпечення інформаційної безпеки на об'єктах інформаційної діяльності. Вони забезпечують комплексний підхід до захисту даних через використання багатофакторної аутентифікації, розмежування прав доступу, моніторинг і аналіз поведінки користувачів, а також завдяки інтеграції зі штучним інтелектом. Перспективи розвитку СКД вказують на важливість адаптивних і самонавчальних систем, які будуть здатні оперативно реагувати на нові виклики та зменшувати ризик кібератак у сучасних умовах зростання кіберзагроз.

Список використаних джерел:

1. Stallings W. Cryptography and Network Security: Principles and Practice. – UK: Pearson, 2020. –P. 768

2. Bishop M. Computer Security: Art and Science. – USA: Addison-Wesley, 2018. – P. 1440

А.П. Злотковський

Київський національний університет будівництва та архітектури, Київ, Україна

ПСИХОЛОГІЧНИЙ АСПЕКТ КІБЕРВТРУЧАНЬ: ВИВЧЕННЯ ПОВЕДІНКИ КОРИСТУВАЧІВ ПІД ЧАС АТАК

Кібербезпека сучасних інформаційних систем залежить не тільки від технологій, але й від людського фактора, зокрема від поведінкових реакцій користувачів у кризових ситуаціях. Вивчення психологічного аспекту кібервтручань, а саме поведінки користувачів під час атак, є надзвичайно важливим для покращення систем протидії загрозам. Актуальність цього дослідження зумовлена збільшенням складності кібератак, зокрема фішингових, соціальної інженерії та шахрайства, що використовує психологічні маніпуляції.

Основні фактори поведінкових реакцій

Дослідження показують, що під час виявлення загрози користувачі часто втрачають здатність діяти раціонально, що призводить до поширення помилкових рішень. Наприклад, при кібератаці з використанням фішингу, попри численні попередження, до 50% користувачів все ще взаємодіють із шкідливими посиланнями та документами [1]. Основними факторами, що впливають на поведінку, є рівень обізнаності, здатність справлятися зі стресом, а також рівень довіри до засобів захисту інформації. Вивчення цих аспектів допомагає знижувати ймовірність ризиків за рахунок правильної побудови політик кібербезпеки та організації навчання користувачів.

Соціальна інженерія та її вплив на прийняття рішень

Соціальна інженерія є небезпечною через використання маніпулятивних тактик, що сприяють успішності кібератак. Часто зловмисники використовують методи соціальної інженерії для стимулювання користувачів до небезпечних дій, таких як передача конфіденційної інформації чи завантаження шкідливих файлів. Прикладом є випадок атаки на компанію X у 2021 році, коли зловмисники змогли отримати доступ до корпоративних ресурсів завдяки фальшивим запитам нібито від імені адміністратора системи, що підтверджує вразливість користувачів до таких методів [2].

Роль стресу та адаптивної поведінки

Відсутність навичок контролю емоцій може впливати на ефективність дій під час інциденту. Дослідження поведінки в умовах стресу демонструють, що більше 40% користувачів допускають помилки через паніку, особливо під час швидко розвиваючих атак. Запровадження регулярних тренінгів і симуляцій дозволяє знизити кількість помилок,

спричинених панікою, та покращує здатність користувачів до прийняття обґрунтованих рішень. Результати звіту компанії IBM показали, що проведення регулярних тренінгів з кібербезпеки знижує ймовірність успішних фішингових атак на 27% завдяки підвищенню обізнаності та здатності співробітників до реагування в умовах стресу [3].

Психологічні тренінги та кіберстійкість

Одним із перспективних методів зниження ризиків є психологічні тренінги для підвищення кіберстійкості. Такі тренінги включають навчання з розпізнавання соціальної інженерії, вправи з контролю емоцій, моделювання кібератак, що дозволяє користувачам краще розуміти, як діяти під час інциденту. За даними досліджень, компанії, які впроваджують тренінги, знижують рівень успішності фішингових атак до 70%, що вказує на ефективність інтеграції психологічних методів у підготовку користувачів [4].

Отже, психологічний аспект поведінки користувачів у кіберсередовищі є одним із ключових факторів у запобіганні кібервтручанням. Вивчення поведінкових реакцій користувачів та їх схильності до паніки й маніпуляцій під час атак дозволяє не лише знизити ймовірність помилок, а й підвищити загальну кіберстійкість організації. Інтеграція психологічних методів, таких як навчання з розпізнавання соціальної інженерії та тренінги з адаптації до стресових ситуацій, у програми підготовки користувачів значно знижує ризик успішних кібератак, зокрема фішингових.

Подальші дослідження в області психологічної кіберстійкості мають великий потенціал для розробки інноваційних підходів до захисту інформаційно-телекомунікаційних систем. Вони сприяють створенню ефективних методик навчання, що враховують як технічні, так і людські фактори, підвищуючи готовність користувачів до дій у складних умовах. Такий комплексний підхід є важливою інвестицією в довгострокову безпеку та стійкість організацій до сучасних кіберзагроз.

Список використаних джерел:

1. McAfee’s 2023 Scam Study Results. URL: https://www.mcafee.com/en-gb/consumer-corporate/newsroom/press-releases/2023/20231108.html (дата звернення: 28.10.2024).

2. Cyber Attack on X Company. ZDNet, 2021. URL: https://www.zdnet.com/article/hacked-my-twitter-user-data-is-out-on-the-dark-web-now-what/ (дата звернення: 28.10.2024).

3. Cost of a Data Breach, 2022. URL: https://www.ibm.com/security/data-breach (дата звернення: 28.10.2024).

4. Analysing Security Training Impact: Effectiveness of Security Awareness Training, 2023. URL: https://www.microminderc s.com/blog/effectiveness-of-security-awareness-training#:~:text=Effective%20security%20awareness%20training%20is,of%20security%20within%20the%20organisation. (дата звернення: 28.10.2024).

В.В. Вишнівський, А.В. Гоменюк,
Державний університет інформаційно-комунікаційних технологій, м. Київ

ДОСЛІДЖЕННЯ БЕЗПЕКИ СИСТЕМИ ПРОГНОЗУВАННЯ ЗАХВОРЮВАНЬ НА ОСНОВІ ТЕХНОЛОГІЇ BIG DATA

Анотація. Смертність від серцево-судинних захворювань (ССЗ) досягає рекордних показників у глобальному масштабі. Вади серця, серцева недостатність, інфаркт та інсульт, пов’язані з патологією серцево-судинної системи, є основними чинниками інвалідизації та смертності. ССЗ займають провідну позицію у структурі захворюваності в Україні і спостерігається тенденція до їх “омолодження”. Для попередження ССЗ створюються інтелектуальні системи прогнозування захворювань на основі технології Big Data, які дозволяють аналізувати великі обсяги медичних і поведінкових даних для виявлення

тенденцій у розвитку захворювань, визначення факторів ризику та своєчасного виявлення можливих епідемій або спалахів інфекційних захворювань. Але будь-які інтелектуальні системи прогнозування мають вплив кіберзагроз. Тому виникає завдання визначення актуальних проблем безпеки програмних засобів інтелектуальних систем прогнозування захворювань на основі технології Big Data та знаходження шляхів їх усунення.

Ключові слова: інтелектуальні системи прогнозування, Big Data, кібербезпека.

Постановка завдання. Системи прогнозування захворювань на основі технології Big Data дозволяють аналізувати великі обсяги медичних і поведінкових даних для виявлення тенденцій у розвитку захворювань, визначення факторів ризику та своєчасного виявлення можливих епідемій або спалахів інфекційних захворювань, наприклад, BlueDot. Технологія Big Data в прогнозуванні захворювань сприяє ефективнішому моніторингу стану здоров'я населення та допомагає у своєчасному вжитті організації заходів для запобігання серйозних наслідків для системи охорони здоров'я [1, 2]. Але системи прогнозування захворювань на основі Big Data стикаються з рядом проблем кібербезпеки, оскільки вони оперують великим обсягом персональних та конфіденційних даних, які є цікавими для зловмисника. Тому виникає завдання метою якого є визначення актуальних проблем безпеки програмних засобів інтелектуальних систем прогнозування захворювань на основі технології Big Data та знаходження раціональних шляхів їх усунення.

Мета дослідження. Підвищення ефективності безпеки даних в системі прогнозування захворювань та стабільне функціонування технологій Big Data (надійний захист конфіденційних медичних даних, знизити ризики несанкціонованого доступу та забезпечити безпечне функціонування таких систем), що сприятиме зниженню ризиків для пацієнтів, підвищенню довіри до систем охорони здоров'я і забезпеченню точних прогнозів для раннього виявлення та запобігання захворювань.

Результати дослідження. Системи прогнозування захворювань на основі технології Big Data створюються для ефективного аналізу великих обсягів медичних, соціальних та екологічних даних, що дозволяє краще розуміти, передбачати та запобігати різним захворюванням. Загалом, основна мета систем прогнозування захворювань на основі Big Data — це забезпечення більш ефективної системи охорони здоров'я, яка може реагувати на виклики вчасно, попереджувати захворювання, скорочувати витрати та сприяти персоналізованій і доказовій медицині.

Системи прогнозування захворювань на основі технології Big Data забезпечують:

1. Прогнозування та попередження епідемій та спалахів інфекцій на основі аналізу поведінкових, медичних та соціальних даних для виявлення ранніх ознак епідемій. Це дозволяє оперативне реагувати на спалахи інфекційних хвороб, як-от грип, COVID-19 чи інші інфекції, і швидко вживати необхідні заходи.

2. Визначення факторів ризику для хронічних захворювань за допомогою аналізу великих обсягів даних щодо факторів ризику для серцево-судинних захворювань, діабету, раку та інших хронічних хвороб. Це дає можливість персоналізувати підхід до профілактики, надаючи пацієнтам рекомендації щодо здорового способу життя.

3. Оптимізацію ресурсів системи охорони здоров'я, що допомагає медичним установам краще планувати ресурси, такі як кількість медичних працівників, необхідні ліки та обладнання, щоб підготуватися до майбутніх потреб, особливо у випадку очікуваних епідемій або сезонних захворювань.

4. Підтримка прийняття рішень для лікарів та медичного персоналу за допомогою прогнозної моделі на основі Big Data, що забезпечує лікарів точними рекомендаціями щодо вибору оптимальних методів діагностики та лікування на основі поточних даних, історії хвороби пацієнта та найновіших досліджень.

5. Скорочення витрат на охорону здоров'я завдяки ранньому виявленню ризиків і попередженню захворювань такі системи можуть значно зменшити фінансові витрати на лікування, зокрема за рахунок уникнення ускладнень, що можуть потребувати додаткових медичних ресурсів.

6. Моніторинг стану здоров'я населення дозволяє постійно відстежувати здоров'я населення в реальному часі. Це допомагає медичним установам отримувати своєчасні дані про стан здоров'я населення, зокрема для моніторингу хронічних хвороб, психічного здоров'я тощо.

7. Персоналізація медицини - Big Data дає змогу переходити до персоналізованої медицини, де кожен пацієнт отримує індивідуальний підхід до лікування та профілактики на основі своїх даних, таких як генетична інформація, спосіб життя та історія хвороб.

8. Дослідження нових захворювань та ризиків завдяки аналізу Big Data можна виявляти нові тенденції у сфері охорони здоров'я, розуміти поширення нових захворювань та виявляти невідомі раніше ризики. Це допомагає науковцям глибше досліджувати захворювання та їхній вплив на населення.

Відомі основні аспекти роботи системи прогнозування захворювань на основі технології Big Data [1, 2 , 3]:

1. Аналіз великих даних для прогнозування

• *Збір даних*: Системи використовують різні джерела даних — електронні медичні записи (EMR), інформацію з мобільних додатків, дані з соціальних мереж і навіть дані про навколишнє середовище (наприклад, рівень забруднення повітря).

• *Інтеграція даних*: Об'єднання даних з різних джерел дозволяє створити більш повну картину здоров'я населення. Це важливо для виявлення кореляцій між зовнішніми факторами та станом здоров'я людей.

2. Машинне навчання та штучний інтелект

• *Алгоритми машинного навчання:* аналізують накопичені дані, щоб виявляти приховані закономірності та чинники, які можуть впливати на поширення захворювань.

• *Прогностичні моделі*: за допомогою моделей прогнозування можна оцінити ймовірність виникнення захворювання у конкретної особи або групи, а також прорахувати ймовірність розвитку ускладнень у хронічних хворих.

Але системи прогнозування захворювань на основі Big Data стикаються з рядом проблем кібербезпеки. Тому дослідження безпеки системи прогнозування захворювань на основі технології Big Data є важливим аспектом для забезпечення конфіденційності даних, захисту від кіберзагроз і дотримання етичних стандартів.

Існують такі виклики та ризики для системи прогнозування захворювань на основі Big Data:

• *Захист даних:* велика кількість медичних даних вимагає надійного захисту для запобігання витокам та несанкціонованому доступу.

• *Якість даних*: для точного прогнозування необхідні якісні й структуровані дані.

• *Етичні питання*: використання особистої інформації вимагає згоди пацієнтів і дотримання прав на приватність.

На основі цих викликів та ризиків можна для системи прогнозування захворювань на основі Big Data визначити проблеми кібербезпеки. Ось основні проблеми кібербезпеки, характерні для таких систем:

1. Конфіденційність даних:

• *Незаконний доступ:* Персональні медичні дані пацієнтів, які використовуються для аналізу та прогнозування, є вразливими до несанкціонованого доступу. Злам системи може призвести до витоку конфіденційної інформації, що порушує права пацієнтів на приватність.

• *Анонімізація даних*: У багатьох випадках дані анонімізують, але навіть анонімні дані можуть бути повторно ідентифіковані шляхом комбінування з іншими джерелами даних.

2. Незахищені канали передачі даних:

• *Віддалений доступ*: Дані для Big Data аналізу часто передаються через незахищені канали, що може призвести до перехоплення або втрати даних під час передачі. Наприклад, якщо медичні дані передаються між лікарнею та зовнішніми аналітичними платформами, важливо забезпечити їх шифрування.

• *Надійність інтернет-з'єднання:* У випадку втрати або компрометації з'єднання система може залишитися незахищеною або нездатною підтримувати необхідний рівень кібербезпеки.

3. Фальсифікація даних:

• *Атаки на дані:* Недобросовісні особи можуть намагатися внести зміни в дані або підмінити їх, що може спотворити результати аналізу та прогнози. Такі атаки, як "отруєння даних" (data poisoning), можуть вплинути на алгоритми машинного навчання, порушуючи точність прогнозів.

4. Фішинг та соціальна інженерія:

• *Шахрайські методи*: Хакери можуть використовувати фішинг або методи соціальної інженерії для отримання доступу до систем прогнозування захворювань через користувачів системи. Це можуть бути медичні працівники, аналітики, або навіть пацієнти, що мають доступ до частини системи.

5. Вразливості в програмному забезпеченні:

• *Невиправлені помилки*: Системи Big Data можуть містити вразливості, пов'язані з недопрацьованим програмним забезпеченням або застарілими версіями бібліотек. Невиправлені помилки стають слабкими місцями, через які зловмисники можуть отримати доступ до системи.

• *Атаки на сервери*: Сервери, які обробляють великі обсяги даних, можуть бути вразливими до DDoS-атак, які можуть порушити роботу системи, зробивши її недоступною для лікарів та інших користувачів.

6. Невідповідність вимогам захисту даних:

• *Вимоги щодо конфіденційності:* В різних країнах діють суворі закони, що регулюють захист персональних даних (наприклад, GDPR в ЄС). Недотримання цих вимог може призвести не тільки до фінансових санкцій, а й до втрати довіри користувачів до системи.

• *Невизначеність у правовому полі*: Використання великих даних в охороні здоров'я ще недостатньо врегульоване в деяких країнах, що може створювати юридичні ризики.

7. Внутрішні загрози:

• *Доступ співробітників*: Внутрішні користувачі, такі як співробітники лікарень або аналітичних центрів, можуть мати надмірний доступ до даних або використовувати їх неналежним чином.

• *Недостатнє навчання персоналу*: Працівники можуть ненавмисно створювати кіберризики через незнання або невміння працювати з системами захисту.

8. Використання IoT і мобільних пристроїв:

• *Вразливі точки IoT:* Пристрої Інтернету речей (IoT), які можуть використовуватися для моніторингу пацієнтів і передачі даних у систему Big Data, часто мають низький рівень безпеки і можуть стати точками входу для зловмисників.

• *Мобільні пристрої*: Оскільки мобільні додатки також можуть збирати і передавати дані, вони є вразливими до атак, зокрема вразливості можуть виникати при використанні ненадійних з'єднань або слабких паролів.

Завдяки визначення цих проблеми кібербезпеки для системи прогнозування захворювань на основі Big Data можна визначити основні елементи, які слід врахувати при дослідженні безпеки такої системи, а саме:

1. Оцінка загроз і ризиків

• *Ідентифікація загроз:* Визначення потенційних загроз, таких як несанкціонований доступ, втрати даних, кібератаки (DDoS, фішинг), а також внутрішні загрози (наприклад, зловмисні дії співробітників).

• *Оцінка ризиків:* Аналіз ймовірності виникнення загроз і їх можливих наслідків для системи та даних, які вона обробляє.

2. Конфіденційність даних

• *Захист персональних даних:* Використання шифрування для захисту чутливих медичних даних. Забезпечення відповідності з законодавством (GDPR, HIPAA).

• *Анонімізація та псевдонімізація*: Застосування методів анонімізації для зменшення ризику розкриття особистості пацієнтів у разі витоку даних.

3. Цілісність і доступність даних

• *Забезпечення цілісності:* Використання механізмів контролю версій і аудитів для запобігання несанкціонованим змінам у даних.

• *Доступність системи*: Реалізація заходів для забезпечення доступності системи для легітимних користувачів, включаючи резервне копіювання даних і відновлення після збоїв.

4. Безпека інфраструктури

• *Захист мережі:* Впровадження міжмережевих екранів (firewalls), систем виявлення вторгнень (IDS), та інших засобів для захисту від зовнішніх атак.

• *Контроль доступу*: Використання багатофакторної аутентифікації та ролей для контролю доступу до системи та даних.

5. Моніторинг і аудит

• *Логи і моніторинг*: Ведення журналів доступу та дій користувачів для виявлення аномальної поведінки. Використання інструментів для моніторингу безпеки.

• *Регулярні аудити*: Проведення регулярних перевірок системи безпеки для виявлення вразливостей та оцінки ефективності заходів безпеки.

6. Реагування на інциденти

• *План реагування:* Розробка чітких протоколів для реагування на інциденти безпеки, включаючи виявлення, реагування та відновлення.

• *Тренінги для персоналу*: Проведення навчань для співробітників щодо реагування на інциденти та забезпечення безпеки даних.

7. Етичні аспекти

• *Відповідальність за дані*: Визначення відповідальності за обробку та захист медичних даних, а також етичних норм для використання інформації.

• *Прозорість алгоритмів:* Забезпечення прозорості в алгоритмах прогнозування, щоб уникнути упередженості та дискримінації.

8. Взаємодія з державними та міжнародними органами

• *Співпраця з регуляторами*: Партнерство з державними органами для забезпечення відповідності нормам та стандартам безпеки.

• *Участь у міжнародних ініціативах:* Співпраця з міжнародними організаціями для обміну досвідом і кращими практиками у сфері безпеки.

Висновки:

1. Технологія Big Data в прогнозуванні захворювань сприяє ефективнішому моніторингу стану здоров’я населення та допомагає у своєчасному вжитті заходів для запобігання серйозних наслідків для системи охорони здоров'я.

2. Дослідження безпеки системи прогнозування захворювань на основі технології Big Data має бути комплексним і враховувати всі можливі аспекти, щоб забезпечити надійний захист даних пацієнтів і ефективність системи в цілому.

3. Загалом, системи прогнозування захворювань потребують комплексних рішень для забезпечення кібербезпеки, включаючи шифрування даних, багаторівневу аутентифікацію, регулярне оновлення програмного забезпечення та навчання персоналу.

Список використаних джерел:

1. Серцево-судинні захворювання — головна причина смерті українців. Висновки з дослідження Глобального тягаря хвороб у 2019 році/ [Електронний ресурс] / режим доступу: https://phc.org.ua/news/sercevo-sudinni-zakhvoryuvannya-golovna-prichina-smerti-ukrainciv-visnovki-z-doslidzhennya / (date of access: 20.10.2024)

2. TRENDS OF THE FUTURE: RISKS, OPPORTUNITIES, TASKS Collection of Materials of the Multidisciplinary Scientific and Practical Conference Kyiv, December 23th, 2016/ [Електронний ресурс] / режим доступу: http://futurolog.com.ua/publish/3/Zbirnyk.pdf/ (date of access: 20.10.2024)

3. Scipione CA, Koschinsky ML, Boffa MB. Lipoprotein(a) in clinical practice: New perspectives from basic and translational science. Crit Rev Clin Lab Sci. 2018 Jan;55(1):33-54.

4. Marcovina SM, Albers JJ. Lipoprotein (a) measurements for clinical application. J Lipid Res. 2016 Apr;57(4):526-37.

5. Kostner KM, März W, Kostner GM. When should we measure lipoprotein (a)? Eur Heart J. 2013 Nov;34(42):3268-76.

О.В. Опихайленко
Київський національний університет будівництва і архітектури, м. Київ

АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Інформаційно-телекомунікаційні системи відіграють ключову роль у сучасному світі, проте з кожним роком загроза їх безпеці зростає. З розвитком новітніх технологій, таких як штучний інтелект (ШІ) та блокчейн, з'являються інноваційні методи захисту, що дозволяють протистояти новим видам кіберзагроз. Сьогодні, коли кіберзлочинці застосовують все складніші методи атак, традиційних способів забезпечення безпеки вже недостатньо. Інноваційні рішення стають необхідними не лише для запобігання атакам, але й для їх раннього виявлення та нейтралізації.

Штучний інтелект і машинне навчання набувають поширення у сфері кібербезпеки, адже вони дають змогу обробляти великі обсяги даних та виявляти аномальні дії в реальному часі. Системи ШІ здатні виявляти кіберзагрози на ранніх стадіях завдяки навчанню на великих масивах даних, зокрема мережевих логах, поведінкових шаблонах та структурованих даних про загрози. Алгоритми машинного навчання дозволяють створювати моделі поведінки користувачів, які аналізують дії і визначають відхилення від нормальної діяльності, що може свідчити про потенційний злом або несанкціонований доступ. Завдяки цьому вдається мінімізувати час реакції на інциденти безпеки, що, в свою чергу, дозволяє оперативніше розслідувати і нейтралізувати кіберзагрози.

Блокчейн, як технологія, яка забезпечує захист цілісності даних, також знаходить застосування в інформаційно-телекомунікаційних системах. Вона використовується для забезпечення безпеки даних у фінансових та інших транзакціях, а також для автентифікації пристроїв і користувачів. Блокчейн гарантує, що будь-які зміни даних в системі фіксуються, і їх не можна підробити, завдяки використанню децентралізованих алгоритмів. Одним із прикладів використання блокчейну є забезпечення захищеності даних у ланцюгах постачань: інформація про переміщення товарів зберігається у вигляді блоків, і кожна зміна має цифровий підпис. Це запобігає можливим спробам шахрайства, оскільки будь-яке втручання в систему буде зафіксоване. Також блокчейн знаходить своє застосування в системах ідентифікації, адже зберігає дані про користувачів таким чином, що їх неможливо змінити без сліду, що значно підвищує рівень безпеки.

Попри всі переваги, впровадження технологій ШІ та блокчейну пов'язане з певними викликами. Один із них — потреба в потужних обчислювальних ресурсах для навчання моделей ШІ. Інший — складність забезпечення масштабованості блокчейн-технологій. Через велику кількість операцій блокчейн-системи можуть бути повільними, а обсяг даних значно збільшується, що ускладнює їхнє ефективне впровадження. Крім того, самі технології безпеки, такі як ШІ, можуть ставати об'єктом кібератак. Зокрема, хакери можуть застосовувати методи

атак на моделі ШІ, зокрема підробні дані для обману алгоритмів виявлення загроз. Це вимагає розробки додаткових механізмів для забезпечення захищеності самих алгоритмів.

Ще один важливий аспект полягає у законодавчій регуляції використання інноваційних технологій. Наприклад, у багатьох країнах питання зберігання та обробки даних за допомогою блокчейну потребує юридичних роз'яснень, адже традиційні механізми захисту даних не завжди відповідають умовам децентралізованих систем. Схожа ситуація спостерігається і з ШІ: існує необхідність встановлення правових рамок для забезпечення відповідності етичним стандартам, особливо у сфері конфіденційності та захисту даних.

Таким чином, використання ШІ та блокчейн-технологій в інформаційно-телекомунікаційних системах є важливим кроком у забезпеченні їхньої захищеності. Ці технології здатні суттєво покращити надійність, допомогти запобігати новим загрозам та мінімізувати ризики витоку даних. Проте для досягнення ефективності необхідно подолати певні технологічні та юридичні бар'єри, що створює додаткові виклики для впровадження інноваційних методів захисту.

Список використаних джерел:

1. Тарасенко, В. В. Інформаційна безпека в інформаційно-телекомунікаційних системах: навчальний посібник. – Київ: Наукова думка, 2020. – 250 с.

2. Коваленко, О. П. Кібербезпека: концептуальні основи та сучасні виклики. – Львів: Видавництво ЛНУ імені Івана Франка, 2019. – 180 с.

Н.С. Скачко,
студент групи КБ-61, ННІ «Комп'ютерних наук та штучного інтелекту»
ХНУ імені В.Н. Каразіна, Харків, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ КОРИСТУВАЧІВ ТА ДАНИХ У ПЕРСПЕКТИВНИХ МЕРЕЖАХ WEB 3.0

В умовах розвитку технологій Web 3.0 постає питання забезпечення приватності даних користувачів, зокрема у децентралізованих мережах, які є основою цього нового етапу еволюції інтернету. На відміну від попередніх версій Web, які покладалися на централізовані платформи і сервіси, Web 3.0 має на меті надати користувачам більше контролю над власною інформацією та її обробкою, що значно підвищує вимоги до захисту персональних даних.

Приватність даних у Web 3.0 стає складнішою у зв'язку з високою прозорістю транзакцій у блокчейн-мережах, а також потребою зберігати і передавати дані таким чином, щоб вони залишалися захищеними, але доступними для підтвердження відповідних транзакцій. Наприклад, використання технологій блокчейну, таких як zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), забезпечує можливість верифікації даних без розкриття їх змісту, що стає надзвичайно важливим для децентралізованих додатків (DApps). Такі інструменти дозволяють користувачам взаємодіяти в мережі, зберігаючи при цьому високий рівень конфіденційності, оскільки їхні особисті дані залишаються недоступними для сторонніх учасників системи.

Ще одним важливим аспектом для Web 3.0 є децентралізовані ідентифікатори (DID), які дозволяють користувачам самостійно управляти власною ідентифікаційною інформацією, не покладаючись на централізовані органи або інфраструктури. DID сприяють підвищенню анонімності користувачів, дозволяючи здійснювати взаємодію між вузлами мережі, не розкриваючи персональних даних. При цьому забезпечується можливість підтвердження ідентичності завдяки цифровим підписам та криптографічним методам шифрування.

У результаті дослідження виявлено, що технології, такі як zk-SNARKs, децентралізовані ідентифікатори (DID), гомоморфне шифрування та багатосторонні обчислення, є перспективними методами для забезпечення приватності користувачів у мережах Web 3.0. Ці

технології дозволяють користувачам контролювати свої дані та взаємодіяти в децентралізованих системах без ризику розголошення особистої інформації. Проте для їх повномасштабного впровадження необхідно вирішити питання оптимізації обчислювальних витрат і підвищення ефективності, щоб забезпечити конфіденційність і безпеку в новому поколінні інтернету.

Список використаних джерел:

1. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper.

2. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184).

3. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press.

4. Wüst, K., & Gervais, A. (2018). Do you need a blockchain?. In 2018 Crypto Valley Conference on Blockchain Technology (pp. 45-54).

5. Buterin, V. (2013). Ethereum white paper: A next-generation smart contract and decentralized application platform.

Н.О Байдюк, К.В. Зарецька
Київський національний університет будівництва та архітектури, Київ, Україна

ЕТИКА ЗБОРУ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ В СИСТЕМАХ КІБЕРЗАХИСТУ

Збір та обробка персональних даних набуває все більшого значення в кіберзахисті. Етичні правила в цій сфері передбачають дотримання певних принципів, які забезпечують конфіденційність і обмежують втручання в особисте життя людини під час обробки персональних даних. Системи кібербезпеки повинні забезпечувати баланс між захистом організації та повагою до прав і свобод кожного окремого користувача, чиї дані зберігаються та обробляються.

Принципи роботи з особистими даними в системах кіберзахисту:

Принцип прозорості. Користувачі повинні знати, які дані збираються, з якою метою та в якому обсязі. Компанії повинні пояснювати, як вони обробляють дані, зокрема, які дані збираються автоматично та які заходи безпеки використовуються. Дослідження показують, що прозорість підкріплює довіру до компаній і позитивно впливає на загальний рівень кібербезпеки [1].

Обмеження обсягу даних. Етичний підхід вимагає, щоб збір даних обмежувався лише тими даними, які необхідні для досягнення визначених цілей. Персональні дані повинні збиратися та оброблятися в мінімальному обсязі, необхідному для досягнення цілей кібербезпеки. Такий підхід дозволяє уникнути надмірного втручання в особисте життя користувачів і мінімізує ризик порушення приватності [1].

Захист конфіденційності. Конфіденційність є фундаментальним етичним принципом обробки персональних даних. Компанії повинні забезпечити захист інформації від несанкціонованого доступу шляхом використання відповідних методів шифрування та резервного копіювання. Системи, які використовують сучасні методи безпеки, мають менший ризик несанкціонованого доступу до персональних даних [2].

Принцип права на доступ та виправлення. Користувачі мають право знати, які дані про них зберігаються, і вимагати виправлення або видалення застарілої чи невірної інформації. Це зменшує ризик використання некоректних даних, що спричиняє непорозуміння та проблеми як для компаній, так і для користувачів.

Законність обробки. Усі дії, пов'язані з персональними даними, повинні відповідати вимогам законодавства, зокрема Загального регламенту ЄС про захист даних (GDPR), який регулює обробку даних на основі згоди або законних інтересів суб'єкта даних. Недотримання цих вимог може призвести до санкцій і судових позовів проти компанії, а також до втрати довіри клієнтів [2].

Рекомендації для підвищення етичності обробки персональних даних у кіберзахисті:

Розробка політик обробки даних. Рекомендується розробити чітку політику збору, обробки та зберігання персональних даних, що відповідає етичним та правовим стандартам. Це включає в себе встановлення політики прозорості, забезпечення доступу користувачів до інформації та контролю над власними даними.

Регулярний аудит етичності обробки даних. Аудити не лише контролюють відповідність політик компанії етичним принципам і нормам, а й допомагають своєчасно виявляти потенційні ризики та зловживання даними. На думку експертів, регулярні аудити відіграють ключову роль у зміцненні довіри до компаній та підвищенні безпеки кіберсистем [1].

Навчання та підвищення обізнаності працівників. Працівники, які працюють з персональними даними, повинні бути ознайомлені з етичними стандартами, правовими обмеженнями, методами захисту даних та відповідальністю за їх порушення. Це зменшить ризик людських помилок і підвищить загальний рівень кібербезпеки в компанії.[3]

Таким чином, етичний підхід до збору та обробки персональних даних є не лише моральним імперативом, але й ключовим елементом, що лежить в основі комплексної та ефективної системи кіберзахисту. Забезпечення безпеки даних на основі прозорих та етичних принципів допомагає побудувати довіру між організаціями та їхніми користувачами, що, в свою чергу, підвищує стійкість всієї організації до кіберзагроз. Дотримання етичних стандартів при обробці даних допомагає мінімізувати ризик порушення конфіденційності, що має вирішальне значення для захисту прав користувачів і підтримки репутації організації., Отже, організації, які включають етичні принципи у свою стратегію кібербезпеки, не лише зменшують можливість неправомірного використання даних, але й створюють міцний фундамент для довгострокового захисту приватності та інформаційних активів, забезпечуючи безпеку та сталий розвиток у цифровому середовищі.

Список використаних джерел:

1. Бойко В. Д., Василенко М. Д. Кібербезпека та захист персональних даних в ЄС: проблеми цифрового суспільства. *Наукові праці Національного університету «Одеська юридична академія»*. Т. 23 / голов. ред. М. В. Афанасьєва ; МОН України, НУ «ОЮА». Одеса : Гельветика, 2019. С. 34-47.

2. АО «Бачинський та партнери». *Захист персональних даних в Україні - все, що потрібно знати*. URL: https://legalaid.ua/ua/zahyst-personalnyh-danyh-v-ukrayini/(дата звернення: 28.10.2024).

3. Полікарпов О. В. Захист персональних даних: посібник для відповідального бізнесу в Україні. URL: https://polikarpov.legal/blogposts/zahist-personalnih-danih-posibnik-dlya-vidpovidalnogo-biznesu-v-ukra%D1%97ni/(дата звернення: 28.10.2024).

Н.О. Байдюк, К.В. Зарецька
Київський національний університет будівництва та архітектури, Київ, Україна

ЕТИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРБЕЗПЕКИ

Штучний інтелект (ШІ) - це інноваційна технологія, яка активно використовується у сфері кібербезпеки для виявлення загроз та оптимізації захисту. Однак разом з її перевагами виникають і серйозні етичні проблеми, пов'язані з конфіденційністю, прозорістю та підзвітністю в процесі прийняття рішень на основі ШІ.

Дослідження етичних аспектів ШІ в кібербезпеці набуває все більшого значення, оскільки відсутність етичних стандартів може призвести до порушень прав людини і потенційних загроз для суспільства.

Як зазначалося вище, штучний інтелект є важливим інструментом у боротьбі з кіберзагрозами, але він також має і темний бік: Алгоритми штучного інтелекту не лише зберігають наявні упередження, а й можуть мимоволі їх посилювати, успадковуючи історичні дані. Це породжує етичні проблеми, коли системи, покликані забезпечувати безпеку, мимоволі приймають дискримінаційні рішення або обмежують права певних груп людей.

Для розуміння та розробки шляхів мінімізації таких ризиків важливо вивчити механізми успадкування упередженості в ШІ, розглянути приклади дискримінації та можливі підходи до вирішення цих проблем.

Як відомо, тучний інтелект покладається на навчальні дані, зібрані з реальних джерел, які часто відображають минулі моделі і можуть містити соціальні упередження. Це може призвести до ненавмисного відтворення упередженого прийняття рішень, дискримінації та соціальної несправедливості, коли системи штучного інтелекту приймають рішення в автоматизованому режимі[1].

Механізми успадкування упереджень:

Навчання на основі даних: ШІ навчається на даних, які можуть містити дискримінаційні елементи. Якщо певна група зазнавала дискримінації в минулому (наприклад, при працевлаштуванні або кредитуванні), цю тенденцію можна врахувати в системі штучного інтелекту.

Дисбаланс даних: низька частка певних груп у наборі даних може призвести до менш точних результатів для цих груп. Це призводить до зниження точності та дискримінації цих груп, особливо в системах безпеки та прийняття рішень[3].

Приклади дискримінації в системах ШІ:

Системи оцінки кредитоспроможності: Багато алгоритмів штучного інтелекту для визначення кредитного рейтингу упереджені на основі історичних даних і можуть надавати перевагу певним групам, наприклад, чоловікам або етнічним групам, що становлять більшість населення.

Алгоритми розпізнавання обличчя: Такі алгоритми мають погану репутацію в розпізнаванні темношкірих людей. Це пов'язано з тим, що навчальний набір даних зазвичай містить багато зображень обличь світлошкірих людей.

Системи підбору персоналу: Автоматизовані системи підбору персоналу можуть надавати перевагу кандидатам певної статі, віку чи національності, якщо ці групи переважають у вхідних даних.

Щоб ШІ був надійним і етичним інструментом, необхідно захистити його від упереджених суджень, особливо в тих сферах, де важливі рішення безпосередньо впливають на життя людей[4].

Через потенційний ризик дискримінації певних груп розробники та користувачі ШІ повинні вживати заходів для зменшення впливу упередженості. Ці заходи слід розглядати з

точки зору технічних, організаційних і регуляторних підходів, які разом забезпечують справедливість і прозорість у функціонуванні систем[2].

Щоб уникнути несправедливого ставлення до певних груп людей, важливо вживати комплексних заходів як на технічному, так і на організаційному та регуляторному рівнях.

Технічні рішення:

Аудит навчальних даних: Регулярний перегляд навчальних даних може допомогти виявити та усунути елементи упередженості.

Балансування датасетів: Забезпечення рівного представництва різних груп запобігає наданню переваг певним категоріям.

Тестування на різних демографічних групах: Алгоритми тестування, які є точними та справедливими для всіх груп, можуть зменшити ймовірність дискримінації.

Метрики справедливості Додавання конкретних індикаторів для вимірювання справедливості рішень ШІ може допомогти оцінити, наскільки збалансованим є алгоритм[3].

Організаційні заходи:

Різноманітність у командах розробників: Команди, до складу яких входять представники різних соціальних груп, можуть краще оцінити потенційний ризик упередженості.

Прозорість алгоритмів: Визначення принципів ШІ може допомогти зрозуміти, як приймаються рішення.

Етичні принципи розробки ШІ: Використання етичних стандартів при розробці алгоритмів може запобігти дискримінаційним рішенням.

Регуляторні вимоги:

Законодавчі норми щодо недискримінації: Державне урегулювання допомагає запобігти упередженим рішенням.

Аудити систем: Регулярні аудити допомагають контролювати справедливість та прозорість системи[2].

Розглянуті етичні аспекти застосування штучного інтелекту в сфері кібербезпеки підкреслюють критичну важливість людського фактору в процесі розробки та впровадження цих систем. Незважаючи на потужність та ефективність ШІ у виявленні та протидії кіберзагрозам, саме людина залишається ключовим елементом у забезпеченні етичного використання цих технологій[1].

Особливої актуальності в контексті кібербезпеки набуває знаменита фраза **«З великою силою приходить велика відповідальність»**. Ця цитата, яка стала відомою завдяки коміксам про Людину-павука, де її промовляє дядько Бен, надзвичайно точно відображає етичну дилему використання ШІ в кібербезпеці. Адже чим потужнішими стають системи штучного інтелекту в захисті інформаційних систем, тим більшу відповідальність несуть розробники та користувачі за їх етичне застосування.

Тому критично важливо забезпечити:

1. Постійний людський нагляд за роботою систем ШІ.
2. Регулярний аудит та перевірку алгоритмів на упередженість.
3. Можливість оскарження автоматизованих рішень.
4. Прозорість процесів прийняття рішень.
5. Баланс між ефективністю захисту та етичними принципами.

Лише за умови відповідального підходу до розробки та впровадження, штучний інтелект може стати надійним інструментом забезпечення кібербезпеки, який не тільки ефективно захищає від загроз, але й поважає права та гідність усіх користувачів.

Список використаних джерел:

1. Юрій Гайдай Тренди ШІ: які етичні загрози несе використання штучного інтелекту, Speka, 2023, 21 травня. (дата звернення 28.10.2024).

2. Яровой Т. С., (2023). Можливості та ризики використання штучного інтелекту в публічному управлінні. Economic Synergy, (2), 36–47. URL: https://doi.org/10.53920/ES-2023-2-3. (дата звернення 28.10.2024).

3. Лозовський, Р., Мороз, А. (2024). Вплив штучного інтелекту на стратегії захисту інформаційних систем від нових типів кіберзагроз. Herald of Khmelnytskyi National University. Technical Sciences, 337(3(2)), 366-372. URL:https://doi.org/10.31891/2307-5732-2024-337-55 (дата звернення 28.10.2024).

4. Яценко В., Терляківська П., (2023). Роль Штучного Інтелекту В Цифровій Економіці: Технологічні Та Етичні Аспекти. The Role Of Artificial Intelligence In The Digital Economy: Technological And Ethical Aspects. Виклики Кібербезпеки Індустрії Фінансових Послуг, 107. (дата звернення 28.10.2024).

В.О. Авраменко
Державний університет інформаційно-комунікаційних технологій, м. Київ

УДОСКОНАЛЕННЯ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ БЕЗДРОТОВИМИ КАНАЛАМИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

На теперішній час для несанкціонованого зняття інформації широко використовуються технічні канали витоку інформації (ТКВІ).

Що являють собою такі канали? Наведемо спочатку загальне визначення.

Технічний канал витоку інформації – це сукупність небезпечних фізичних сигналів, серед яких розповсюдження та зберігання, об'єктів технічної розвідки й способів і засобів технічної розвідки, що можуть бути застосовані для зняття інформації з об'єкту, що охороняється.

Небезпечний фізичний сигнал (небезпечний сигнал) – це сигнал, що містить інформацію, яку необхідно захищати.

У нашій країні прийнято поділяти ТКВІ за наступною класифікацією:

- **акустичні канали витоку інформації**, куди входять також канали з акустично-електричним перетворенням;
- **радіотехнічні канали витоку інформації**, куди входять, по-перше, відкриті канали радіотехнічного зв'язку та, по-друге, канали, що утворюються за рахунок паразитичних випромінювань та наводок;
- **оптичні канали витоку інформації.**
- **речовий канал витоку інформації**, який визначається людським фактором.

В даному матеріалі розглянемо радіотехнічні канали оскільки вони є бездротовими. Радіотехнічні канали застосовуються для таких технологій як Wi-Fi, Bluetooth, NFC.

Wi-Fi - загальновживана назва для стандарту IEEE 802.11 передавання цифрових потоків даних по радіоканалах. Поширеним на сьогодні є протокол IEEE 802.11n, що забезпечує до 300 Мбіт/с.

Bluetooth - технологія бездротового зв'язку, створена у 1998 році групою компаній: Ericsson, IBM, Intel, Nokia, Toshiba. Інтерфейс Bluetooth дає змогу передавати як голос (зі швидкістю 64 Кбіт/с), так і дані. Для передачі даних можуть бути використані асиметричний (721 Кбіт/с в одному напрямку і 57,6 Кбіт/с в іншому) та симетричний (432,6 Кбіт/с в обох напрямках) методи. Працюючи на частоті 2.4 ГГц, прийомопередавач (Bluetooth-chip) дає змогу встановлювати зв'язок у межах 10 або 100 метрів.

Ось кілька способів підвищити ефективність бездротових систем передачі даних:

- **Оновлення обладнання**: Перехід на сучасні пристрої, що підтримують новітні стандарти, такі як Wi-Fi 6 або Wi-Fi 6E, Bluetooth 5.1 та 5.2 забезпечить вищу швидкість, стабільність і краще впорається з перевантаженням.
- **Оптимізація налаштувань мережі**:
  - Канали: Вибір вільних каналів, особливо на частоті 5 GHz(для Wi-Fi), зменшить завади та покращить продуктивність.
  - Ширина каналу: Залежно від умов мережі, оптимальним може бути налаштування ширших каналів (наприклад, 40 або 80 MHz) для підвищення швидкості, хоча вони більш чутливі до завад.
- **Вигідне розташування роутера**: Для найкращого покриття роутер слід розмістити в центрі приміщення, подалі від перешкод і джерел завад, таких як інші електронні пристрої.
- **Розширення покриття за допомогою Mesh-систем і повторювачів**: Встановлення Mesh-систем або повторювачів у великих приміщеннях забезпечить стабільне покриття на всій площі.
- **Покращення антен і модулів**:
  - Використання антен з більшим коефіцієнтом підсилення підвищує якість сигналу.
  - Підтримка технології MU-MIMO дозволяє роутерам обслуговувати кілька пристроїв одночасно, зменшуючи затримки.
- **Захист від завад**: Зменшення зовнішніх завад шляхом вибору вільних каналів або встановлення фільтрів стабілізує сигнал.

Список використаних джерел:

1. Лекція_1_ОПНД_2024
2. https://uk.wikipedia.org/wiki/IEEE_802.11
3. https://uk.wikipedia.org/wiki/Bluetooth

Ю.І. Катков, Д.А. Соболєв,
Державний університет інформаційно-комунікаційних технологій, м. Київ

АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ КЕРУВАННЯ IP-АДРЕСАМИ В КОРПОРАТИВНІЙ МЕРЕЖІ

Анотація. У сучасних корпоративних мережах зростає кількість пристроїв і, відповідно, IP-адрес, які необхідно контролювати, ефективно розподіляти та забезпечувати безпеку засобів керування IP-адресами в корпоративній мережі. Програмні засоби для керування IP-адресами в корпоративній мережі можуть зазнавати різні види атак для підриву їхньої ефективності. Сутність безпеки програмних засобів для керування IP-адресами в корпоративній мережі полягає у забезпеченні конфіденційності, цілісності та доступності інформації про IP-адреси, що використовується в мережі. Ці програмні засоби дозволяють управляти розподілом, резервуванням та відстеженням IP-адрес, а також забезпечувати їхню правильну інтеграцію з іншими мережевими компонентами, такими як DNS та DHCP. Тому виникає завдання метою якого є визначення актуальних проблем безпеки програмних засобів для керування IP-адресами в корпоративній мережі

Ключові слова: керування IP-адресами, кібербезпека.

Постановка завдання. У сучасних корпоративних мережах зростає кількість пристроїв і, відповідно, IP-адрес, які необхідно контролювати та ефективно розподіляти. Ручне керування IP-адресами є трудомістким і помилковим, особливо для великих організацій. Сьогодні з’являються програмні засоби для автоматизації процесу керування IP-адресами, що забезпечують точність і надійність в адмініструванні мереж. Але програмні засоби для керування IP-адресами в корпоративній мережі можуть зазнавати різні види атак для підриву

їхньої ефективності. Таким чином, впровадження програмних засобів для керування IP-адресами в корпоративних мережах вимагає дослідження актуальних проблем безпеки програмних засобів для керування IP-адресами в корпоративній мережі, що своєчасним та актуальним завданням [1, 2].

Мета дослідження. Підвищення ефективності безпеки управління IP-адресами в корпоративній мережі через дослідження актуальних проблем безпеки програмних засобів для керування IP-адресами в корпоративній мережі для їх використання, що дозволить знизити трудовитрати та мінімізувати кількість помилок при адмініструванні IP-простору.

Результати дослідження. Програма для управління IP-адресами (IP Address Management, IPAM) — це програмне забезпечення, яке використовується для централізованого керування, відстеження і адміністрування IP-адрес в корпоративній мережі. Ринок пропонує різні програмні рішення, такі як IPAM-системи, які забезпечують ефективну роботу з IP-адресами у великих і складних мережах. IPAM допомагає автоматизувати процеси розподілу, резервування та моніторингу IP-адрес, що особливо корисно у великих мережах з численними пристроями. Основні функції таких програм включають [1, 2, 3, 4]:

1. **Автоматичне призначення IP-адрес** — динамічне розподілення адрес через DHCP (Dynamic Host Configuration Protocol), що зменшує ймовірність конфліктів.
2. **Відстеження та аудит IP-адрес** — забезпечує видимість усіх IP-адрес, пристроїв і їх активність у мережі.
3. **Виявлення та уникнення конфліктів** — допомагає уникнути дублювання IP-адрес, яке може спричинити проблеми в мережі.
4. **Інтеграція з DNS та DHCP** — IPAM часто об'єднується з іншими мережевими службами, як-от DNS (Domain Name System) та DHCP, що дає змогу централізовано керувати всіма мережевими ресурсами.
5. **Звітність та аналітика** — надає інформацію про використання адресного простору, історію змін і тенденції для оптимізації мережі.

Прикладами таких програм є Infoblox IPAM, SolarWinds IP Address Manager, BlueCat Address Manager та Microsoft IPAM. Серед найпопулярніших IPAM-рішень на сьогоднішній день виділяються SolarWinds IPAM, Infoblox та BlueCat.

Програмні засоби для керування IP-адресами надають можливість автоматизувати розподіл, моніторинг та адміністрування IP-простору в організаціях різного масштабу. Вони підтримують централізоване управління, що знижує ризик помилок у налаштуванні IP-адрес, підвищує безпеку мережі та покращує продуктивність команди. Також важливим аспектом є доступність можливості інтеграції з іншими системами для спрощення адміністрування мережі, зокрема з DNS та DHCP сервісами, що дозволяє забезпечити автоматичне оновлення записів.

Серед основних переваг програмного керування IP-адресами можна виділити наступні:

1. **Зниження трудовитрат:** Автоматизація процесів дозволяє звільнити ресурси для інших завдань.
2. **Підвищення надійності:** Менше ручної роботи зменшує ризик помилок і втрат інформації.
3. **Гнучкість в управлінні:** IPAM-системи дозволяють швидко адаптуватися до змін у мережі, додавати або видаляти IP-адреси без потреби у значному ручному втручанні.

Але існують сучасні виклики безпеки програмного забезпечення для керування IP-адресами в корпоративній мережі, що пов’язані з постійним розвитком кіберзагроз та розширенням мережевої інфраструктури. Основні актуальні проблеми безпеки таких систем включають [5]:

1. Недостатній захист від несанкціонованого доступу

Проблема: Уразливі інтерфейси для адміністрування IP-адрес можуть дозволяти несанкціонованим користувачам доступ до конфіденційної мережевої інформації. Захист від несанкціонованого доступу передбачає контроль над тим, хто може отримувати доступ до

інформації про IP-адреси та змінювати налаштування мережі. Це включає аутентифікацію та авторизацію користувачів, захист від зловмисників і випадкових помилок.

Рішення проблеми: Застосування багатофакторної аутентифікації (MFA) та рольового доступу, який забезпечує доступ лише до необхідних функцій для кожної групи користувачів.

2. Незахищені API та зовнішні з'єднання

Проблема: API для інтеграції з іншими мережевими системами можуть мати вразливості, що відкривають доступ до маніпуляцій з IP-адресами. Захист від внутрішніх загроз: передбачає забезпечення того, щоб співробітники не могли несанкціоновано змінювати чи переглядати дані про IP-адреси, а також обмеження привілеїв доступу лише необхідними для роботи.

Рішення проблеми: Використання захищених каналів зв'язку (SSL/TLS), обмеження доступу до API за IP-адресами, а також регулярне тестування безпеки API.

3. Неправильне налаштування доступу до бази даних

Проблема: Відсутність належного захисту баз даних з інформацією про IP-адреси може призвести до втрати або витоку даних.

Рішення проблеми: Налаштування обмежень доступу до бази даних, шифрування даних та використання моніторингу доступу для виявлення підозрілих дій.

4. Ризики внаслідок відсутності шифрування

Проблема: Дані можуть передаватися незашифрованими, що дозволяє зловмисникам перехопити інформацію про IP-адреси та використовувати її для атаки на мережу. Шифрування даних означає шифрування інформації під час передачі та зберігання, щоб у разі перехоплення даних вони не могли бути прочитані або використані зловмисниками.

Рішення проблеми: Використання шифрування даних як на рівні передачі, так і в самій системі, щоб запобігти несанкціонованому доступу.

5. Вразливість до DDoS-атак

Проблема: Доступ до сервісу може бути заблокований через перенасичення запитами, що перешкоджає нормальній роботі системи.

Рішення проблеми: Використання захисту від DDoS-атак, який може включати обмеження на кількість запитів з однієї IP-адреси та залучення мережевих засобів захисту.

6. Відсутність моніторингу та журналювання (протоколювання)

Проблема: Відсутність ефективного моніторингу може залишити систему уразливою до атак і складнощів з ідентифікацією загроз. Моніторинг і журналювання означає постійний моніторинг активності в системі та запис дій, що дозволяє вчасно виявляти та реагувати на підозрілі або небезпечні дії.

Рішення проблеми: Реалізація систем моніторингу, які дозволяють оперативно виявляти аномалії та реагувати на підозрілі дії.

7. Застаріле програмне забезпечення та вразливості у версіях

Проблема: Використання старих версій ПО може залишати систему вразливою до відомих експлойтів.

Рішення проблеми: Регулярне оновлення та патчування програмного забезпечення, а також використання останніх версій із виправленими вразливостями.

8. Безпека API та інтеграцій:

Проблема: Відсутність контролю за API, які використовуються для зв'язку з іншими системами, щоб уникнути небажаних втручань або маніпуляцій з даними. Безпека API та інтеграцій є важливим аспектом захисту програмного забезпечення для управління IP-адресами (IPAM) в корпоративних мережах, оскільки ці програми часто взаємодіють із критичними мережевими компонентами, такими як DHCP, DNS і системи управління мережею. Уразливості в API можуть дати змогу зловмисникам отримати несанкціонований доступ до IP-інфраструктури, що може призвести до компрометації всієї мережі.

Рішення проблеми: Забезпечення безпеки API та інтеграцій у програмному забезпеченні для керування IP-адресами в корпоративній мережі можливе шляхом виконання ключових заходів і стратегій, які можуть допомогти вирішити ці проблеми, а саме:

аутентифікація та авторизація; шифрування даних; регулярне тестування безпеки; моніторинг та аудит; валідація введених даних; обмеження доступу; застосування принципів безпеки «найменших привілеїв» (Least Privilege) та регулярне оновлення та патчинг програмного забезпечення для усунення відомих вразливостей та навчання персоналу:

9. Захист від DDoS-атак:

Проблема: Відсутність використання захисних технологій для зниження ризику перезавантаження системи, що може порушити доступ до даних та сервісів.

Рішення проблеми: Забезпечення безпеки API шляхом використання захисних технологій, а саме: системи виявлення та запобігання вторгненням (IDS/IPS); засоби контролю трафіку; розподілена архітектура; Content Delivery Networks (CDN); використання CDN для кешування контенту і розподілу трафіку між різними серверами; обмеження запитів (Rate Limiting); фільтрація трафіку; аналіз поведінки; партнерство з постачальниками послуг захисту; резервне копіювання та відновлення; моніторинг і реагування.

Висновки.

1. Ефективне керування IP-адресами є важливим завданням для будь-якої сучасної організації з розвиненою мережею. Використання програмного забезпечення для автоматизації цього процесу допомагає уникнути багатьох проблем і зменшити кількість помилок.

2. Сучасні програмні рішення для керування IP-адресами пропонують широкий функціонал, але часто можуть бути перевантаженими непотрібними функціями. Тому в роботі було розглянуто найважливіші інструменти та особливості IPAM-рішень, які можуть допомогти організаціям оптимізувати процеси керування IP-простором, спростити адміністрування мережі та забезпечити її надійність.

3. З огляду на ці проблеми виникає необхідність розробки комплексного підходу до забезпечення безпеки, включаючи регулярний аудит системи, захищені методи доступу, шифрування та моніторинг подій, є ключовим для надійного управління IP-адресами в корпоративних мережах.

Список використаних джерел:

1. IP Address Management (IPAM). URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/ipam/ipam-top (дата звернення: 29.10.2024).

2. Типи рішень для IPAM та особливості їх застосування. URL: https://www.networkcomputing.com/networking/ip-address-management-ipam-solutions (дата звернення: 29.10.2024).

3. Найкращі IPAM інструменти для корпоративних мереж. URL: https://www.techradar.com/best/best-ipam-tools (дата звернення: 29.10.2024).

4. Переваги використання програмних засобів для керування IP-адресами. URL: https://www.solarwinds.com/ip-address-manager/use-cases/ipam (дата звернення: 31.10.2024).

5. Common Software Security Issues & Strategies to Prevent Their Impact URL: https://www.orientsoftware.com/blog/software-security-issues/(дата звернення: 31.10.2024).

А. Г. Любушкіна,
Київський національний університет будівництва і архітектури, м. Київ

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРБЕЗПЕЦІ

З початком повномасштабної війни роль штучного інтелекту в кібербезпеці України стала особливо важливою. Збільшення кількості атак на цифрову інфраструктуру України вимагає швидкої та ефективної реакції, яка можлива лише за допомогою автоматизованих систем, які самонавчаються. Штучний інтелект використовується для захисту критично важливих об'єктів, таких як енергетичні та комунікаційні мережі, які стають мішенню для російських хакерів. На графіку 1 показана різниця в кількості у 2021 та 2023 роках.

Сергій Галаган, директор та IT-директор Укренерго, повідомив, що IT-спеціалісти державної компанії «Укренерго» помітили збільшення кількості кібератак на свої системи у січні 2022 року. З 24 лютого 2022 року кількість кіберінцидентів зросла втричі порівняно з попереднім роком Він каже, що кількість кіберінцидентів зросла втричі порівняно з попереднім роком.

Змінюється і мета атак. До початку повномасштабної війни російські хакери були зацікавлені у фінансовій вигоді. Це і викупи за відновлення систем, і викрадення даних для продажу. Сьогодні вони частіше координують свої дії з військовими в атаках на енергетичні об'єкти, зазначає Сафаров.

З 2022 року однією з пріоритетних цілей російських кібервійськ стануть енергетичні системи України. Мета - дестабілізувати критичну інфраструктуру, щоб припинити енергопостачання, заявляє прес-служба ДТЕК.

Графік 1

На сьогодні штучний інтелект відіграє ключову роль в кібербезпеці, підвищуючи ефективність виявлення, аналізу та реагування на загрози. Сучасні кіберзагрози зазнали великих змін та стали все дедалі витонченішими, і традиційні методи безпеки втрачають свою ефективність. Використання штучного інтелекту дозволяє автоматизувати складні процеси захисту інформаційних систем, виявляючи загрози у реальному часі.

Одним із найкращих прикладів застосування штучного інтелекту у сфері безпеки є використання алгоритмів машинного навчання для аналізу поведінки користувачів та виявлення закономірностей. Розуміючи, що є нормальним, ці системи можуть виявляти аномальну поведінку, яка може бути ознакою кібератаки. В іншому прикладі фахівці з безпеки виконують генеративний ШІ, щоб поставити питання про конкретну подію або середовище і

отримувати у відповідь діаграми або текст природною мовою, що дає більш детальний контекст і розуміння, засноване на кількох джерелах даних.

Штучний інтелект обробляє велику кількість даних, щоб виявити аномалії та ваші зловмисні дії. Моделі машинного навчання (ML) аналізують історичні дані та прогнозують можливості атак. Наприклад, алгоритми ML розпізнають шаблони поведінки користувачів і додають про підозрілі дії, скорочуючи час реагування. Швидкість і точність таких моделей значно перевищують людські можливості.

Основними типами аномалій, в яких можливе використання штучного інтелекту є

- Виявлення недоліків банківських операцій (Credit-card Fraud)
- Виявлення вторгнень (Intrusion Detection)
- Виявлення нестандартних гравців на біржі (інсайдерів)

Адаптивна природа Штучного інтелекту дозволяє постійно вдосконалювати моделі кібербезпеки. Системи виявлення загроз навчаються на нових типах атак і адаптуються до змін. Це особливо важливо в боротьбі зі шкідливими програмами, які швидко мутують. Наприклад, антивірусне програмне забезпечення зі штучним інтелектом може виявляти нові віруси навіть без раніше створених підписів.

Автоматизація рутинних завдань. ШІ виконує таке завдання, як моніторинг системи та оновлення політики безпеки без втручання людини, таким чином знижуючи ризик людської помилки. Однак це також ризики, пов'язані з помилковими дослідженнями та неправильним аналізом даних.

Варто зазначити, що прогрес у галузі ШІ створює нові виклики. Зловмисники починають використовувати ШІ для проведення більш складних атак, таких як автоматизовані фішингові кампанії та приховані DDoS-атаки. Це вимагає від експертів з кібербезпеки розробки більш досконалих систем захисту.

ШІ робить кібербезпеку більш ефективною, але необхідно вирішити етичні та правові питання, пов'язані з обробкою персональних даних. Використання ШІ також має обґрунтовуватися на прозорих алгоритмах і відповідних нормах.

Таким чином, штучний інтелект значно підвищує рівень безпеки інформаційних систем, але його застосування має бути виваженим і відповідальним, з урахуванням можливих ризиків і наслідків для користувачів і організацій.

Список використаних джерел:

1. Валентина Шимкович. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. *robot_dreams - онлайн-курси для фахівців у сфері big data, machine learning, data science | Робот Дрімс*. URL: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku (дата звернення: 03.11.2024).

2. Валентина Шимкович. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. *robot_dreams - онлайн-курси для фахівців у сфері big data, machine learning, data science | Робот Дрімс*. URL: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-ne-vikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku (дата звернення: 03.11.2024).

3. Ровесниця незалежності. як BAYADERA GROUP 33 роки зростає разом з україною – forbes.ua. *Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії*. URL: https://forbes.ua/company/rovesnitsya-nezalezhnosti-yak-bayadera-group-33-roki-zrostae-razom-z-ukrainoyu-31102024-24478 (дата звернення: 03.11.2024).

Р.М. Стиранка, І. М. Козубцов,
Київський національний університет будівництва і архітектури, м. Київ

ЗАГРОЗИ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Загрози безпеки Інтернету речей (IoT) набувають критичного значення через стрімке збільшення кількості підключених пристроїв. Ця технологія, що забезпечує автоматизований обмін даними між фізичними об’єктами, відкриває нові можливості для оптимізації процесів у різних сферах, проте супроводжується ризиками, які можуть призвести до серйозних наслідків. Вразливості IoT-пристроїв, включаючи недостатній захист даних та відсутність стандартизованих протоколів безпеки, можуть бути використані зловмисниками для здійснення атак на мережі, що загрожує конфіденційності та цілісності інформації в інформаційно-телекомунікаційних системах.

Успішне функціонування сучасних інформаційних систем вимагає глибокого розуміння специфіки загроз, пов’язаних із IoT. Проблеми захисту та безпеки цих систем стали предметом численних досліджень, однак їх реалізація в промисловості залишається нерегульованою. З огляду на складність взаємодії між пристроями, важливо розробити ефективні стратегії для мінімізації ризиків та забезпечення безпеки користувачів. Без належної уваги до цих викликів подальший розвиток IoT може призвести до серйозних збоїв у функціонуванні критичних інфраструктур.

Інтернет речей (IoT) відкриває нові горизонти для автоматизації та взаємодії пристроїв, однак цей прогрес супроводжується численними загрозами безпеки. Зростаюча кількість підключених пристроїв підвищує ризик атак, оскільки кожен з них може стати потенційною мішенню для кіберзлочинців. За оцінками, до 2025 року ми можемо спостерігати десятки мільярдів нових IoT-пристроїв, що призведе до значних економічних вигод, але лише за умови, що проблеми безпеки будуть вирішені[1].

Однією з основних загроз є недостатня безпека на етапі виробництва. Багато виробників не приділяють достатньо уваги захисту своїх продуктів, що призводить до вразливостей. Наприклад, атаки ботнету Mirai продемонстрували, як використання слабких паролів на масово вироблених пристроях може призвести до масштабних атак, що затопили інфраструктуру Інтернету [1]. Дані, які збираються та передаються через IoT-пристрої, можуть бути зламані або викрадені, що становить загрозу для конфіденційності та безпеки користувачів.

Зростаюча кількість підключених пристроїв створює нові виклики для управління даними та мережами. Взаємодія між пристроями вимагає постійного обміну даними, що робить їх більш уразливими до атак з використанням шкідливого програмного забезпечення. Важливо зазначити, що не лише кінцеві користувачі, а й виробники та постачальники послуг мають дбати про безпеку своїх продуктів і послуг.

Впровадження IoT у повсякденне життя також породжує етичні та правові питання, пов'язані з конфіденційністю даних. Споживачі все частіше стурбовані тим, як їхні дані збираються, зберігаються та використовуються. Результати опитування показали, що багато людей вважають, що пристрої IoT вже мають належні системи безпеки, тоді як насправді виробники часто недооцінюють важливість захисту [2].

Безпека Інтернету речей (IoT) стикається з численними викликами, які заважають його інтеграції в сучасні інформаційно-телекомунікаційні системи. Пристрої IoT, зазвичай, мають обмежені ресурси, що ускладнює впровадження складних механізмів захисту. Наприклад, відсутність стандартів безпеки призводить до вразливості, адже зловмисники можуть легко отримати доступ до слабких вузлів сприйняття [3].

Крім того, варто враховувати ризики, пов’язані з передачею даних. Можливе перехоплення інформації та витік даних можуть стати наслідком ненадійного програмного забезпечення або вразливостей у мережевих протоколах. Дослідження свідчать, що недоліки

в аутентифікації можуть призводити до атак типу DDoS, що є серйозною загрозою для цілісності системи [3].

Критично важливим є управління оновленнями та патчами для забезпечення захисту пристроїв. Власники IoT-пристроїв часто ігнорують ці оновлення, що робить їх уразливими до нових загроз. Зростаюча кількість підключених пристроїв також створює проблеми масштабованості, адже складність управління мережею з великою кількістю елементів збільшує вразливість до атак.

Проблеми безпеки IoT безпосередньо впливають на ефективність інформаційно-телекомунікаційних систем, оскільки зростання кількості непідконтрольних пристроїв може призвести до серйозних наслідків, таких як втрати даних або зниження довіри до технологій. Тому важливо розробити комплексні стратегії для посилення безпеки в цій екосистемі, включаючи впровадження новітніх технологій захисту та регулярне оновлення стандартів безпеки.

Таким чином, для забезпечення безпеки IoT необхідно враховувати не лише технологічні, але й соціально-економічні аспекти, які впливають на прийняття технологій користувачами. Важливо гарантувати не тільки безпеку даних, а й довіру користувачів, що є критично важливим для подальшого розвитку цієї сфери.

Список використаних джерел:

1. Проблеми та загрози IoT пристроїв URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/231/205 (Дата звернення: 01.11.2024)

2. Загрози у світі речей інтернету (Безбека інтернету речей) URL: https://hackyourmom.com/osvita/chastyna-1-zagrozy-u-sviti-rechej-internetu-bezpeka-internetu-rechej/ (Дата звернення: 01.11.2024)

3. Аналіз проблеми безбеки інтернету речей URL: https://confopcbproc.iee.kpi.ua/article/download/114909/109357 (Дата звернення: 01.11.2024)

І.В. Савотіков,
Державний університет інформаційно-комунікаційних технологій м.Київ

МОДЕЛЮВАННЯ АНТЕННИХ СИСТЕМ ГЕНЕРАТОРІВ РАДІОЗАВАД

Роль радіозавад у системах захисту та зв`язку

Радіозавади використовуються в багатьох сферах для забезпечення безпеки та ефективності комунікацій. Наприклад, у військових комунікаціях застосовуються спеціалізовані радіозавади, які створюють шум в певних частотних діапазонах, щоб перешкоджати роботі систем зв'язку ворога під час військових операцій. У дипломатичних місіях радіозавади можуть використовуватися для захисту чутливих переговорів від перехоплення сторонніми особами. Крім того, радіозавади використовуються для тестування надійності систем зв'язку. Це може включати моделювання умов, при яких зв'язок може бути ускладнений, наприклад, в умовах екстремальних погодних явищ, таких як сильні дощі чи снігопади. Тестування нових бездротових технологій, наприклад, 5G, також може включати радіозавади, щоб перевірити стійкість системи до перешкод. У цивільних сферах радіозавади можуть використовуватися для захисту комунікаційних систем від втручання або прослуховування. Наприклад, у банківських системах радіозавади можуть застосовуватися в банкоматах або терміналах для захисту платіжних карток від несанкціонованого доступу. Також у розумних будинках радіозавади можуть допомогти захистити пристрої інтернету речей (IoT) від зовнішніх атак або хакерських спроб. Радіозавади також відіграють важливу роль у моніторингу та виявленні загроз. У сфері кібербезпеки радіозавади можуть використовуватися для виявлення та моніторингу активності ворожих сигналів або пристроїв,

що намагаються перехопити зв'язок. У системах безпеки, які використовують бездротові технології, радіозавади можуть допомогти у виявленні спроб несанкціонованого доступу.У аеронавігаційних системах радіозавади можуть використовуватися для захисту від спроб підробки сигналів GPS, що є критично важливим для безпеки літаків під час зльоту та посадки. Ці приклади демонструють, як радіозавади можуть бути корисними в різних сферах, забезпечуючи безпеку та ефективність систем зв'язку.

Стандартні компоненти генератора радіозавад

Генератор сигналів

Основний компонент, який виробляє радіосигнали. У роботі досліджено різні компоненти, включаючи коливальний контур на основі резисторів, конденсаторів і котушок індуктивності, а також спеціалізовані інтегральні схеми, такі як генератор на основі NE555. Аналіз їх принципів роботи дозволив виявити переваги і недоліки кожного варіанту. Наприклад, коливальні контури забезпечують високу стабільність частоти, однак можуть вимагати складнішого налаштування, тоді як інтегральні схеми простіші у використанні, але можуть мати обмеження за частотним діапазоном.

Підсилювач

Збільшує потужність сигналу, що генерується генератором. Зазвичай це операційний підсилювач або транзистор, який може працювати в різних режимах (наприклад, як підсилювач напруги). У дипломній роботі порівнювалися різні типи підсилювачів, і було визначено, який із них найкраще підходить для даного генератора радіоперешкод, з урахуванням таких факторів, як ефективність, частотний діапазон і простота інтеграції в пристрій.

Антена

Використовується для передачі згенерованих радіопомех у просторі. Антени можуть бути простими проводами, рамковими антенами або дипольними антенами. У роботі проведено порівняння всіх типів антен, щоб визначити, яка з них найбільш ефективна для передачі радіопомех, враховуючи радіус дії та напрямленість сигналу.

Фільтри

Дозволяють відділяти корисні сигнали від перешкод і можуть використовуватися для налаштування частоти генератора. Це можуть бути LC-фільтри або RC-фільтри. Основне призначення фільтрів полягає в покращенні якості сигналу, зменшенні небажаних шумів і забезпеченні чистоти радіочастотного спектра. Без фільтрів можливі втрати в якості передаваного сигналу і виникнення небажаних перешкод, що може негативно вплинути на роботу всього пристрою.

Корпус

Захищає внутрішні компоненти пристрою і запобігає небажаному впливу навколишнього середовища на роботу генератора.

Висновок

У даній роботі було проведено детальний аналіз конструкції та принципу роботи простого генератора радіопомех. Розглянуто основні компоненти, їхні переваги та недоліки, а також проведено порівняння різних типів підсилювачів та антен, що дозволило вибрати оптимальні рішення для створення ефективного пристрою. Результати дослідження можуть бути корисними для подальшої розробки та вдосконалення систем радіозавад, що має важливе значення в умовах сучасного інформаційного середовища.

Список використаних джерел:

1. Hill, D. A. "Схемотехніка: принципи і застосування". Техніка, 2015.
2. Balanis, C. A. "Antenna Theory: Analysis and Design". John Wiley & Sons, 2016.
3. Pozar, D. M. "Microwave Engineering". John Wiley & Sons, 2012.

М.В. Біленький,
Київський національний університет будівництва і архітектури, м. Київ

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

У сучасному інформаційному суспільстві кібербезпека набуває все більшої значущості через зростаючу залежність державних та приватних структур від цифрових технологій. Разом із цим зростає і кількість, а також складність кіберзагроз, що вимагає впровадження новітніх методів захисту інформаційних ресурсів. Одним із найперспективніших напрямків у сфері кібербезпеки є використання штучного інтелекту (ШІ) для виявлення та нейтралізації кіберзагроз.

Основною проблемою, з якою стикаються сучасні системи кібербезпеки, є необхідність швидкого та точного виявлення аномалій у великих обсягах даних мережевого трафіку. Традиційні методи захисту часто не справляються з новими та невідомими типами атак, що підвищує ризик витоків інформації, фінансових збитків та інших серйозних наслідків. Штучний інтелект, зокрема методи машинного навчання та глибинного навчання, пропонує ефективні рішення для подолання цих викликів.

Метою цього дослідження є аналіз сучасних методів застосування ШІ для виявлення кіберзагроз, оцінка їхньої ефективності та визначення найбільш перспективних напрямків розвитку. Для досягнення цієї мети планується провести огляд існуючих алгоритмів машинного навчання, таких як нейронні мережі, дерева рішень, методи ансамблевого навчання, а також дослідити їхню здатність до самонавчання та адаптації до нових типів атак без необхідності ручного оновлення систем захисту.

Одним із ключових аспектів дослідження є використання глибинного навчання, зокрема конволюційних нейронних мереж (CNN) та рекурентних нейронних мереж (RNN), для аналізу складних патернів у даних мережевого трафіку. CNN ефективно обробляють просторові дані, що дозволяє їм виявляти специфічні ознаки атак, тоді як RNN здатні аналізувати тимчасові залежності, що є корисним для розпізнавання послідовностей дій під час кібератак. Крім того, методи ансамблевого навчання, такі як Random Forest та Gradient Boosting, дозволяють комбінувати кілька моделей для покращення точності та надійності виявлення загроз.

Важливою частиною дослідження є також інтеграція моделей ШІ з існуючими системами моніторингу та управління безпекою. Це забезпечить більш гнучке та динамічне реагування на потенційні атаки, а також дозволить здійснювати глибший аналіз загроз шляхом інтеграції даних з різних джерел, таких як журнали подій, мережевий трафік та поведінкові моделі користувачів. Таким чином, системи на базі ШІ можуть не лише виявляти поточні загрози, але й прогнозувати потенційні атаки на ранніх стадіях їх розвитку.

Незважаючи на значні переваги, впровадження ШІ у кібербезпеку супроводжується рядом викликів. Одним із головних є потреба у великих обчислювальних ресурсах для тренування складних моделей, а також забезпечення їхньої надійності та точності. Крім того, існує ризик виникнення хибних спрацьовувань, що може призводити до непотрібних блокувань легітимного трафіку та негативно впливати на продуктивність системи. Важливо також враховувати питання безпеки самих моделей ШІ, оскільки вони можуть стати мішенню для атак, спрямованих на їх маніпуляцію або злом.

У контексті національної безпеки України застосування ШІ для виявлення кіберзагроз набуває особливої актуальності. З огляду на зростаючу кількість кібератак з боку різних суб'єктів, включаючи державні структури та організовані злочинні групи, ефективні системи кіберзахисту стають невід'ємною частиною забезпечення інформаційної безпеки країни. Відповідно до Доктрини інформаційної безпеки України, розвиток інноваційних технологій, таких як ШІ, є пріоритетним напрямком у боротьбі з кіберзагрозами.

Для успішної інтеграції ШІ у системи кібербезпеки необхідно розробити стандарти та протоколи, які забезпечать безпечне впровадження цих технологій. Крім того, важливо проводити постійне оновлення моделей ШІ для адаптації до нових видів загроз, а також забезпечувати навчання та підвищення кваліфікації фахівців у сфері кібербезпеки. Співпраця між науковими установами, державними органами та приватним сектором є ключовою для спільного вирішення питань кібербезпеки та забезпечення ефективного використання ШІ у цьому напрямку.

Список використаних джерел:

1. Янн, Ю. К., та Іванов, П. С. *Машинне навчання в кібербезпеці*. Київ: Наукова думка, 2020.
2. Сміт, Дж. *Deep Learning for Cyber Security*. New York: Springer, 2019.
3. Олексієнко, М.В., та Петров, А.К. "Застосування нейронних мереж для виявлення DDoS-атак." *Журнал інформаційної безпеки*, Т. 12, №3, с. 45-58, 2021.
4. Brown, L., & Davis, S. "Artificial Intelligence in Cyber Threat Detection: A Review." *Cybersecurity Journal*, Vol. 8, No. 2, pp. 123-135, 2022.
5. Національний стандарт України ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання».

Д.О. Токар,
Київський національний університет будівництва і архітектури, м. Київ

СИСТЕМИ ПРИДУШЕННЯ МОБІЛЬНОГО ЗВ`ЯЗКУ В КОНТЕКСТІ ЗАХИСТУ ІНФОРМАЦІЇ

З розвитком технологій мобільного зв’язку, особливо у напрямку 4G і 5G, питання інформаційної безпеки набуло нової актуальності. Сучасні мобільні мережі забезпечують безперервну комунікацію і передачу даних, що є надзвичайно важливим у багатьох сферах, але це також створює значні ризики для захисту конфіденційної інформації. Використання мобільних пристроїв на чутливих об’єктах може призвести до витоку інформації, а також до загроз кібербезпеки [1]. Системи придушення мобільного зв'язку, які перешкоджають передачі даних між мобільними пристроями і базовими станціями, є важливим інструментом у захисті даних. Вони створюють штучні перешкоди, що блокують передачу сигналів, або фізично обмежують зону, де можуть працювати мобільні пристрої.

Метою цього дослідження є аналіз методів придушення мобільного зв'язку, оцінка їх ефективності та потенційного впливу на інформаційну безпеку. Серед різновидів таких систем придушення є активні, пасивні та гібридні технології. Активні системи використовують генерацію перешкод у радіочастотних діапазонах, на яких працюють мобільні мережі, завдяки чому відбувається перекриття сигналів. Ці перешкоди ефективно блокують обмін даними між мобільним пристроєм і базовою станцією, перериваючи зв’язок у певній зоні. Пасивні системи включають матеріали, що блокують або поглинають сигнал у фізичному просторі, наприклад, через металеві екрани чи спеціальні конструкції, які обмежують поширення радіохвиль. Гібридні системи, які поєднують активні та пасивні методи, забезпечують максимальну ізоляцію сигналу, що особливо важливо для об’єктів із підвищеними вимогами до інформаційної безпеки, наприклад, для державних установ або стратегічних підприємств.

Разом із технічними аспектами застосування систем придушення мобільного зв'язку необхідно враховувати правові та етичні питання. У багатьох країнах їх використання суворо регулюється законом через потенційні загрози для роботи критично важливих служб. Використання таких систем може порушити роботу служб екстреної допомоги, які також використовують мобільні мережі для забезпечення оперативного зв’язку, що може стати

серйозною проблемою у випадках надзвичайних ситуацій [2]. Крім того, зловживання такими технологіями може розглядатися як втручання в особисте життя громадян, оскільки ці системи можуть перешкоджати звичайному зв’язку та доступу до інформації. Етичні питання використання таких систем вимагають дотримання принципу мінімізації впливу на громадськість і суворого дотримання законодавчих норм, щоб забезпечити баланс між інформаційною безпекою та правами людини.

Перспективи розвитку систем придушення мобільного зв’язку пов’язані з мініатюризацією та підвищенням енергоефективності пристроїв. Інноваційні підходи, такі як використання алгоритмів штучного інтелекту, дозволяють таким системам адаптуватися до змін у радіочастотному середовищі та швидко налаштовувати параметри роботи. Алгоритми ШІ можуть в реальному часі аналізувати спектр частот, виявляти активні сигнали та автоматично коригувати роботу системи так, щоб зменшити вплив на законні канали зв’язку. Це особливо важливо у випадках роботи з мережами нового покоління, таких як 5G, які використовують ширший спектр частот та більш складні методи модуляції сигналу [3]. Застосування когнітивного радіо як частини цих систем дозволяє аналізувати спектр і обирати оптимальні канали для блокування сигналу, знижуючи тим самим ризики втручання в частоти, які використовуються для екстреного зв’язку та інших критично важливих послуг.

Сучасні тенденції розвитку систем придушення зв’язку також передбачають створення компактних мобільних рішень для використання у випадках, де необхідний тимчасовий контроль над мобільним зв’язком. Наприклад, у ситуаціях забезпечення безпеки високопосадовців або під час проведення закритих переговорів, де необхідно уникнути можливих витоків інформації, використовуються переносні системи придушення, що мають обмежений радіус дії і не впливають на навколишні зони [4]. Для стратегічних об’єктів, таких як урядові будівлі, де потрібна постійна ізоляція мобільного зв'язку, застосовуються стаціонарні системи високої потужності, що створюють стабільне середовище без зв’язку в межах великої території.

Таким чином, системи придушення мобільного зв’язку є важливими інструментами забезпечення інформаційної безпеки, однак їхнє використання повинно відбуватися з урахуванням технічних можливостей, правових норм та етичних стандартів. Сучасні системи стають все більш адаптивними, що дозволяє мінімізувати їх вплив на суспільство, зберігаючи при цьому високий рівень захисту інформації. Подальше вдосконалення технологій дозволить ще краще адаптувати їх до нових стандартів зв’язку, таких як 5G, забезпечуючи надійний захист конфіденційної інформації у швидко змінюваних умовах комунікаційного середовища [5].

Список використаних джерел:

1. ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання».

2. Білоконь І.О. Ефективність активних і пасивних систем глушіння у безпекових технологіях. — Харків, 2020.

3. Сухомлин Ю.О. 5G та інформаційна безпека: виклики для систем придушення зв'язку. — Київ, 2022.

4. Кравець М.І. Сучасні технології для безпеки в умовах підвищеного ризику. — Львів, 2019.

5. Поліщук О.М. Перспективи вдосконалення систем придушення зв'язку в умовах зростання вимог до безпеки. — Київ, 2021.

К.В. Суровікін,
Київський національний університет будівництва і архітектури, м. Київ

АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Дротові та бездротові комп'ютерні мережі відіграють важливу роль у повсякденній діяльності. Особи та організації залежать від функціонування власних комп'ютерів і мереж. Вторгнення сторонньої людини може призвести до вартісних відключень мережного з'єднання і втрати роботи. Атаки на мережу мають руйнівні наслідки і можуть призводити до значних витрат часу і грошей через пошкодження або крадіжку важливої інформації або активів.

Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері. Вторгнення сторонньої людини може призвести до вартісних відключень мережного з'єднання і втрати роботи. Атаки на мережу мають руйнівні наслідки і можуть призводити до значних витрат часу і грошей через пошкодження або крадіжку важливої інформації або активів. Таких порушників, які отримують доступ, змінюючи програмне забезпечення або використовуючи вразливості програм, називають суб'єктами загрози. Доступ хакера до мережі може спровокувати чотири типи загроз:

• **Крадіжка інформації**. Втручання до комп'ютерних систем з метою отримання конфіденційної інформації, яку можна використати або продати для різних цілей. Зокрема, крадіжка приватної інформації організації, наприклад даних досліджень і розробок.

• **Втрата даних та маніпулювання**. Зламування комп'ютера з метою знищення або зміни записів даних. Прикладом втрати даних може бути атака, у якій хакер надсилає вірус, що форматує жорсткий диск комп'ютера. Прикладом маніпулювання даними є розбиття системи записів для зміни інформації, наприклад ціни товару.

• **Крадіжка ідентичності.** Є формою крадіжки інформації, при якій особиста інформація викрадається з метою заволодіння персональними даними. Використовуючи цю інформацію, хакер може отримати юридичні документи, подати заявку на кредит і зробити несанкціоновані покупки в Інтернеті. Крадіжка ідентичності -це зростаюча проблема, яка щорічно завдає шкоди на мільярди доларів.

• **Порушення в обслуговуванні.** Перешкоджання законним користувачам скористатися послугами, на які вони мають право. Наприклад: атака відмови в обслуговуванні (DoS) спрямована на сервери, мережні пристрої або канали зв'язку.

Для запобігання цим заргозам в першу чергу необхідно визначити найвразливіші та найважливіші точки в системі, зосередити на них увагу та посилити безпеку. І так поступово від найбільш важливих до найменш важливих точок. Коли найважливіші точки мають бути безумовно захищені від будь якого несанкціонованого доступу чи то ззовні, чи то з середини системи, менш важливі вузли мають також постійно перевірятися на можливість їх використання як для несанкціонованого доступу до системи в цілому, так і для доступу до критичних вузлів. Порушення цього може призвести до проблем від втрати особистої інформації людини до загроз не тільки витоку, але і повного знищення інформації корпоративного або національного рівня, що може призвести не тільки до збитків великого масштабу, а й до людських жертв. Але підвищення рівня безпеки може призвести до значного збільшення дискомфорту користування системою. У такому випадку необхідно переоцінювати рівень важливості безпеки. Хоча при постійному користуванню системою без змін, її безпека буде зменшуватись, адже зловмисник, який бажає отримати доступ як до особистої інформації людини, так і корпоративної, за час, під час якого зміни не проводились зміни та посилення безпеки, може знайти обхідні шляхи або вразливості. Зловмиснику може

знадобитись різна кількість часу в залежності від того наскільки велика команда працює, чи є в них необхідні ресурси і чи знаходяться вони під керівництвом корпорації конкурента або держави-ворога.

Для зменшення вірогідності витоку особистої інформації достатньо притримуватись основних правил поводження в мережі, до прикладу, перевіряти ресурси, якими користується людина, регулярно змінювати та створювати складні паролі, які рекомендовано створювати з використанням цифр, літер різного регістру та іншими символами, або використовувати генератори паролів та змінювати їх з певною періодичністю, використовувати двофакторну аутентифікацію та постійно оновлювати захисне ПЗ.

Для корпорацій заходи інформаційної безпеки мають бути більш жорсткими, щоб по максимуму запобігти будь якому витоку. Для цього розробляються доктрини та концепції до яких входить використання надійного ПЗ, створення відділів, які займаються внутрішньою безпекою компанії та робота з персоналом щодо безпеки, адже порушення будь якого з цих пунктів може призвести до витоку даних, втрати коштів та руйнуванню корпорації в цілому.

До державного рівня ці пункти також стосуються, але ще додається робота з населенням, до прикладу, в умовах війни стає більш жорсткою цензура та контроль інформаційного поля, адже порушення інформаційної безпеки всередині країни призведе вже до людських жертв, що можна спостерігати на прикладі Російсько-Української війни, що почалася в лютому 2014 року, а в лютому 2022 року почалось повномасштабне вторгнення.

Важливим документом, який визначає стратегічні напрями розвитку інформаційної безпеки в країні, є Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016р. «Про Доктрину інформаційної безпеки України». Документ описує ключові напрями дій щодо інформаційної безпеки, а саме: військові дії в інформаційному просторі, ворожу пропаганду, кібератаки та дезінформацію. Але даний документ не описує і інші важливі аспекти безпеки, наприклад, пріоритет дій під час загроз, план програм у цьому напрямі та фінансування цієї програми.

В умовах повномасштабного вторгнення Російської Федерації в Україну питання про необхідність єдиної інформаційної політики стало ще більш актуальним. Враховуючи вказане Президентом України підписано Указ №152/2022, яким введено в дію Рішення Ради Національної Безпеки і Оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану».

Список використаних джерел:

1. Вячеслав Редзюк, Наталія Редзюк. Сучасні проблеми інформаційної безпеки україни та напрями їх вирішення, Публічне управління: концепції, парадигма, розвиток, удосконалення №3/2023, с. 61-62. https://pa.journal.in.ua/index.php/pa/article/view/66/70

2. Делембовський М.М., Шабала Є.Є., Тєрєнтьев О.О., Міжнародний науковий журнал «Грааль науки» №1(Лютий, 2021). б с. 249-250 https://ojs.ukrlogos.in.ua/index.php/grail-of-science/article/view/9132/8880

3. Бібліотечна енциклопедія Харківщини, Інформаційно-комунікаційна безпека https://libenc.korolenko.kharkov.com/informatsiini-tekhnolohii/informacijno-komunikacijna-bezpeka

Р.Є. Писаний,
Київський національний університет будівництва і архітектури, м. Київ

ПРОСТИЙ АЛГОРИТМ РОЗПОДІЛУ ТРАФІКУ ЯК ЗАСІБ ЗАХИСТУ ВІД DDOS АТАК

У сфері кібербезпеки розподіл трафіку є важливим інструментом, оскільки він може знижувати ризики перевантаження мережі та підвищувати стійкість до деяких видів атак, зокрема DDoS-атак.

Сучасні алгоритми, такі як **алгоритм оптимізації кита (Whale Optimization Algorithm, WOA)**, показують високу ефективність у зниженні середнього часу відповіді та попередженні критичних перевантажень[1].

Проте, у малих та середніх мережах, де немає ресурсів для впровадження складних оптимізаційних алгоритмів, примітивні методи можуть забезпечити достатній рівень захисту. Це актуалізує необхідність дослідження базових алгоритмів розподілу трафіку, як-от **round-robin**, які за своєю простотою залишаються ефективним засобом для підтримки стабільності мережі під час атак.

Зокрема, у дослідженні Round-Robin Load Frequency Control (R-RLFC) в поєднанні з механізмом захисту SETM дозволив зменшити вплив DoS-атак на мережу, забезпечивши стабільність під час значних збурень, зокрема, у контексті інтеграції відновлюваних джерел енергії. Використання такого простого підходу до розподілу трафіку дозволяє знижувати кількість переданих пакетів, що зменшує навантаження на мережу та запобігає перевантаженню окремих каналів [2].

Базовий алгоритм розподілу, який працює за принципом Round-Robin, направляє трафік на кожен доступний канал по черзі, знижуючи ризик перевантаження [3]. Цей метод не потребує моніторингу параметрів каналів, таких як затримка чи пропускна здатність, що значно спрощує його реалізацію і знижує навантаження на обладнання. Рівномірний розподіл трафіку не тільки забезпечує стабільність, але й зменшує ризик відмови, коли один із каналів стає основною мішенню для атаки.

При DDoS-атаках, коли масивний потік трафіку націлений на один канал, такий алгоритм дозволяє уникнути ситуації, коли вся мережа зупиняється через перевантаження єдиного маршруту. За умови рівномірного розподілу частина трафіку все одно буде продовжувати передаватися через альтернативні канали, що дозволяє мережі залишатися доступною для легітимних користувачів.

Примітивні алгоритми можна налаштувати на різних маршрутизаторах і комутаторах, які підтримують Policy-Based Routing (PBR) або Equal-Cost Multi-Path (ECMP). Наприклад, Cisco підтримує PBR, що дозволяє налаштувати правила для спрямування трафіку на кілька каналів, що знижує ризик повного блокування мережі під час атаки [4]. MikroTik із функцією RouterOS дозволяє легко налаштувати чергування для всіх типів трафіку, рівномірно розподіляючи його між інтерфейсами.

Простий розподіл трафіку є захистом першої лінії проти атак на перевантаження, оскільки він запобігає накопиченню трафіку на одному каналі. Це важливо для відбиття атак, що мають на меті переповнення мережі, таких як SYN-flood або UDP-flood. Коли канали чергуються у передаванні пакетів, система не зосереджує трафік на одному ресурсі, що робить атаку менш ефективною. Базовий алгоритм забезпечує постійне перемикання між каналами, що ускладнює для зловмисників розподіл ресурсу для повного блокування.

У контексті кібербезпеки навіть базове обладнання може забезпечити додатковий захист, якщо реалізувати алгоритм балансування навантаження. Наприклад, у середовищі Cisco за допомогою CEF (Cisco Express Forwarding) можна налаштувати рівномірний розподіл трафіку між кількома каналами, що мінімізує ризик повного зупинення мережі під час атаки. Аналогічно, ECMP можна налаштувати для рівного розподілу шляхів передачі даних, що є ефективним захистом від атак на перевантаження.

Простий алгоритм розподілу трафіку надає базову стійкість мережі під час високих навантажень або атак, не вимагаючи складного налаштування чи високих ресурсів. Це рішення особливо цінне для малих та середніх компаній, яким потрібен захист, але бракує ресурсів для реалізації дорогих рішень з адаптивним розподілом трафіку. Такий алгоритм може бути основою для розробки більш комплексної системи захисту, доповнюючи його додатковими заходами моніторингу трафіку та управління доступом.

Це демонструє, що навіть найпростіший підхід у розподілі трафіку може забезпечити важливий рівень захисту від перевантаження та атак, дозволяючи мережі працювати стабільно і залишатися доступною для легітимного трафіку навіть у критичних ситуаціях.

Список використаних джерел:

1. AbdulKareem N.M., Zeebaree S.R.M. Optimization of load balancing algorithms to deal with DDoS attacks using whale optimization algorithm. Journal of University of Duhok. 2022. Vol. 25, No. 2. Pp. 65–85.

2. Du X., Liu G., Zhang H., Park J.H., Liu X. Security load frequency control of networked power systems via Round-Robin protocol under denial of service attacks. Journal of the Franklin Institute. 2024. Vol. 361. Issue 16. P. 107155

3. Round-robin load balancing. VMware: веб-сайт. URL: https://www.vmware.com/topics/round-robin-load-balancing (дата звернення: 02.11.2024).

4. Policy-Based Routing (PBR) [Електронний ресурс]: Cisco. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/150SY/configuration/guide/15_0_sy_swcg/policy_based_routing_pbr.pdf (дата звернення: 03.11.2024)

Г.О. Кужентський,
Державний університет інформаційно-комунікаційних технологій, м. Київ

МЕТОДИ ШИФРУВАННЯ ДАНИХ У СУБД ORACLE ЯК ЗАСІБ ПОСИЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Шифрування даних є ключовим елементом забезпечення інформаційної безпеки, особливо в сучасних умовах зростаючих загроз кібератак і несанкціонованого доступу до конфіденційної інформації. Серед систем управління базами даних (СУБД) особливе місце займає Oracle, яка пропонує низку методів і механізмів шифрування, що забезпечують високий рівень захисту даних. У даній роботі буде розглянуто основні методи шифрування даних у СУБД Oracle та їх роль у посиленні безпеки інформаційних систем.

1. Значення шифрування в СУБД Oracle

Oracle як провідна СУБД розробляє інструменти та технології для забезпечення захисту даних на всіх рівнях зберігання та доступу до інформації. Шифрування даних дозволяє перетворювати конфіденційну інформацію у формат, що є недоступним для розуміння без відповідного ключа дешифрування. Це особливо важливо у випадках несанкціонованого доступу до даних або їх крадіжки. Шифрування у Oracle має інтеграцію на рівні апаратного забезпечення та зберігання даних, що зменшує ризик витоків інформації.

2. Основні методи шифрування у СУБД Oracle

Шифрування на рівні транспорту (Data Encryption at Rest)

Цей тип шифрування забезпечує захист даних, коли вони зберігаються у базі, але не захищає під час передачі. В Oracle це реалізовано за допомогою механізму Transparent Data Encryption (TDE), який дозволяє автоматично шифрувати дані у файлах бази даних. TDE підтримує як шифрування колонок, так і шифрування таблиць або файлових систем, зберігаючи продуктивність бази даних.

- **Шифрування колонок** — дозволяє шифрувати тільки конкретні, чутливі колонки в таблицях, наприклад, номери кредитних карт або персональні ідентифікаційні номери.
- **Шифрування таблиць** — застосовується до всього обсягу даних таблиці, забезпечуючи захист на рівні файлів бази даних.

Шифрування під час передачі (Data Encryption in Transit)

Для захисту даних під час передачі між клієнтом і сервером Oracle використовує SSL (Secure Sockets Layer) або TLS (Transport Layer Security). Цей метод забезпечує захист даних під час їх передавання, запобігаючи атакам перехоплення.

Шифрування на рівні додатків

Цей підхід вимагає від розробників забезпечувати шифрування безпосередньо у програмному забезпеченні, що взаємодіє з базою даних. В Oracle даний метод може бути реалізований за допомогою DBMS_CRYPTO – вбудованого пакета для роботи з криптографічними алгоритмами, що забезпечує високу гнучкість.

3. Переваги та виклики застосування шифрування у СУБД Oracle

Застосування методів шифрування даних у СУБД Oracle дозволяє значно підвищити безпеку інформаційних систем, особливо для організацій, що працюють з великими обсягами конфіденційних даних. Проте впровадження шифрування також має деякі виклики, зокрема:

- **Продуктивність** – шифрування і дешифрування даних може знижувати швидкість доступу до них.
- **Управління ключами** – належне зберігання і контроль доступу до ключів шифрування є критично важливим аспектом безпеки.

Висновок

Методи шифрування даних, які пропонує Oracle, дозволяють ефективно захищати конфіденційну інформацію, зберігаючи її від несанкціонованого доступу і кібератак. Системи, що використовують TDE та інші методи, забезпечують високу безпеку даних як під час зберігання, так і при передачі. Проте важливо пам'ятати, що застосування шифрування має свої виклики, які слід враховувати для побудови надійної і ефективної інформаційної безпеки.

Список використаних джерел:

1. Осельський С. В. ПОЯСНЮВАЛЬНА ЗАПИСКА на тему:Методика захисту конфіденційності інформації в базах даних MS SQL та MySQL від sql-атак [Електронний ресурс] / С. В. Осельський. – 2019. – Режим доступу до ресурсу: https://elartu.tntu.edu.ua/bitstream/lib/30595/12/Dyp_%20Oselskyi_2019.pdf.

Г.О. Кужентський,
Державний університет інформаційно-комунікаційних технологій, м. Київ

АНАЛІЗ КІБЕРЗАГРОЗ І ВРАЗЛИВОСТЕЙ У РОЗДРІБНІЙ ТОРГІВЛІ: ПІДХОДИ ДО ЇХ ОЦІНКИ ТА УПРАВЛІННЯ РИЗИКАМИ

У сучасному світі роздрібна торгівля дедалі частіше переходить у цифровий формат, що підвищує ризик виникнення кіберзагроз і вразливостей. Інтернет-магазини, мобільні додатки, POS-системи та онлайн-платежі забезпечують зручність для користувачів, але одночасно створюють можливості для кіберзлочинців, які можуть порушити конфіденційність, цілісність і доступність даних. Для ефективного управління кібербезпекою компанії повинні впроваджувати сучасні методи оцінки ризиків і розробляти стратегії для їх мінімізації.

Ключові кіберзагрози в роздрібній торгівлі

Кіберзагрози в роздрібній торгівлі охоплюють широкий спектр атак, серед яких:

1. **Фішингові атаки та соціальна інженерія**. Хакери обманом отримують доступ до конфіденційних даних, зокрема до інформації про платіжні картки, логіни та паролі співробітників.

2. **Атаки на POS-системи**. POS-системи часто стають об'єктом атак, оскільки можуть зберігати й обробляти платіжні дані клієнтів. Використання застарілого програмного забезпечення та недостатній захист цієї інфраструктури створюють додаткові вразливості.

3. **Шкідливе програмне забезпечення**. Використання шкідливих програм для проникнення у внутрішню мережу компанії й подальшого викрадення даних клієнтів та інформації про фінансові операції.

4. **DDoS-атаки**. Зловмисники можуть перевантажувати сервери компанії, тимчасово виводячи з ладу її онлайн-платформи, що призводить до втрати доходів і погіршення репутації.

Оцінка ризиків та вразливостей

Оцінка кіберризиків у роздрібній торгівлі здійснюється шляхом ідентифікації та аналізу потенційних загроз і вразливостей:

1. **Аудит безпеки інформаційних систем**. Регулярні перевірки інфраструктури для виявлення та усунення вразливостей.

2. **Оцінка потенційних загроз і моделей атак**. Визначення можливих методів атак, які можуть використовувати зловмисники, і моделювання сценаріїв для запобігання їх реалізації.

3. **Аналіз вразливостей**. Використання автоматизованих інструментів для пошуку вразливостей у коді програмного забезпечення, що використовується компанією.

4. **Класифікація та пріоритизація ризиків**. Критичні ризики, такі як загрози для платіжних даних, потребують пріоритетного усунення.

Підходи до управління ризиками

Ефективне управління ризиками передбачає реалізацію заходів, що дозволяють зменшити ймовірність атак та мінімізувати їхні наслідки:

1. **Впровадження багатофакторної аутентифікації**. Додатковий рівень захисту для доступу до конфіденційних даних знижує ймовірність викрадення облікових записів.

2. **Регулярне оновлення програмного забезпечення**. Забезпечує захист від новітніх загроз і ускладнює можливість зловмисникам використовувати відомі вразливості.

3. **Контроль доступу до критичної інфраструктури**. Обмеження доступу до важливих систем лише для тих співробітників, які безпосередньо працюють із ними.

4. **Навчання персоналу**. Підвищення обізнаності про основні методи фішингу та соціальної інженерії дозволяє уникнути більшості атак, спрямованих на людський фактор.

5. **Інцидент-менеджмент та план реагування на кіберзагрози**. Наявність плану дій на випадок кіберінциденту дозволяє швидко відновити роботу й мінімізувати збитки.

Висновок

Успішне управління кіберризиками в роздрібній торгівлі потребує комплексного підходу, що включає як технічні, так і організаційні заходи. Виявлення вразливостей, оцінка ризиків і впровадження ефективних захисних технологій знижує ймовірність виникнення інцидентів та захищає конфіденційну інформацію клієнтів і фінансові активи компанії. Зростаючі загрози вимагають постійного оновлення знань та адаптації до нових методів захисту для підтримання конкурентоспроможності й надійності на ринку.

Список використаних джерел:

1. КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ [Електронний ресурс] – Режим доступу до ресурсу: https://ippi.org.ua/sites/default/files/2024-3.pdf.

Є.О. Шакура,
Київський національно університет будівництва та архітектури, м. Київ

АНАЛІТИЧНІ ІНСТРУМЕНТИ СУБД ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ЗВІТНОСТІ ЗА АНТИКОРУПЦІЙНИМИ МЕХАНІЗМАМИ ЗГІДНО З ISO 37001

Застосування міжнародного стандарту ISO 37001 "Антикорупційні системи управління" у сфері аналізу фінансових транзакцій є важливим аспектом для підвищення ефективності антикорупційних заходів. Стандарт містить вимоги щодо створення і підтримання антикорупційної системи, яка дозволяє організаціям ідентифікувати, контролювати та запобігати корупційним діям. Використання аналітичних функцій сучасних СУБД відкриває нові можливості для автоматизованого виявлення аномальних фінансових транзакцій і генерації звітності для контролю корупційних ризиків.

Використання аналітичних функцій СУБД для виявлення аномалій у фінансових транзакціях

Аналітичні функції СУБД дозволяють реалізувати алгоритми аналізу транзакційних даних, спрямовані на виявлення аномальних патернів поведінки, які можуть свідчити про корупційну діяльність. Далі наведено кілька практичних прикладів реалізації з використанням відповідних функцій.

Приклад 1: Виявлення аномальних транзакцій за допомогою кластеризації

Для виявлення підозрілих транзакцій може використовуватись кластеризація на основі таких функцій, як AVG (середнє значення), STDDEV (стандартне відхилення) та CASE для створення умов виділення аномалій. Наприклад:

- AVG та STDDEV можуть використовуватися для виявлення транзакцій, що значно відхиляються від середніх значень, — такі транзакції можуть вказувати на корупційну діяльність.

- CASE дозволяє створювати правила для класифікації операцій, як-от позначення транзакцій, що перевищують середнє значення більш ніж на два стандартні відхилення, як підозрілих.

Плюси: автоматизація процесу, можливість гнучко налаштувати пороги аномалій залежно від політики безпеки компанії.

Недоліки: потребує попередньої обробки даних та визначення стандартних порогів; висока кількість неправдивих спрацьовувань при широкому розподілі значень.

Приклад 2: Аналіз часових рядів для виявлення порушень

Часові ряди можна реалізувати за допомогою функцій TIMESTAMPDIFF (визначення інтервалів часу) та WINDOW FUNCTIONS (OVER) для аналізу змін у часі. Наприклад:

- TIMESTAMPDIFF визначає різницю між часовими мітками транзакцій, дозволяючи виділити аномально часті повторювані операції.

- WINDOW FUNCTIONS (OVER) застосовується для обчислення середніх показників за визначеними періодами, що дозволяє виявити раптові зростання або падіння у транзакційній активності.

Плюси: висока ефективність для виявлення довготривалих аномалій; дозволяє створювати прогнози на основі історичних даних.

Недоліки: потребує значних ресурсів при обробці великих масивів даних; складність налаштування віконних функцій для специфічних потреб.

Розробка модуля звітності для антикорупційних заходів на базі СУБД

Модуль звітності для антикорупційних заходів на базі СУБД автоматизує формування звітів для моніторингу підозрілих операцій, надаючи інструменти для аналізу даних з різних вимірів (тип операції, час, підрозділ) за допомогою OLAP-кубів. Використання PIVOT-таблиць спрощує візуалізацію звітів, відображаючи ключові показники антикорупційної діяльності, такі як частота перевірок і підозрілі транзакції. Планувальники завдань

забезпечують регулярне оновлення даних, підтримуючи звітність завжди актуальною для вчасного виявлення аномалій.

Модуль також дозволяє експортувати звіти у формати JSON та XML для інтеграції з іншими системами, що забезпечує комплексний аналіз і візуалізацію даних. За допомогою функцій часових рядів можна відстежувати тренди та прогнозувати корупційні ризики, що сприяє коригуванню антикорупційних заходів відповідно до довгострокових змін у фінансовій діяльності.

Приклад 3: Система автоматизованої звітності з використанням OLAP-кубів

Технологія OLAP (On-Line Analytical Processing) дозволяє створювати багатовимірні звіти, які можуть бути адаптовані для перегляду даних з різних кутів, наприклад, типи операцій, підрозділи, контрагенти.

- PIVOT-таблиці дозволяють групувати дані, відображати показники по відділах, користувачах і періодах.

- CROSS JOIN для створення комбінацій показників дозволяє відобразити взаємозв’язки між різними типами даних для подальшого аналізу.

Плюси: надає комплексний огляд даних; можливість швидкого доступу до інформації для ухвалення рішень.

Недоліки: складність впровадження; потребує ресурсів для постійного оновлення даних.

Застосування аналітичних функцій та модулів звітності у СУБД, адаптованих для стандарту ISO 37001, є важливим кроком для підвищення ефективності та прозорості фінансових операцій. Реалізація таких інструментів дає змогу виявляти корупційні ризики в автоматичному режимі, оперативно реагувати на аномальні транзакції та знижувати ймовірність шахрайства. Автоматизована звітність значно спрощує процес контролю і відповідає вимогам міжнародних стандартів щодо антикорупційних заходів.

Список використаних джерел:

1. ISO 37001:2016 "Системи управління боротьбою з корупцією. Вимоги з настановою щодо застосування".

А.С. Сидоренко,
Київський національно університет будівництва та архітектури, м. Київ

ЗАХИСТ ВЕБ-ДОДАТКІВ НА ПРОТОКОЛІ WEBSOCKET: АНАЛІЗ ТА ПРОТИДІЯ РІЗНОМАНІТНИМ АТАКАМ

В умовах стрімкого розвитку веб-технологій та зростаючої потреби в реальночасовій комунікації, протокол WebSocket став невід'ємною частиною сучасних веб-додатків. Проте з його широким впровадженням зросли й ризики безпеки, що вимагає детального аналізу можливих атак та розробки ефективних методів захисту.

Мета дослідження полягає у систематизації існуючих вразливостей протоколу WebSocket та розробці комплексного підходу до захисту веб-додатків від різноманітних типів атак.

У роботі проведено детальний аналіз основних типів атак, що можуть бути здійснені на WebSocket-з'єднання. Це дозволяє глибше зрозуміти механізми, які зловмисники можуть використовувати для компрометації безпеки таких з'єднань. Серед них:

• Cross-Site WebSocket Hijacking (CSWSH) – CSWSH-атака відбувається, коли зловмисник змушує браузер жертви відкривати WebSocket-з’єднання з сервером, на якому користувач авторизований. Якщо сервер не перевіряє заголовок Origin, зловмисник може надсилати запити від імені користувача.

• Denial of Service (DoS) – DoS-атака полягає в перевантаженні сервера надмірною кількістю з'єднань або запитів, що може зробити його недоступним для легітимних користувачів.

• Man-in-the-Middle (MITM) – у MITM-атаці зловмисник може перехоплювати та змінювати повідомлення між клієнтом і сервером. Захист: шифрування з'єднання за допомогою WebSocket Secure (WSS) та використання актуальних SSL-сертифікатів.

• Flood-атаки – у Flood-атаці зловмисник надсилає велику кількість запитів за короткий час, що перевантажує сервер.

• Маніпуляції з WebSocket-фреймами – зловмисник може маніпулювати фреймами, змінюючи їхній вміст чи порядок, що може порушити цілісність даних.

o Запропоновано багаторівневу систему захисту, яка складається з кількох ключових елементів, кожен з яких спрямований на забезпечення комплексної безпеки WebSocket-з'єднань. Серед них:

• Валідація походження запитів (Origin Validation) – цей механізм перевіряє HTTP-заголовок Origin, що дозволяє виявити та блокувати запити з ненадійних джерел. Верифікація походження дозволяє захистити WebSocket-з'єднання від CSWSH-атак, забезпечуючи, що з’єднання ініціюється лише з дозволених доменів.

• Токени автентифікації – кожен запит на встановлення WebSocket-з'єднання має включати унікальний токен, що дозволяє аутентифікувати користувача. Це додатково захищає систему від несанкціонованих з'єднань та запобігає використанню старих або перехоплених токенів.

• Обмеження частоти запитів (Rate Limiting) – ця технологія застосовується для запобігання DoS-атакам, обмежуючи кількість з'єднань або повідомлень від одного користувача за визначений проміжок часу. Rate Limiting забезпечує ефективний контроль за активністю користувачів, запобігаючи перевантаженню сервера.

• Шифрування даних за допомогою WSS – WebSocket Secure (WSS) забезпечує захист даних на рівні транспортного шару завдяки використанню SSL/TLS. Це гарантує, що дані між клієнтом та сервером передаються в зашифрованому вигляді, що унеможливлює MITM-атаки.

• Система моніторингу аномальної активності – ефективна система моніторингу базується на аналізі поведінкових патернів та відстежує кількість з'єднань, частоту повідомлень та виявлення підозрілих шаблонів у даних. Вона дозволяє своєчасно реагувати на аномальну активність, запобігаючи можливим атакам.

На основі проведеного дослідження розроблено практичні рекомендації щодо імплементації захисних механізмів та запропоновано архітектурні рішення для побудови безпечних веб-додатків з використанням WebSocket-протоколу.

Експериментальні результати показали, що запропонований комплексний підхід дозволяє знизити ризик успішних атак на 94% порівняно з базовою реалізацією WebSocket-з'єднання.

Список використаних джерел:

1. Chen, J., & Wang, X. (2023). «WebSocket Security: Comprehensive Analysis and Protection Mechanisms». IEEE Security & Privacy, 21(2), 45-52.

2. Smith, A. (2023). «Modern Web Application Security Patterns». O'Reilly Media.

3. Bright. «WebSocket Security: Top 8 Vulnerabilities and How to Solve Them» https://brightsec.com/blog/websocket-security-top-vulnerabilities/

І.С. Шкурай,
Київський національний університет будівництва і архітектури, м. Київ

ВПЛИВ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ НА БЕЗПЕКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Із розвитком інформаційно-комунікаційних технологій застосування штучного інтелекту (ШІ) у сфері інформаційної безпеки набуло нового рівня. ШІ дозволяє значно підвищити ефективність і швидкість виявлення потенційних загроз, зменшуючи час, необхідний на ручний аналіз інцидентів. Автоматизація процесів аналізу мережевого трафіку та ідентифікації аномалій забезпечує переваги для забезпечення кібербезпеки. Сучасні системи, побудовані на базі машинного навчання, можуть адаптуватися до змін у поведінці загроз, забезпечуючи захист у режимі реального часу. Наприклад, використання алгоритмів класифікації дозволяє оперативно розпізнавати зловмисні дії навіть у випадку, коли вони раніше не були зафіксовані [1].

Водночас широке використання ШІ у сфері інформаційної безпеки супроводжується певними викликами та ризиками. Зокрема, значний ризик становлять атаки на алгоритми ШІ, зокрема маніпуляції з навчальними даними. Якщо зловмисникам вдається ввести хибні дані в систему, це може призвести до її неправильної роботи або навіть до сприяння реалізації атак [2]. Інший аспект ризиків пов’язаний із використанням ШІ для автоматизації кібератак, наприклад, для створення фішингових повідомлень, які важко відрізнити від справжніх [3].

Важливим напрямком є розробка нових методів забезпечення захисту самих систем штучного інтелекту, зокрема захисту їхніх моделей навчання та даних, на основі яких вони працюють. Захист від атак типу «отруєння даних» та маніпуляцій з результатами алгоритмів є одним з актуальних завдань для кібербезпеки. Окрім цього, впровадження методів глибинного навчання та нейронних мереж у безпекові системи дозволяє оптимізувати аналіз поведінки користувачів, прогнозувати дії та попереджати атаки ще до їх фактичного виникнення [4].

Поряд з цим, впровадження ШІ у сферу кібербезпеки потребує комплексного підходу. Необхідно створювати законодавчі та етичні рамки, які б регулювали використання штучного інтелекту, забезпечуючи баланс між захистом приватності даних та надійністю системи [5]. Застосування ШІ може допомогти не лише у виявленні загроз, але й у розробці політик безпеки, що враховують специфіку нових типів атак і технологічних ризиків. Наукова спільнота активно працює над створенням гібридних моделей захисту, що поєднують ШІ з традиційними методами кібербезпеки, для ефективного протистояння сучасним загрозам.

Отже, використання штучного інтелекту в кібербезпеці відкриває значні можливості, проте потребує розробки спеціалізованих захисних механізмів для протидії новим ризикам. Для цього необхідна співпраця експертів із кібербезпеки, ШІ та права, що забезпечить безпеку у нашій сфері.

Список використаних джерел:

1. Мєшков В. Аналіз систем інтелектуального моніторингу трафіку комп’ютерної мережі для систем виявлення атак // Information Technology: Computer Science, Software Engineering and Cyber Security. 2023. №1. С. 85–92.

2. Котенко Д., Хлапонін Ю. Штучний інтелект у системах виявлення і запобігання кібератакам: перспективи та виклики // Підводні Технології. 2024. №1. С. 48–55.

3. Бенчак В., Рудянова Т. Використання штучного інтелекту в кібербезпеці // The 10th International scientific and practical conference "Topical aspects of modern scientific research" (13–15 червня 2024 р.). Tokyo, Japan: CPN Publishing Group, 2024. С. 181–184.

4. Примиська С., Кримська А., Супрун О. Стратегії забезпечення безпеки даних у системах штучного інтелекту // Таврійський науковий вісник. Серія: Технічні науки. 2024. №2. С. 88–99.

5. Зозуляк О. Штучний інтелект як об’єкт цивільно-правового регулювання // Матеріали міжнародної науково-практичної конференції, присвяченої пам’яті проф. В. П. Маслова. 2022. С. 95–102.

Є.В. Бондаренко,
Державний університет інформаційно-комунікаційних технологій, м. Київ
В.Р. Сокольвак, Д.М. Бичек
Національний авіаційний університет, м. Київ

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ БЕЗДРОТОВИХ КАНАЛІВ ПЕРЕДАЧІ ДАННИХ В УМОВАХ ВПЛИВУ НАВМИСТНИХ ІМПУЛЬСНИХ НЕФЛУКТАЦІЙНИХ ЗАВАД

Побудова гнучких мереж збирання та керування даними є завданням, яке постійно актуальне в різних галузях науки та промисловості. Одним з видів таких мереж є мережі, засновані на бездротових технологіях передачі даних.

Серед усього різноманіття технологій цифрової передачі корисних даних, що використовуються в сучасних безпроводових телекомунікаційних мережах, чільне місце займають технології передачі сигналів з багатопозиційною фазовою маніпуляцією (БФМ).

Сигналам, що передаються по технології БФМ притаманний весь спектр зовнішніх та внутрішніх негативних збурень, перешкод та впливів, які можуть достатньо сильно впливати на якість передачі та отримання інформації через безпроводову мережу. Поряд з постійно існуючими флуктаційними завадами також на якість передачі даних через бездротові мережі можуть чинити завади, що виникають по випадковим законам та можуть мати як природні джерела так і бути навмисно сформованими з метою перешкоджання отримання корисної інформації засобами даної мережі [1].

Таким чином формується актуальне наукове задання щодо визначення та оцінки впливу навмисних нефлуктаційних імпульсних завад на ефективність передачі даних бездротовими каналами.

Проблема впливу навмисних нефлуктаційних імпульсних завад на ефективність функціонування бездротових телекомунікаційних мереж

Бездротові технології - по суті, є окремим випадком інформаційних технологій, які застосовуються, коли необхідно передати сигнал між двома і більше об'єктами, при цьому не використовуючи дроти для їх зв'язку.

На поточний момент нам доступно безліч бездротових технологій, таких як Wi-Fi, Bluetooth, WiMAX, ZigBee, GPRS, NFC, LTE і т.д. Актуальним є питання їх огляду, аналізу, оцінки та порівняння з метою визначення можливостей щодо вирішення конкретного технічного завдання по розробці бездротової мережі збору та обробки інформації на основі технології БФМ [1,2].

Технологія БФМ, при її використанні, реалізується на простих алгоритмах обробки пакетів даних та на основі алгоритмів швидкого перетворення Фур’є, що обумовлює простоту апаратної реалізації при можливості забезпечення одночасної передачі сигналів різного спектру через одну мережу.

Сигнал з БФМ на тактовому інтервалі Т приймає одне з М можливих значень [2,3]:

$$S_I(t) = A_0 \cos(\omega_0 t + \varphi_i + \varphi_c) \quad (1)$$

У радіосистемах для прийому сигналів з БФМ використовуються два методи – когерентний (багатоканальній або квадратурний) та некогерентний автокореляційний прийом сигналу.

В залежності від умов розповсюдження радіохвиль, місця, часу організації, технічних характеристик каналів радіозв'язку, в них присутня велика кількість різних завад. Це завади

флуктуаційного (шумового) та нефлуктуаційного типу, адитивні і мультиплікативні. До числа найбільш розповсюджених нефлуктуаційних завад відносяться сигналоподібні, у тому числі вузькосмугові, наприклад, гармонійні, а також навмисна імпульсні завади [2,3].

Зазвичай, на вході приймача безпроводової системи передачі даних крім корисного сигналу присутня шкідлива складова, яка включає білий гаусовський шум n(t) і низку різних нефлуктуаційна завада, суму яких позначимо як *Sn(t) :*

Таким чином, прийнятий гармонійний цифровий сигнал $x(t)$, буде мати вигляд:

$$x(t) = S_i(t) + S_n(t) + n(t) \tag{3}$$

Особливості впливу імпульсної нефлуктаційної завади на сигнал БФМ

В загальному вигляді, поява нефлуктаційної завади може внести елементи спотворення в структуру сигналу, що приводить до формування помилки прийому окремих символі сигналу БФМ. Відповідно проведеним дослідженням мінімальна ймовірність помилки на символ, що досягається, при оптимальній когерентній обробці сигналу БФМ з M визначається виразом [2]:

$$P_S(M) \approx 2\Phi\left(\sqrt{2\pi\gamma_b}\sin\frac{\pi}{M}\right), \quad \Phi(x) = \frac{1}{2\pi\int_x^\infty e^{-r^2/2}\,dt} \tag{4}$$

де $\gamma_b = E_B / N_0$ – відношення сигнал/шум, що перераховане на один біт інформації.

Виходячи з вищеподаного, можна зазначити що функціонування бездротової мережі передачі даних на базі технології БФМ в умовах впливу імпульсних нефлуктаційних завад буде вимагати втілення заходів підвищення завадостійкості цифрових сигналів.

Особливо це актуально з врахуванням позиційності сигналів. Наприклад, при позиційності M ≥ 4, саме ці сигнали перспективні з точки зору підвищення пропускної спроможності каналів передачі даних в умовах впливу нефлуктаційних завад.

Дані обставини формують нове наукове задання щодо розробки окремої моделі формування імпульсної нефлуктаційної завади та проведення досліджень по її впливу на імовірність символьної помилки сигналу БФМ

Висновок:

1. В роботі розглянуті питання оцінки особливостей функціонування бездротових каналів передачі даних в умовах впливу навмисних імпульсних нефлуктаційних завад

2. Встановлено, що функціонування бездротової мережі передачі даних на основі технології БФМ в умовах впливу нефлуктаційних завад буде характеризуватися спотворенням символів сигналів та зростанням імовірності символьної помилки.

3. З метою зменшення впливу на завадостійкість ТКМ на базі сигналів з БФМ запропонована відповідна методологія оцінки впливу нефлуктуаційних завад на завадостійкість прийому дискретних сигналів з багатопозиційною фазовою маніпуляцією.

Етапом її реалізації в статті визначено розробку окремої моделі, призначеної для оцінки завадостійкості бездротової мережі при прийомі дискретних сигналів БФМ в умовах впливу нефлуктуаційних імпульсних завад

Список використаних джерел:

1. Балашов В. О., Воробієнко П. П., Ляховецький Л. М., Педяш В. В. Системи передавання широкосмуговими сигналами. Одеса: Вид. центр ОНАЗ ім. О.С. Попова, 2012. 336 с.

2. Попівський В.В., Лемешко О.В., Ковальчук В.К. Плотніков М.Д., Картушин Ю. П. (2012) Телекомунікаційні системи та мережі. Структура й основні функції. Том 1. URL: http://www.znanius.com/3534.html.

3. Стеклов В.К. Костік Б.Я., Беркман Л.Н. Сучасні системи управління в телекомунікаціях. Київ: Техніка, 2005. 400 с.

Р.С. Хворостяний, Р.М. Сад
Державний університет інформаційно-комунікаційних технологій, м.Київ
П.В. Верещак,
Національний авіаційний університет, м.Київ

АНАЛІЗ ПРОЦЕСУ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ ТА СПОСОБІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО НИХ

Питання захисту інформації від несанкціонованого доступу набуло актуальності відколи людство навчилось писемності та передачі інформації іншими шляхами. З тих пір існувала інформація, яка має бути доступною не для всіх. Ті хто володів такою інформацію, вдавалися до різних способів її захисту. Нині в епоху комп'ютеризації, контроль та управління різними об'єктами, благополуччя та навіть життя багатьох, залежить від забезпечення інформаційної безпеки, комп'ютерних систем обробки інформації. Для нормального та безпечного функціонування цих систем необхідно підтримувати їх безпеку та цілісність, тобто задіяти так званий «спеціальний захист» даних.

Персональні данні користувача

Термін «персональні дані» є вхідним початком застосування рагального регламенту захисту даних (GDPR). Лише якщо обробка даних стосується персональних даних, застосовується Загальний регламент захисту даних. Термін визначено ст. 4 (1) (GDPR). Персональні дані - це будь-яка інформація, яка стосується ідентифікованої або ідентифікованої фізичної особи[1].

Суб'єкти даних можна ідентифікувати, якщо їх можна прямо чи опосередковано ідентифікувати, особливо за допомогою ідентифікатора, такого як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або одна з кількох спеціальних характеристик, які виражають фізичні, фізіологічні, генетичні ментальна, комерційна, культурна чи соціальна ідентичність цих фізичних осіб[2]. На практиці сюди також входять усі дані, які будь-яким чином належать або можуть бути присвоєні особі. Наприклад, номер телефону, номер кредитної картки або персональний номер особи, облікові дані, номерний знак, зовнішній вигляд, номер клієнта або адреса – все це персональні дані.

Локальна комп'ютерна мережа

Інститут інженерів з електротехніки та електроніки (IEEE) визначив локальну мережу як «систему передачі даних, яка дозволяє кільком незалежним пристроям безпосередньо спілкуватися один з одним у межах географічної області помірного розміру через фізичний канал зв'язку з помірними швидкостями»[2,3].

Зазвичай локальна мережа через загальну мережеву операційну систему з'єднує сервери, робочі станції, принтери та пристрої масової пам'яті, дозволяючи користувачам спільно використовувати ресурси та функції, які надає локальна мережа[3].

Проблема безпеки локальної комп'ютерної мережі

Архітектура ЛКМ та специфіка її роботи надає змогу зловмиснику знаходити або спеціально створювати прогалини для прихованого доступу до інформації, враховуючи різноманітність відомих на даний момент зафіксовних злочинних дій, наштовхує на думку що даних лазівок існує ми може бути створено набагато більше[2,3].

Несанкціонований доступ до локальної комп'ютерної мережі

Архітектура ЛКМ та специфіка її роботи надає змогу зловмиснику знаходити або спеціально створювати прогалини для прихованого доступу до інформації, враховуючи різноманітність відомих на даний момент зафіксовних злочинних дій, наштовхує на думку що даних лазівок існує ми може бути створено набагато більше[1,3].

Несанкціонований доступ до інформації, що знаходиться в ЛКМ буває:

- прямим – (з фізичним доступом до елементів ЛКМ).
- непрямим – (без фізичного доступу до елементів ЛКМ);

Використання програмних засобів для несанкціонованого доступу до локальної комп'ютерної мережі

Клас шкідливих ПЗ (далі – віруси), що використовуються для НС, складають розроблені комп'ютерні віруси, троянські коні (закладки) та засоби проникнення у віддалені системи через локальні та глобальні мережі.

За середовищем існування розрізняють файлові, завантажувальні, комбіновані (файловозавантажувальні), пакетні та мережні віруси. Файлові віруси звичайно заражають файли з розширеннями .comта .exe. Однак, деякі їх різновиди можуть інфікувати файли й інших типів (.dll, .sys, .ovl, .prg, .bat, .mnu), при цьому вони, як правило, втрачають здатність до розмноження[1,2,3].

У свою чергу, за способом зараження середовища існування файлові віруси поділяють на резидентні та нерезидентні. Останні починають діяти тільки під час запуску зараженого файла на виконання і залишаються активними обмежений час[1].

Для мережевого захисту процесу обробки персональних даних в локальних комп'ютерних мережах необхідно провести роботу по створенню системи безпеки інформації. Мета функціонування якої – захист персональних даних.

Цілі функціонування системи безпеки інформації подано в наступному переліку.

Забезпечення конфіденційність даних під час їх зберігання, обробки або передачі в локальній мережі;

Підтримування цілісності даних під час їх зберігання, обробки або передачі в локальній мережі.

Підтримку доступність даних, що зберігаються в локальній мережі, а також здатність своєчасно обробляти та передавати дані.

Висновок:

1. В роботі розглянуті питання процесу обробки персональних даних в локальних комп'ютерних мережах та способів несанкціонованого доступу до них

2. Розглянули шляхи та канили витоку інформації що можуть бути причиною несанкціонованого доступу до персональних даних через локальну мережу підприємства.

3. Визначені цілі впровадження системи безпеки інформації в локальних комп'ютерних мережах.

Список використаних джерел:

1. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. — К. : Вид. ДУІКТ, 2009. — 292 с.

2. Максименко Ю.Є. Теоретико-правові засади забезпечення кібербезпеки України: дис. канд. юрид. наук :12.00.01 / Ю.Є. Максименко. — К., 2007. — 186 с.

3. Марущак А.І. Кібербезпека як об'єкт дослідження правової науки / А.І. Марущак // Актуальні проблеми управління кібербезпекою держави: зб. матер. наук.- прак. конф., 17 березня 2010 року м. Київ. — К. : Наук. вид. відділ НА СБ України, 2010. — С. 36−41

Б.В. Чабан
Державний університет інформаційно-комунікаційних технологій, м. Київ

МАТЕМАТИЧНА МОДЕЛЬ МАТЕРІАЛЬНО-РЕЧОВОГО КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ

Вступ та загальна постановка проблеми. Технічний захист інформації сьогодні стає все більш актуальним, особливо через ризики витоку даних через матеріально-речові канали, які важко контролювати традиційними методами. Матеріально-речові канали передбачають передачу даних через фізичні носії, такі як документи та електронні накопичувачі, і є складними для моніторингу через потребу в фізичному доступі. Основні ризики включають несанкціоноване копіювання, відновлення залишкових даних і використання вразливостей носіїв, що потребує точного моделювання для зниження можливих витоків. Розробка математичної моделі для таких каналів необхідна для оцінки ймовірності витоку, обсягу інформації та створення ефективних захисних заходів.

Огляд існуючих методів математичного моделювання матеріально-речового каналу. Існуючі методи математичного моделювання матеріально-речового каналу витоку інформації базуються на ймовірнісних, статистичних і диференційних підходах, які дозволяють оцінювати ризики та обсяги витоку інформації залежно від умов середовища і рівня доступу до носія. Ймовірнісні моделі використовуються для оцінки ймовірності доступу зловмисника до носія та обчислення ризиків, тоді як чисельні методи, такі як метод Монте-Карло, допомагають моделювати різні сценарії можливих витоків [1]. Диференційні рівняння застосовуються для опису динаміки витоку інформації з часом і дозволяють врахувати вплив середовищних факторів на швидкість витоку даних через фізичні носії [2]. Ці методи створюють основу для комплексного підходу до захисту інформації через матеріально-речові канали.

Схема математичної моделі. Для розробки математичної моделі матеріально-речового каналу витоку інформації необхідно врахувати процеси передачі інформації через фізичні об’єкти (рис. 1).

Рис. 1. Блоки моделі та взаємодія між ними

Модель може складатися з таких блоків:

1. Блок носія інформації: описує тип носія (наприклад, паперові документи, жорсткі диски, накопичувачі) та його ключові характеристики, що впливають на вразливість до витоку.

2. Блок середовища передачі: визначає фізичні умови, за яких можливий доступ до носія, а також шляхи та можливі перешкоди для передачі інформації.

3. Блок користувача: моделює поведінку користувача, включаючи ймовірність порушення процедур захисту та вплив людського фактора на ймовірність витоку.

Взаємодія між блоками описується через систему залежностей, де, наприклад, зміна типу носія або умов середовища впливає на рівень захищеності та ймовірність несанкціонованого доступу.

Концепція моделювання процесів витоку інформації через матеріально-речові канали

Для математичного опису процесів, що відбуваються в матеріально-речовому каналі, доцільно використовувати ймовірнісні та статистичні методи, а також методи теорії черг та надійності. За допомогою диференційних рівнянь можливо описати швидкість та обсяг витоку інформації, враховуючи час зберігання, надійність носія та його захищеність. Наприклад, можна використовувати рівняння виду:

$$\frac{dI}{dt} = -k \cdot I(t), \tag{1}$$

де $I(t)$ – обсяг інформації, що може бути викрадений за певний час; k – коефіцієнт витоку, залежний від рівня захищеності носія та умов середовища.

Система рівнянь, що описують процес витоку інформації, враховує основні чинники витоку:

1. Ймовірність доступу: імовірність того, що носій стане доступним для зловмисника, може бути виражена як функція часу та захищеності об'єкта:

$$P_a = f(t, S), \tag{2}$$

де t – час, протягом якого носій залишається без нагляду; а S – параметр захищеності.

2. Швидкість витоку: залежить від типу носія, обсягу інформації та рівня доступності:

$$v = g(I_0, T, D), \tag{3}$$

де I_0 – початковий обсяг інформації; T – час контакту; а D – рівень доступності носія для зловмисника.

3. Об'єм витоку: загальний обсяг інформації, що витікає за час t, може бути обчислений інтегруванням швидкості витоку в часі:

$$I(t) = \int_0^t v dt. \tag{4}$$

Ця система рівнянь дозволяє оцінити обсяг та ймовірність витоку інформації через матеріально-речовий канал, враховуючи основні фактори ризику.

Висновок. Запропонована математична модель матеріально-речового каналу витоку інформації дозволяє кількісно оцінювати рівень ризику витоку через фізичні об'єкти. Вона може використовуватись для розробки ефективних заходів захисту, враховуючи конкретні характеристики середовища, носія інформації та поведінки користувачів.

Список використаних джерел:

1. Половінкін, М. І., Глухов, С. І., Черній, Д. І., & Пархоменко І. І. (2024). Алгоритм виявлення витоку інформації на основі перевірки статистичних гіпотез. Телекомунікаційні та інформаційні технології. No 1(82). 95–105. https://doi.org/10.31673/2412-4338.2024.019505.

2. Shcheblanin, Y., & Rabchun, D. (2018). Математична модель порушника інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(1), 63–72. https://doi.org/10.28925/2663-4023.2018.1.6372.

Ю.І. Катков,
доктор технічних наук, професор кафедри комп'ютерних наук, ННІТ, ДУІКТ, Київ, Україна
М.М. Бураков,
Студент групи КНДМ-63, ННІТ, ДУІКТ, Київ, Україна

ПРОБЛЕМИ БЕЗПЕКИ СИСТЕМ АВТОМАТИЗОВАНОГО ЗБОРУ ДАНИХ ПРО КОНФІГУРАЦІЇ СЕРВЕРНОГО ОБЛАДНАННЯ

Анотація. Система автоматизованого збору даних про конфігурації серверного обладнання має вирішувати питання безпеки, оскільки збирає, зберігає і обробляє конфіденційну інформацію про IT-інфраструктуру. Такі системи мають проблеми безпеки, а саме: несанкціонований доступ; ненадійна аутентифікація та контроль доступу; вразливості в програмному забезпеченні; компрометація зібраних даних; атаки на збирання даних (Man-in-the-Middle, DoS); внутрішні загрози (інсайдери); надмірна довіра до зовнішніх постачальників; недостатня сегментація мережі та інші. Звідси безпека систем автоматизованого збору даних про конфігурації серверного обладнання є критично важливою для захисту IT-інфраструктури. Інвестування у сучасні методи захисту, регулярні оновлення та моніторинг допоможуть зменшити ризики та забезпечити стабільність роботи систем.

Постановка завдання. Проблеми безпеки системи автоматизованого збору даних про конфігурацію серверного обладнання є важливим аспектом загальної безпеки організації. Вразливість цих систем до кібератак і несанкціонованого доступу становить серйозну загрозу. З появою нових технологій та методів атак, ризики для таких систем зростають, що може призвести до крадіжки конфіденційних даних, порушення роботи серверного обладнання та інших серйозних наслідків для організації. Проте система автоматизованого збору даних про конфігурації серверного обладнання має вирішувати питання безпеки щодо IT-інфраструктури. Тому виникає завдання визначення проблем безпеки, зрозуміти їх механізм дії та розробка варіантів вирішення. Це є своєчасним та актуальним завданням.

Ключові слова: *безпека даних, конфігурація серверного обладнання, аутентифікація, автентифікація, кібербезпека*.

Мата дослідження. Підвищення ефективності безпеки системи автоматизованого збору даних про конфігурації серверного обладнання через дослідження актуальних проблем безпеки, що дозволить знизити трудовитрати та мінімізувати кількість помилок при адмініструванні серверного обладнання.

Результати дослідження. В результате дослідження визначені наступні проблеми:

1. Несанкціонований доступ:

• *Сутність проблеми*. Зловмисники можуть спробувати отримати доступ до системи автоматизованого збору даних про конфігурації серверів для викрадення інформації про структуру та параметри серверного обладнання, конфігурацію серверів або для втручання в їхню роботу, що може призвести до значних ризиків, коли зловмисник дізнатися про слабкі місця в конфігурації серверів, уразливості програмного забезпечення чи застарілі версії, що використовуються. А це надає можливість точного планування подальших атак або шкідливого втручання в роботу серверів [1].

• *Можливі ризики.* Несанкціонований доступ до даних про структуру та параметри серверного обладнання може призвести до серйозних збоїв, а також полегшити підготовку до кібератак, таких як DDoS або атаки з метою порушення конфіденційності. Зокрема, отримавши доступ до цих даних, зловмисники можуть змінювати конфігурації, завантажувати шкідливе програмне забезпечення або навіть вивести сервери з ладу через перевантаження або саботаж, що може призвести до зупинки важливих бізнес-процесів. Атаки на систему автоматизованого збору даних часто здійснюються за допомогою експлойтів або шкідливих скриптів, які використовують недоліки в конфігураціях серверів або помилки в захисті мережі.

• *Рішення.* Для захисту системи автоматизованого збору даних про конфігурацію серверів необхідно впроваджувати комплексні заходи кібербезпеки, які включають шифрування даних, контроль доступу, автентифікацію на основі багатофакторної ідентифікації та регулярний моніторинг. Використання багаторівневої аутентифікації (наприклад, MFA — багатофакторна аутентифікація), налаштування ролей доступу (role-based access control, RBAC) та шифрування під час передачі даних (SSL/TLS). Важливо також забезпечити ізоляцію системи збору даних від загальнодоступних мереж, використовуючи сегментацію мережі, що зменшує ризик несанкціонованого доступу.

2. Ненадійна аутентифікація та контроль доступу:

• *Сутність проблеми*: Недостатньо захищені облікові записи або слабкий контроль доступу можуть дозволити зловмисникам отримати привілейований доступ.

• *Можливі ризики*: Зловмисники можуть змінювати конфігурації серверів або відключати критичні системи моніторингу.

• *Рішення:* Посилена політика паролів, обмеження доступу за IP-адресами, використання журналів доступу для відстеження активності користувачів.

3. Вразливості в програмному забезпеченні:

• *Сутність проблеми*: Програмне забезпечення, яке використовується для автоматизації збору даних, може мати вразливості, які зловмисники можуть використовувати для отримання доступу або атак на систему.

• *Можливі ризики:* Хакери можуть експлуатувати вразливі компоненти системи для впровадження шкідливого програмного забезпечення, або для викрадення конфіденційної інформації.

• *Рішення:* Регулярне оновлення програмного забезпечення та виправлення вразливостей (патч-менеджмент), проведення регулярних перевірок безпеки (security audits).

4. Компрометація зібраних даних:

• *Сутність проблеми***:** Дані про конфігурацію серверного обладнання можуть бути зламані або викрадені, якщо вони не захищені належним чином.

• *Можливі ризики*: Якщо дані потраплять у руки зловмисників, це може дати їм повну картину інфраструктури, що значно спростить проведення атак.

• *Рішення:* Шифрування даних на рівні зберігання та під час передачі, розмежування прав доступу до даних, а також регулярне резервне копіювання.

5. Атаки на збирання даних (Man-in-the-Middle, DoS):

• *Сутність проблеми***:** Атаки типу "людина посередині" (Man-in-the-Middle) можуть дозволити зловмисникам перехоплювати або підміняти дані під час їх передачі між сервером та системою моніторингу. Атаки на відмову в обслуговуванні (DoS) можуть зупинити або сповільнити процес збору даних.

• *Можливі ризики*: Перехоплені дані можуть бути змінені або використані для подальших атак. Атака DoS може призвести до втрати контролю над серверним обладнанням.

• *Рішення*: Використання шифрування на рівні мережевої передачі даних (TLS), встановлення системи виявлення та запобігання атак (IDS/IPS), а також обмеження доступу до мережі збирання даних через VPN або захищені канали.

6. Внутрішні загрози (інсайдери):

• *Сутність проблеми:* Співробітники або особи з доступом до системи можуть використовувати свої привілеї для викрадення або саботажу даних.

• *Можливі ризики:* Інсайдери можуть використовувати свої права для нанесення збитків організації, зміни конфігурації серверів або пошкодження систем моніторингу.

• *Рішення:* Створення політики мінімальних привілеїв, постійний моніторинг дій користувачів, ведення журналів аудиту.

7. Надмірна довіра до зовнішніх постачальників:

• *Сутність проблеми:* Якщо система збору даних використовує рішення сторонніх постачальників, існує ризик витоку даних через їхні уразливості або ненадійність.

- *Можливі ризики:* Зловмисники можуть атакувати інфраструктуру постачальника, щоб отримати доступ до вашої системи.
- *Рішення:* Перевірка безпеки сторонніх рішень, використання угод про рівень обслуговування (SLA), постійний моніторинг безпеки партнерських систем.

8. Недостатня сегментація мережі:

- *Сутність проблеми:* Відсутність чіткої сегментації мережевої інфраструктури може дозволити зловмисникам отримати доступ до всієї системи через одну уразливу точку.
- *Можливі ризики:* Атаки можуть швидко поширюватися на інші частини IT-інфраструктури, що призведе до значних пошкоджень.
- *Рішення:* Сегментація мережі, ізоляція критичних компонентів, використання брандмауерів та систем контролю доступу.

9. Можливі ризики витоку даних.

- *Сутність проблеми:* Зловмисники, отримавши доступ до даних, можуть підготуватися до проведення цілеспрямованих атак, таких як DDoS-атаки для перевантаження серверів або атаки з порушенням конфіденційності, зокрема, шляхом крадіжки чутливої інформації або маніпуляції даними конфігурацій [2].
- *Можливі ризики:* Це створює потенційні загрози для бізнесу, включаючи втрату доступності серверів, порушення роботи критичних процесів та значні фінансові збитки.
- *Рішення:* Для захисту систем автоматизованого збору даних про конфігурацію серверів застосування багаторівневої аутентифікації (MFA) забезпечує додаткові рівні безпеки, вимагаючи підтвердження користувачів за допомогою кількох факторів автентифікації, таких як пароль, одноразовий код (OTP) або біометричні дані. Це значно знижує ризик несанкціонованого доступу навіть у випадку, якщо облікові дані були скомпрометовані [4]. Для зниження ризику несанкціонованого доступу необхідно впроваджувати політику багатошарової безпеки, яка включає багатофакторну автентифікацію, обмеження доступу до системи лише для авторизованих користувачів та регулярний аудит безпеки для виявлення та усунення вразливостей [3]. Інструменти моніторингу, які контролюють підозрілу активність, можуть допомогти ідентифікувати потенційні загрози та оперативно на них реагувати. Такий підхід також спрощує управління доступом в організації та підвищує безпеку. Шифрування даних під час передачі за допомогою SSL/TLS забезпечує безпечний канал для обміну інформацією, захищаючи її від перехоплення і модифікації під час пересилання через незахищені мережі. Використання SSL/TLS дозволяє підтвердити автентичність сервера, забезпечити цілісність та конфіденційність даних [5]. Ця технологія є стандартом захисту для чутливої інформації та широко застосовується у фінансових і державних установах для захисту від атак типу «людина посередині» (Man-in-the-Middle, MITM).

Висновки:

1. Безпека систем автоматизованого збору даних про конфігурації серверного обладнання є критично важливою для захисту IT-інфраструктури.
2. Інвестування у сучасні методи захисту, регулярні оновлення та моніторинг допоможуть зменшити ризики та забезпечити стабільність роботи систем.
3. Для мінімізації ризиків необхідно впроваджувати комплексні заходи кібербезпеки, включаючи багаторівневу автентифікацію, управління ролями доступу та шифрування даних під час передачі. Використання цих стратегій дозволить не лише захистити конфіденційну інформацію, але й забезпечити безперервність роботи критичних бізнес-процесів, підвищуючи загальний рівень безпеки в організації.

Список використаних джерел:

1. Andress, J. (2019). "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice." – Режим доступу до ресурсу*: URL: https://web.xidian.edu.cn/yanzheng/files/20160919_170521.pdf (дата звернення: 29.10.2024).*

2. Shon Harris, F. (2013). "CISSP All-in-One Exam Guide." [Електронний ресурс] / – Режим доступу до ресурсу*:* *URL:https://eduarmandov.wordpress.com/wp-content/uploads/2017/05/ security-cissp-all-in-one-exam-guide-6th-edition.pdf (дата звернення: 29.10.2024).*

3. Харріс Шон. **CISSP All-in-One Exam Guide** / Шон Харріс. – McGraw-Hill Education, 2019. – 1280 p.10 notable critical infrastructure cybersecurity initiatives in 2023. Центр ресурсів CSO

4. Столлінгс В., Браун Л. **Computer Security: Principles and Practice** / Вільям Столлінгс, Лія Браун. – Pearson, 2018. – 624 p.

5. Андресс Джейсон. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice / Джейсон Андресс. – Syngress, 2014. – 352 p.

В.Р. Аношко,
Державний університет інформаційно-комунікаційних технологій, м.Київ
М.Є. Мартинов, А.О. Лодигін
Національний авіаційний університет , м.Київ

АНАЛІЗ ОСНОВНИХ МЕРЕЖЕВИХ ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Однією важливих та характерною проблем сьогодення стало питання забезпечення безпеки функціонування державних установ, підприємств, загальнонаціональних систем та мереж забезпечення життєдіяльності населення які кваліфікуються як об'єкти інформаційної діяльності. Виходячи з важливих змін в розвитку науки та техніки, ускладнення процесів економічного життя та суспільних відноси, розвитку різноманітних технологій, на основі яких функціонують вказані об'єкти можна зробити висновок про те, що одним з факторів, який забезпечує якість функціонування є різноманітна інформація [1].

Зі всього різноманіття корпоративної інформації, що циркулює каналами передачі інформації на об'єкті інформаційної діяльності,частина такої інформації підпадає під всі види обмежень на передачу, збереження та захист та кваліфікується як інформація з обмеженим доступом (ІзОД). Забезпечення ефективної діяльності технічної системи охорони об'єктів інформаційної діяльності в напрямку запобігання витоку інформації мережевими засобами є актуальним заданням, вирішенню якого присвячена дана робота.

Проблема впливу шкідливого програмного забезпечення на ефективності функціонування технічної системи охорони об'єкта інформаційної діяльності через мережеві канали передачі інформації.

Під терміном *шкідливе програмне забезпечення* (англ. - malware) розуміють програмні засоби, що несанкціоновано впроваджують у комп'ютерну систему і які здатні викликати порушення політики безпеки, завдавати шкоди інформаційним ресурсам, а в окремих випадках — і апаратним ресурсам комп'ютерної системи [1,2]. Шкідливе програмне забезпечення класифікують за різними ознаками. Наприклад, у монографії його поділяють на дві категорії — таке, що виконує деструктивні функції, і таке, що їх не виконує. В інших джерелах виділяють як окремий клас шкідливого програмного забезпечення так звані програмні закладки. Іноді термін *програмні закладки* (рос. — программные закладки, англ. — program bug) застосовують майже до всього шкідливого програмного забезпечення, крім комп'ютерних вірусів [1,2].

Шкідливі програмні засоби можуть чинити негативний вплив по дікільком напрямкам.. По-перше, як уже зазначалося, вони у будь-якому разі порушують політику безпеки. По-друге, навіть якщо розробник шкідливого засобу не передбачив у ньому руйнівних функцій, такий засіб може призвести до значних втрат — як через необхідність спрямування зусиль

висококваліфікованих (і високооплачуваних) фахівців на виявлення, ідентифікацію, видалення шкідливого програмного засобу, так і через недоступність систем.

Мережеві програмні застосунки несанкціонованого витоку інформації.

Програмні закладки — це програми або окремі функції програм, що тривалий час працюють у комп'ютерній системі, здійснюючи заходи, спрямовані на приховування свого існування від користувача. Нижче наведено класифікацію, яка враховує «новинки» розробників «троянських коней» [2,3].

Перехоплення і передавання інформації:

- крадіжка паролів;
- шпигунські програми.

Порушення функціонування систем («логічні бомби»):

- знищення інформації;
- зловмисна модифікація інформації;
- блокування системи.

Модифікація програмного забезпечення:

- утиліти віддаленого адміністрування (люки);
- інтернет-клікери;
- проксі-сервери;
- дзвінки на платні ресурси;
- організація DoS- і DDoS-атак.

Психологічний тиск на користувача:

- реклама;
- лихі жарти і містифікації.

Окрему категорію складають програми, що збирають і надсилають паролі доступу до локальної системи і до мережних ресурсів, зокрема платних, а також до банківських систем і систем електронних платежів

До категорії «логічних бомб» належать програмні закладки, які за певних умов здійснюють деякі, як правило, руйнівні дії. Іноді виокремлюють категорію «часові міни» — фактично, це окремий випадок «логічних бомб», де умовою запуску є настання певного моменту часу. «Люки» — утиліти віддаленого адміністрування це програмні закладки цієї категорії є утилітами віддаленого адміністрування комп'ютерів у мережі. Функціонально вони подібні до систем адміністрування, що розробляють і розповсюджують відомі виробники програмних продуктів.

Програмні закладки, які несанкціоновано працюють із мережею (надсилають або отримують повідомлення чи спеціальні пакети даних), становлять доволі численну групу. Ми вже згадували раніше ті з них, що надсилають шпигунську інформацію задля здобуття даних про користувача і його комп'ютер, а також ті, що отримують команди з мережі та виконують їх. Необхідно відмітити, що в даний час проводиться активна робота по створення інших шкідливих програм, призначених для роботи з мережею, які здатні завдати значної шкоди користувачу [2,3]. Що породжує необхідність постійного моніторингу, розробки та впровадження нових методів боротьби з таким програмним забезпеченням.

Висновок:

Проведено аналіз основних мережевих загроз несанкціонованого витоку конфіденційних даних на об'єкті інформаційної діяльності.

Проаналізоване шкідливе програмне забезпечення, його функції та класифікація.

Здійснено аналіз властивостей та можливостей застосування спеціальних програмних засобів та комп'ютерних вірусів несанкціонованого доступу до інформації.

Список використаних джерел:

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К. : Консум. — 2005. — 576 с.

2. Засоби створення шкідливого програмного забезпечення [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://studfile.net/preview/5206321/page:17/.

3. Безпека інформаційно-комунікаційнихсистем. Шкідливе програмне забезпечення [Електронний ресурс] – Режим доступу до ресурсу: http://virt.ldubgd.edu.ua/pluginfile.php/39805/mod_resource/content/3/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.4.pdf.

О.О. Панасюк,
Державний університет інформаційно-комунікаційних технологій, м.Київ
В.О. Марченко, Р.В. Скоробагатько
Національний авіаційний університет, м.Київ

ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

На сучасному етапі розвитку суспільства, однією з найактуальніших проблем, яка є не тільки в Україні, а й в світі, полягає в захисту інформації на об’єктах інформаційної діяльності. Одним з аспектів вирішення вказаного питання є організація та здійснення багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

Захист інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації (ТЗІ). Несанкціоноване ознайомлення із інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками [1,5,6].

Управління доступом – ефективний метод захисту інформації, регулюючий використовування ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки (ІБ). Методи і системи захисту інформації, що спираються на управління доступом, включають наступні функції захисту інформації в ІКС [1,2]:

– ідентифікація користувачів, ресурсів і персоналу системи ІБ;

– впізнання і встановлення достовірності користувача за обліковими даними, що вводяться (на даному принципі працює більшість моделей ІБ);

– допуск до певних умов роботи згідно регламенту, наказаному кожному окремому користувачу, що визначається засобами захисту інформації і є основою інформаційної безпеки більшості типових моделей ІКС;

– протоколювання звертань користувачів до ресурсів, ІБ яких захищає ресурси від НСД і відстежує некоректну поведінку користувачів системи.

Система ідентифікації і автентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційно-комунікаційної системи.

Задачею систем ідентифікації і автентифікації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи.

Ідентифікація - це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки).

Автентифікація – це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу.

Сьогодні існує декілька технологій ідентифікації та автентифікації користувачів в інформаційно-комунікаційних системах (рис.1) [1,2]

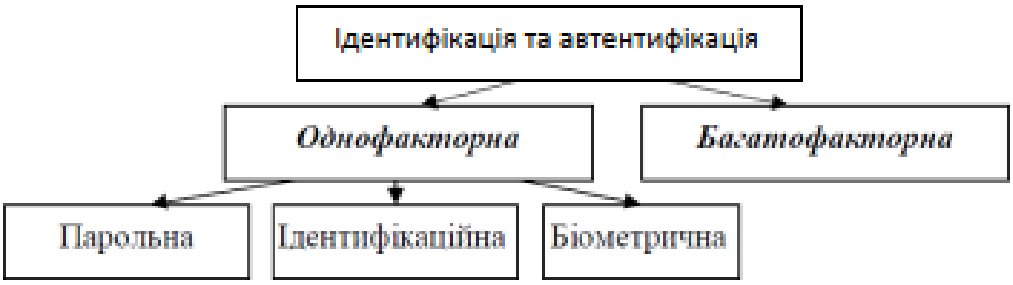

Рис.1. Система технологій ідентифікації та автентифікації

Класифікація та характеристики методів ідентифікації та автентифікації користувача

Нещодавно парольна ідентифікація та автентифікації була ледве не єдиним способом визначення особистості користувача. І в цьому немає абсолютно нічого дивного. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні [2,3].

Суть її зводиться до наступного. Кожен зареєстрований користувач якої певної системи одержує набір персональних реквізитів (звичайно використаються пари логін-пароль).

Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати ряд додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів. Загальний підхід до застосування одноразових паролів заснований на послідовному використанні хеш-функції для розрахунку чергового одноразового пароля на основі попереднього. На початку користувач одержує впорядкований список одноразових паролів, останній з яких також зберігається в системі автентифікації.

Апаратна ідентифікація та автентифікація користувачів в ІКМ.

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні.

На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (безконтактні-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера.

Біометрія – це ідентифікація користувача по унікальним, властивим тільки йому біологічним ознакам. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особистості людини [16].

Серед біометричних механізмів ідентифікації можна виділити такі [2,3]:

1) по статичних ознаках – те, що практично не міняється з часом, починаючи з народження людини (фізіологічні характеристики);

2) по динамічних ознаках – поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії.

Важко не погодитися, що біометричні технології надійніші і зручніші за ті засоби захисту, які широко застосовувалися до теперішнього часу. Але, незважаючи на активну діяльність протягом останніх років у напрямку розробки та вдосконалення методів ідентифікації користувачів з метою управління доступом до ресурсів інформаційних систем, надійність та стійкість існуючих систем недостатня для потреб сьогоднішнього дня. Головним достоїнством біометричних технологій є найвища надійність.

Основним міжнародним стандартом по криптографічним протоколам аутентифікації є стандарт Міжнародної організації по стандартизації та Міжнародної електротехнічної комісії ISO / IEC 9798 - Information technology – Security techniques - Entity authentication mechanisms, що складається з п'яти частин [1,3].

Висновки

1. Проведено огляд існуючих технологій ідентифікації та автентифікації користувача в інформаційно-комунікаційних системах об'єкту інформаційної діяльності. визначені основні поняття та функції доступу до інформації з обмеженим доступом. подана система технологій ідентифікації та автентифікації користувачів.

2. Розглянуто зміст, особливості застосування, переваги та недоліки парольної, апаратної, біометричної ідентифікації та автентифікації користувачів в інформаційно - комунікаційних системах.

Список використаних джерел:

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К. : Консум. — 2005. — 576 с.

2. Засоби створення шкідливого програмного забезпечення [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://studfile.net/preview/5206321/page:17/.

3. Безпека інформаційно-комунікаційнихсистем. Шкідливе програмне забезпечення [Електронний ресурс] – Режим доступу до ресурсу: http://virt.ldubgd.edu.ua/pluginfile.php/39805/mod_resource/content/3/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.4.pdf.

О.В. Корецький,
Державний університет інформаційно-комунікаційних технологій, м. Київ

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ІНФТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТА ДЛЯ АНАЛІЗУ НАВАНТАЖЕННЯ ТА РОЗПОДІЛУ ТРАФІКУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ П'ЯТОГО ПОКОЛІННЯ

На даному етапі розбудови телекомунікаційних мереж п'ятого покоління отримали розвиток та широко застосовуються наступні перспективні концепції побудови високошвидкісних інформаційно-комунікаційних мереж, а саме.

Мережа широкої машинної взаємодії (с англ. ММС – Massive Machine type Communications).

Покращений мобільний широкосмуговий зв'язок (з англ. eMBB – Enhanced Mobile Broadband).

Наднадійна телекомунікаційна мережа з ультрамалими затримками (з англ. URLLC – Ultra- reliable and low latency communications).

В даний час мережа URLLC є найбільш перспективною при створені і розвитку нових властивостей глобальної мережі Інтернет. Покращити її властивості та забезпечити надійний і швидкісний процес передачі та обробки даних в такій мережі дозволяє також використання мікросервісної архітектури програмного забезпечення. Поєднання можливостей мережі та можливостей мікросервісної архітектури програмного забезпечення, широке впровадження програмно-конфігурованих мереж і системи оркестрації обчислювальних структур висуває нові вимоги до оперативності прийняття рішення по забезпеченню якості обслуговування. Задоволення вище поданих вимог передбачає наявність точних та своєчасних прогнозів навантаження трафіку на окремі сервіси мережі, врахування географічного фактору та динамічність об'єктів кінцевих користувачів. Вирішити яке можна при умові залучення до такого процесу інструментів штучного інтелекту [1,2].

Завдання Штучного інтелекту при управлінні трафіком телекомунікаційної мережі п'ятого покоління.

В якості таких завдань, що будуть вирішуватися інструментами ШІ визначимо наступні:

- однозначна індентифікація трафіку;

- прогнозування трафіку;

- динамічний розподіл трафіку по елементам мікросервісного програмного забезпечення;

- прогнозування і ідентифікація можливих перевантажень в системі управління мережею.

При цьому, ідентифікація трафіку включає в себе завдання розпізнавання великої кількості типів сервісів при умові мінімізації часу затримки трафіку на етапі розпізнавання та можливість підлаштування інструментів та алгоритмів ШІ під особливості функціонування та географічне розташування елементів мережі та задіяних сервісів.

Поруч з новими технологіями забезпеченні високого рівня функціонування мереж п'ятого покоління та широкого втілення нових рішень в галузі хмарних технологій, які спрямовані на задоволення вимог сервісів до інфраструктури мережі існують не менш важливі задання модернізації логіки оброблення трафіку.

В даний час для вирішення задання покращення якості обслуговування широко застосовуються технолгії DiffServ а також інші рішення TE (Traffic Engineering). Наприклад технологія DiffServ та інші, що використовують протоко резервування ресурсів RSVP-TE. Данні технології і побудовані на їх основі рішення мають ряд недоліків, а саме. Відсутність динамічного управління в залежності від змін профіля трафіку, відсутність швидкої переконфігурації політики обслуговування підконтрольного домену мережі. До недоліків також віднесем дещо обмежений набір класифікаторів трафіку, що в умовах швидкого розвитку Інтернету речей, появи нових відмінних один від одного сервісів в мережі та існуючих відмінностях в якості обслуговування для кожному з них може мати фатальні негативні наслідки.

В загальному вигляді, неоднорідність трафіку складність розрахунку його росту, оперативні розрахунки змін його профілю не забезпечуються існуючими методами «ручного управління». Одним з рішень по мінімізації впливу даних обставин та підвищенню оперативності реагування на зміни якості обслуговування в мережі є втілення принципу абстрагування мереж зв'язку, пристроїв комутації та маршрутизації від «фізики» процесу управління. Тобто високоточна ідентифікація трафіку повинна здійснюватися без втручання в потік на рівні передачі даних, внесення змін в профіль трафіку та затримок.

Необхідний рівень абстрагування від процесів передачі трафіку може забезпечити ряд технологій. Однією з яких є технологія є концепція SDN и NFV.

Для вирішення вищеподаного задання було проаналізовано математичні методи та процедури класифікації з врахуванням особливостей вхідних даних про потоки та аналізувалися можливості системи по роботі «на взлеті». Як результат проведеного аналізу, було обрано підхід використання нейронних мереж зазначеної конфігурації, яку може забезпечити такий інструмент ШІ, як архітектор нейронних мереж.

Висновок:

Проведено аналіз основних концепції побудови високошвидкісних інформаційно-комунікаційних мереж.

Сформовано основні задання по управлінню трафіком телекомунікаційної мережі п'ятого покоління інструментами Штучного інтелекту.

Обґрунтовано застування, визначені напрямки вирішення функціональних завдані і сформовано обрис необхідного інструменту ШІ, призначено для управління трафіком телекомунікаційної мережі.

Запропоновано застосування архітектора нейронних мереж, безпосередньо призначеного для вирішення завдань високоточної ідентифікації трафіку без втручання в потік на рівні передачі даних, внесення змін в профіль трафіку та затримок.

Список використаних джерел:

1. Recommendation M.2083-0 IMT-Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. ITU-R, Geneva. – 2015.

2. Recommendation Y.3300 Framework of Software-defined networking. ITU-T, Geneva. – June 2014.

3. Technical Specification. FG-NET2030 – Focus Group on Technologies for Network 2030. Network 2030 Architecture Framework. ITU-T, Geneva. – June 2020.

О.Л. Туровський, А.М. Аронов,
Державний університет інформаційно-комунікаційних технологій, м. Київ
М.В. Шуляк,
Національний авіаційний університет , м. Київ

МОДЕЛЬ ОЦІНКИ ЕФЕКТИВНСТІ СТЕГАНОГРАФІЧНИХ МЕТОІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ЗОБРАЖЕННЯХ

Обмеження на використання криптографічних засобів у ряді країн світу та виникнення проблеми захисту прав власності на інформацію, представлену в цифровому вигляді зумовлюють популярність досліджень у сфері стеганографії. Методи стеганографії – приховування і передачі інформації через зображення дозволяють не тільки приховано передавати дані (так звана класична стеганографія), але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку, пошуку інформації в мультимедійних базах даних тощо.

Стеганографія – це наука, яка вивчає способи та методи приховання конфіденційних даних. Її основною задачею є приховання саме факту існування таємних даних при передачі, зберіганні або обробці. Задача ж вилучення інформації відсувається на другий план і вирішується у більшості випадків стандартними криптографічними методами.

Структурна схема стеганосистеми як системи передачі інформації наведена на рис. 1.[5,7].

Рис. 1. Структурна схема стеганосистеми як системи передачі інформації

Математична модель стеганосистеми.

Процес тривіального стеганографічного перетворення описується залежностями [1,8]:

$$E: C \times M \rightarrow S; \quad (2.1) \qquad (1.1)$$

$$D: S \rightarrow M, \quad (2.2) \qquad (1.2)$$

де S = {(c1, m1), (c2, m2), ..., (cn, mn), ..., (cq, mq)} = {s1, s2, ..., sq} – множина контейнерів-результатів (стеганограм).

Залежність (1.1) описує процес приховування інформації, залежність (1.2) – видобування прихованої інформації. Необхідною умовою при цьому є відсутність "перетинання" [1,8] тобто, якщо ma ≠ mb, причому ma, mb ∈ M, а (ca, ma), (cb, mb) ∈ S, то E(ca, ma) ∩ E(cb, mb) = ∅. Крім того, необхідно, щоб потужність множини |C| ≥ |M|. При цьому обидва адресати (відправник і одержувач) повинні знати алгоритм прямого (E) та оберненого (D) стеганографічного перетворення.

Отже, в загальному випадку стеганосистема – сукупність Σ = (C, M, S, E, D) контейнерів (оригіналів і результатів), повідомлень і перетворень, що їх пов'язують.

Для більшості стеганосистем множина контейнерів C обирається таким чином, щоб в результаті стеганографічного перетворення (1.1) заповнений контейнер і контейнер-оригінал були подібними, що формально може бути оцінене за допомогою функції подібності [1,7].

При умові, щодана стеганосистема C – непорожня множина, функція:

$$sim(C) \rightarrow (-\infty, 1]$$

є функцією подібності на множині C.

Якщо для будь-яких x, y ∈ C справедливо, що sim(x, y) = 1 у випадку x = y і sim(x, y) < 1 при x ≠ y.

Стеганосистема може вважатися надійною, якщо sim[c, E(c, m)] ≈ 1 для всіх m ∈ M і c ∈ C. Причому в якості контейнера c повинен обиратися такий, що раніше не використовувався.

Кількісні критерії оцінки стеганосистеми.

В якості таких показників пропонується використання:

1. Співідношення сигнал шум (SRN), що дозволяє оцінити рівень спотворень, які вносяться в контейнер під час приховання в ньому інформації;
2. Нормована середня абсолютна різниця (NAD), що показує ступінь відмінності між вихідним контейнером і контейнером з вбудованим секретним файлом$
3. Якість зображення (IF) - однf з основних оціночуих характеристик для стеганографічних методів, які працюють із зображеннями;
4. Середньоквадратична похибка (MSE) - середньоквадратичне відхилення вибіркового розподілу статистичних даних;
5. Середня абсолютна різниця (AD), що визначає середнє значення модулю різниці між пікселями порожнього і заповненого контейнеру.

Якісні критерії оцінки стеганосистеми

До найважливіших якісних характеристик стеганографічних систем, утворених з використанням різних методів, відносяться [5,6,7]:

Пропускна здатність – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру [8,9].

Стійкість – здатність вилучити приховану інформацію після загальних операцій з обробки зображень.

Невидимість – характеристика, що відповідає за неспроможність людського зору виявити стеганографічне повідомлення без використання спеціальних засобів.

Захищеність – вбудована інформація не може бути видалена цілеспрямованими атаками, заснованими на відомому алгоритмі вбудовування та вилучення (окрім секретного ключа), і знанні принаймні одного носія з прихованим повідомленням. [8,9].

Складність вбудовування і вилучення – кількість стандартних операцій, які будуть виконані для вбудовування і виявлення прихованого повідомлення.

Висновок:

Подано узагальнено структуру стеганографічної системи приховування інформації.

Запропонована математична модель стеганосистеми, що забезпечує умову надійності приховування інформації.

Визначено якісні та кількісні критерії оцінки ефективності стеганосистеми.

Список використаних джерел:

1. Конахович г.ф. комп’ютерна стеганографія. теорія і практика / Г.Ф. конахович, А. Ю. Пузиренко. - Київ: МК-ПРЕСС, 2006. – 288с.

2. Кузнецов О. О. Стеганографія: навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. - Х.: вид. ХНЕУ, 2011. - 232с.

П.М. Поночовний,
Державний університет інформаційно-комунікаційних технологій, м. Київ

"КІБЕРЗАГРОЗИ В ЕПОХУ ЦИФРОВІЗАЦІЇ: МОДЕЛЮВАННЯ ТА ЗАХИСТ ВІД DDOS-АТАК"

Фраза "якщо тебе немає в Інтернеті, тебе взагалі немає" стала дуже популярною в суспільстві і в діловому світі. Комп'ютерні мережі дозволяють не тільки поширювати інформацію, але також використовувати і надавати різні послуги для інших комп'ютерних систем. Така розподілена система або служба забезпечує швидкий і простий спосіб доступу до інформації та віддаленого управління процесами або об'єктами. Таким чином, бізнес-маркетинг буде орієнтований на користувачів Інтернету та їх послуги.

Ви також можете помітити іншу тенденцію. Основна мета хакерів - не тільки отримати визнання, але і кібератаки стануть способом заробити гроші. Одним із способів монетизації кібератаки є DDoS-атака. Тим часом, деякі сервіси декомунізовані і більше не будуть доступні їх законним користувачам. Обіцяючи скасувати атаку (іноді навіть не ініціюючи її взагалі), хакер просить у нього певну суму грошей. Жертва або конкурент певного інтернет-сервісу і погоджується заплатити за усунення конкурентів у певний час. Є багато способів заробити гроші на кібератаках. Але доступність може бути однією з найдорожчих функцій безпеки.

Ще одна проблема доступності полягає в тому, що ви можете легко виконувати DDoS-атаки. Це пов'язано з різними DDoS-атаками, наявністю ботнетів, функціями запозичення і т.д. через популярність природних DDoS-атак і інструментів для їх реалізації такі кібератаки також можуть виконуватися любителями. Таким чином, системні адміністратори повинні бути ретельно навчені для забезпечення різних рівнів доступності системи.

Однак немає єдиного способу продемонструвати стійкість системи до DDoS-атак. Системним адміністраторам необхідно покладатися на досвід і знання, щоб визначити ефективність різних заходів і масштаби DDoS-атак. Якщо клієнт хоче перевірити наявність послуги, клієнт повинен покладатися на думку постачальника послуг, яка може бути суб'єктивною та ненадійною.

Ця модель дозволяє вимірювати успішність DDoS-атак на мережеві системи і оцінювати ефективність можливих потоків, втрат і відповідей.

Існує багато способів заборонити законним користувачам доступ до послуги. Боротьба з DOS-атаками є дуже складною та ресурсоємною, оскільки DoS-атаки можуть використовувати вразливості в протоколах зв'язку та архітектурі системи. Іноді немає готових відповідних заходів, які можна було б використовувати. Тому дуже важливо знати про потенційну загрозу.

Не існує унікальної таксономії DOS. Огляди існуючих таксономій DoS і DDoS показують, що більшість з них не дозволяють повністю описати DoS-атаки або функції, відомі тільки зловмиснику. Як результат, жодна з існуючих таксономій не може бути використана недбало і не дозволяє повністю класифікувати вхідні DoS-атаки з точки зору жертви.

Дуже важко точно змоделювати поведінку комп'ютерної мережі або DoS-атаки. Найбільша проблема в цій області-представлення інтернет-трафіку. Через дуже складну структуру комп'ютерної мережі, що розробляється, та широкий спектр протоколів зв'язку дуже важко ідентифікувати та моделювати реальні ситуації.

При моделюванні DoS-атак найпоширенішими є моделі на основі витрат, ігрові моделі, теорія перезапису та математичні моделі. Як правило, перші 3 типи є підходами до реалізації моделі релейного програмування, але модель mat може бути реалізована як в програмуванні, так і в ряді рішень. Цей тип моделі DoS-атак дозволяє швидше отримувати результати моделювання, дозволяючи виявляти DoS-атаки в режимі реального часу і налаштовувати параметри реакції.

Детермінованих рішень недостатньо для представлення фактичного трафіку комп'ютерної мережі, а моделювання та моделювання DOS - і DDoS-атак повинно включати певний рівень випадковості трафіку.

Список використаних джерел:

1. Mirkovic, J., & Reiher, P. (2004). "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms." ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

2. DDoS Attack Mitigation: A Practical Approach. (2018). IEEE Communications Magazine, 56(4), 40-46.

3. Zargar, S., Joshi, J., & Tipper, D. (2014). "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks." IEEE Communications Surveys & Tutorials, 16(2), 761-778.

О.В. Іванцов,
Державний університет інформаційно-комунікаційних технологій, м.Київ
О.В. Таров, Н.О. Левчук
Національний авіаційний університет , м.Київ

АНАЛІЗ ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ТЕХНІЧНИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Однією важливих та характерною проблемою сьогодення стало питання забезпечення безпеки функціонування державних установ, підприємств, загальнонаціональних систем та мереж забезпечення життєдіяльності населення від несанкціонованого доступу до інформації з обмеженим доступом. З усього різноманіття можливих вторгнень та взломів інформаційних систем та мереж передачі інформації особливу увагу викликає група каналів передачі інформації, яка кваліфікується як технічні канали передачі інформації. В свою чергу, поряд з загально відомими та широко доступними типами даних, яку циркулюють по таким каналам, в них можу передаватися інформація з обмеженим доступом. Доступ до якої є особливо чутливим з точки зору корпоративної та державної інформаційної безпеки.

Класифікація та розподіл інформації з обмеженим доступом на об'єкті інформаційної діяльності

Інформації з обмеженим доступом - інформація, що становить державну або іншу передбачену законом таємницю, а також конфіденційна інформація, що є власністю держави або вимога щодо захисту якої встановлена законом.

Таємна інформація - вид інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані, у порядку встановленому Законом, державною таємницею і підлягають охороні державою. Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України "Про державну таємницю" [2].

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб поширюються за їх бажанням відповідно до передбачених ними умов. Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств,

установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ - надано статус конфіденційної [2].

У відповідності до Закону "Про захист інформації в інформаційно-телекомунікаційних системах" захисту в системі підлягає:

- відкрита інформація, яка є власністю держави;
- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація);
- інформація, що становить державну або іншу передбачену законом таємницю (таємна інформація) [2].

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження [2].

Аналіз загроз несанкціонованого доступу до конфіденційної інформації на об'єкті інформаційної діяльності

Обробка ІзОД на об'єктах інформаційної діяльності дозволяє забезпечити безпеку інформації, змістом якої є збереженні наступних критеріїв інформаційної безпеки**:**

- цілісність - властивість інформації бути захищеною від несанкціонованого знищення, модифікації.
- конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення.
- доступність - властивість інформації бути захищеною від несанкціонованого блокування [2].

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення повідомлення, технічні канали витоку можна розділити на:

- радіоканал;
- електричний;
- акустичний;
- оптичний;
- матеріально-речовий [3].

Структура технічного каналу витоку інформації подана на Рис.1

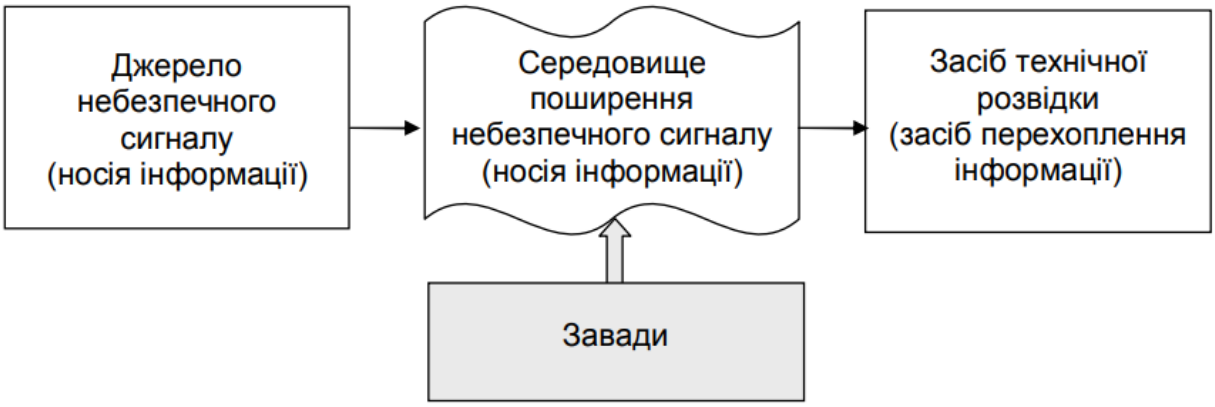

Рис. 1. Структура технічного каналу витоку інформації

Класифікація технічних каналів витоку інформації на об'єкті інформаційної діяльності

Для встановлення вимог та організації захисту інформації від витоку технічними каналами здійснена їх класифікація за певними ознаками. Зокрема відокремлені типи ТКВІ за такими ознаками:

- за видом інформаційної діяльності на ОІД,
- за принципом (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації),
- за середовищем поширення небезпечного сигналу,
- за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

Висновок:

1. В роботі розглянуті питання аналізу загроз несанкціонованого доступу до технічних каналів передачі інформації з обмеженим доступом

2. Подано розподіл інформації на об'єкті інформаційної діяльності, її класифікація та класифікація технічних каналів, по яким вона може передаватися.

Список використаних джерел:

1. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.

2. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г Защита информации в телекоммуникационных системах.. — К.: МК-Пресс, 2005. — 288 с, ил.

3. Домарєв В.В. Організація захисту інформації на об'єктах державної та підприємницької діяльності /Домарєв В.В., Скворцов С.О./ Навч. Посібник. – К.: Вид-во Європейського університету, 2006. – 102с.

Є.Р. Сердюк,
Державний університет інформаційно-комунікаційних технологій, м.Київ
Р. С. Марчук, О. В. Рожков
Національний авіаційний університет , м.Київ

НАПРЯМКИ УДОСКОНАЛЕННЯ ЄДИНОЇ МОДЕЛІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ ТЕХНІЧНИМИ КАНАЛАМИ

Характерною та важливою проблемою сьогодення стало питання забезпечення безпеки функціонування державних установ, підприємств, загальнонаціональних систем та мереж забезпечення життєдіяльності населення які кваліфікуються як об'єкти інформаційної діяльності. Тобто об'єкти, неналежне функціонування чи вихід зі строю яких можуть значною мірою вплинути на якість управління життєдіяльності населення цілих регіонів. Виходячи з важливих змін в розвитку науки та техніки, ускладнення процесів економічного життя та суспільних відноси, розвитку різноманітних технологій, на основі яких функціонують вказані об'єкти можна зробити висновок про те, що одним з факторів, який забезпечує якість їх функціонування є різноманітна інформація [1].

Забезпечення ефективного функціонування системи захисту інформації від витоку технічними каналами на об'єкті інформаційної діяльності є актуальним заданням, вирішенню якого присвячена дана робота.

Вектори захисту інформації від витоку технічними каналами

Створення комплексної системи захисту інформації на об'єкті інформаційної діяльності, що спрямована на запобігання витоку інформації технічними каналами має базуватися на трьох векторах захисту інформації [1,2,3]:

1. Технічний захист інформації
2. Програмний захист інформації
3. Організаційно-технічний захист інформації

Вимоги до захисту технічних каналів витоку інформації

Узагальнимо перелік можливих технічних каналів витоку інформації на об'єкті інформаційної діяльності включає [2,3]:

1. канал побічних електромагнітних випромінювань (ПЕМВ) ОТЗС;
2. каналу побічних електромагнітних випромінювань ДТЗС;
3. канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС;
4. канал побічних електромагнітних наведень на комунікації ДТЗС;
5. канал ВЧ нав'язування;
6. оптичний канал витоку інформації;
7. встановлення закладних пристроїв.

Захист вказаних технічних каналів витоку інформації має забезпечуватися наступними вимогами [1,3]:

- *канал побічних електромагнітних випромінювань ОТЗС шляхом* екранування ОТЗС або локального екранування електронних елементів.
- *канал побічних електромагнітних випромінювань ДТЗС* шляхом визначення R1 зони випромінювання та з подальшими рекомендаціями щодо розміщення ноутбука за межами цієї зони.
- *канал побічних електромагнітних наведень на лінії електроживлення (заземлення) ОТЗС* шляхом використання лінійного зашумлення ліній електроживлення ОТЗС.
- *канал побічних електромагнітних наведень на комунікації ДТЗС* вирішується електроживленням ДТЗС від автономних електричних джерел: електростанцій, акумуляторів, використання в лінії електроживлення ДТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів.

В цілому модельзапобігання витоку інформації, що обробляється в ОТЗС, та унеможливлення створення ТКВІ з врахуванням розглянутих ефектів подано в вигляді окремого комплексу захисту, який включає [2,3]:

- створення КЗ не меншої за найбільшу Зону 2, яку розраховують з врахуванням усіх властивих об'єкту ЕОТ технічних каналів витоку інформаці;
- організація режиму доступу до КЗ та ОІД;
- екранування ОТЗС;
- просторове електромагнітне зашумлення на об'єкті ЕОТ;
- індикація відхилення параметрів підсилювачів та блокування роботи ОТЗС;
- розміщення ДТЗС не ближче Зони 1 ОТЗС, а ОТЗС - на ближче своєї Зони 1 до можливих сторонніх провідників;
- використання в лініях ДТЗС технічних засобів захисту, що затримують сигнали низького рівня;
- використання в лініях ДТЗС та сторонніх провідниках лінійного зашумлення;
- живлення ОТЗС від автономних електричних джерел: електростанцій, акумуляторів;
- використання в ланцюгу живлення ОТЗС технічних засобів захисту, що затримують сигнали низького рівня, мережевих фільтрів;
- використання в ланцюгу живлення ОТЗС лінійного зашумлення;
- автономне заземлення ОТЗС;
- забезпечення вимог щодо монтажу на опору заземлення ОТЗС;
- розташовування заземлювача з шинами заземлення в межах контрольованої зони на

максимальній відстані від границі КЗ та сторонніх провідників;

- зашумлення ліній заземлення ОТЗС та ДТЗС.

Захист інформації на основі КСЗІ має враховувати та гарантувати забезпечення цілісності, конфіденційності, доступності інформації та давати можливість спостережності за діями користувача та функціонуванням системи [2,3].

Висновок:

В роботі подано результати дослідження напрямків удосконалення єдиної моделі комплексної системи захисту від витоку інформації технічними каналами.

Сформовані вимоги до захисту технічних каналів від несанкціонованого витоку інформації.

Визначені вектори захисту інформації від витоку технічними каналами та подані способи захисту..

Список використаних джерел:

4. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах / Ю.В. Землянко, О.А. Замула, О.О. Ткач, Н.І. Литвинова, Я.А. Пересічанська.]., 2010.

5. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.]–Вінниця : ВНТУ, 2017.– 120 с.

6. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення – Київ, 2007. – 6 с.

Ю.В. Жеребок,
Державний університет інформаційно-комунікаційних технологій, м. Київ
Б.І. Цимбал, В.С. Бойко,
Національний авіаційний університет, м. Київ

ОЦІНКА ІНФОРМАЦІЙНИХ РИЗИКІВ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

У міжнародній банківській практиці процес управління ризиками є центральною сферою фінансового менеджменту. Велика увага приділяється вивченню зон ризику та основних видів ризиків, пошуку ефективних методів їх оцінки, контролю та моніторингу, створенню адекватних систем управління.

Банківські ризики – це ймовірність того, що очікувані або несподівані події можуть негативно вплинути на капітал та/або дохід банку.

З точки зору банку, ризик – це потенційна втрата доходу або зниження ринкової вартості капіталу банку через негативні зовнішні чи внутрішні фактори. Такі збитки можуть бути прямими (втрата доходу або капіталу) або непрямими (обмежує можливості банку для досягнення бізнес-цілей) [1,2].

Ризик вимірюється ймовірністю того, що очікувана подія не відбудеться і що це призведе до небажаних наслідків. У банківській справі, як і в інших видах бізнесу, ризик пов’язаний переважно з фінансовими втратами, які виникають при реалізації певних ризиків.

У зв’язку з тим, що банк веде як активний, так і пасивний бізнес, виникають додаткові ризики, такі як ризик незбалансованої ліквідності, ризик розриву часу в зборі та розміщенні коштів, валютний ризик. Це спонукає до пошуку особливих підходів для обмеження його наслідків, які називаються «управлінням банківськими активами та пасивами».

У зв’язку з тим, що банк веде як активний, так і пасивний бізнес, виникають додаткові ризики, такі як ризик незбалансованої ліквідності, ризик розриву часу в зборі та розміщенні коштів, валютний ризик. Це спонукає до пошуку особливих підходів для обмеження його наслідків, які називаються «управлінням банківськими активами та пасивами».

Методи контролю та мінімізації банківських ризиків

У світовій фінансовій практиці використовуються наступні методи контролю та мінімізації ризиків, конкретні комбінації яких залежать від особливостей конкретного сегмента фінансового ринку:

– фондові біржі і, зокрема, органи зберігання та компенсації пред'являють мінімальні вимоги до професійного складу учасників, їх матеріального становища та навіть репутації. Чим надійніший кожен з учасників системи, звісно, тим менший ризик для всіх інших учасників, але в той же час не всі вони зможуть задовольнити ці вимоги;

- біржі та клірингові організації можуть встановлювати різні ліміти для транзакцій учасників. Чим суворіші ліміти, тим нижча взаємна заборгованість учасників і менші ризики. Проте занадто жорсткі обмеження призводять до зниження обсягів торгів та стагнації ринку. Тому потрібен компроміс між надійністю та розміром ринку;

- вкладники та клірингові організації – впроваджують методи розподілу ризиків між усіма учасниками системи, зокрема використання «клірингових» та «інноваційних» методів;

- учасники переговорів – можуть створити спеціальний резервний фонд, який компенсує збитки від невиконання або несвоєчасного виконання угод окремими учасниками, яким зазвичай керують депозитарій та клірингова організація;

- за допомогою зберігача та розрахункової палати учасники ринку – можуть створити систему розподілу збитків, якщо вони виникають внаслідок невиконання окремими учасниками своїх зобов'язань за угодами;

- розрахункова палата депозитарію або учасники переговорів через клірингову палату використовують механізм акредитації боржників, які мають тимчасові труднощі з оплатою.

Кредиторами за свій рахунок або за рахунок учасників можуть бути як самі учасники, так і клірингова організація. Найбільш складні та небезпечні за своїми фінансовими наслідками ризики страхуються спеціальними страховими компаніями шляхом укладання відповідного договору.

Фінансові ризики включають валютний, кредитний, інвестиційний, ринковий ризик, ризик ліквідності, ризик процентної ставки, інфляцію, базисний ризик тощо.

Виходячи з поняття кредитного ризику комерційного банку, слід розрізняти такі терміни:

-Кредитний ризик позичальника: ймовірність того, що позичальник (боржник) не зможе виконати свої зобов'язання перед банком щодо сплати боргу за умовами договору (угоди);

- Кредитний ризик при отриманні кредитів: ймовірність того, що банк не використає гарантію своєчасно і в повному обсязі для покриття можливих збитків;

- Кредитний ризик кредитного договору: ймовірність того, що позичальник (боржник) не виконає свої зобов'язання перед банком щодо погашення заборгованості за договорами (контрактами) і банк не використає гарантію по кредиту вчасно та в повному обсязі, щоб покрити будь-які збитки. Визначення кредитного ризику можна розглядати з різних сторін. По-перше, його можна визначити як ймовірність того, що банк зазнає збитків у разі невиконання позичальником певного кредитного договору. По-друге, кредитний ризик можна охарактеризувати як максимальну суму збитків і незароблених доходів, які є результатом непогашення позичальником повністю або частини основного боргу та/або відсотків.

Регіональний ризик – це ризик, пов'язаний з діяльністю в певному регіоні в конкретній країні. Ризик, пов'язаний з веденням бізнесу в країні, іноді називають ризиком країни.

Регіональний ризик визначається особливостями даної адміністративно-географічної території, яка характеризується умовами, що відрізняються від середніх умов по всій країні. Відмінності можуть бути пов'язані з кліматичними, національними, політичними, правовими та іншими специфічними для регіону факторами, які впливають на становище позичальника і тому стають частиною кредитного ризику. Кредитний ризик притаманний не лише прямим кредитним операціям, а й супроводжує оформлення лізингу, факторингу, гарантій та процес створення портфеля цінних паперів.

Ризик дисбалансу ліквідності пов'язаний з імовірністю того, що банк не зможе вчасно виконати свої зобов'язання або втратить частину доходу від надмірно високоліквідних активів. Ризик незбалансованої ліквідності можна розглядати як два різних ризики: ризик недостатньої ліквідності та ризик надлишкової ліквідності. Виміряти ризик ліквідності дуже складно, оскільки на цей показник впливає багато факторів, більшість з яких банк не може контролювати самостійно. На практиці для контролю ліквідності використовуються спеціальні індикатори, більшість з яких регулюються центральними банками країн.

Висновок:

В роботі подано результати оцінки інформаційних ризиків банківської діяльності.

Сформовані методи контролю та мінімізації банківських ризиків.

Проведено огляд фінансових ризиків.

Список використаних джерел:

1. https://niss.gov.ua/publikacii/monografii/bankivska-bezpeka-derzhavi-v-umovakh-rozvitku-informaciynoi-ekonomiki

2. https://ru.osvita.ua/vnz/reports/bank/19767/

3. https://financial.lnu.edu.ua/wp-content/uploads/2020/11/Blashchuk_Petyk_13_end.pdf

В.В. Токарев, Є.В. Ковальова В.С. Вишинський,
Національний авіаційний університет, м. Київ

ЗАХИСТ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ КОМ'ЮТЕРНІЙ МЕРЕЖІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Питання захисту інформації від несанкціонованого доступу набуло актуальності відколи людство засвоїло писемності. На сучасному етапі, в епоху комп'ютеризації, контроль та управління різними об'єктами, благополуччя та навіть життя багатьох, залежить від забезпечення інформаційної безпеки, комп'ютерних систем обробки інформації.

Система захисту інформації — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в інформаційних системах.

До складу вказаної системи входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо [1].

Способи захисту інформації в ЛКМ включають всі наступні елементи [1].

1. Перешкода – фізична перешкода що захищає носії інформації від зловмисників.

2. Управління доступом – система захист інформації при якому використовуються всі ресурси підприємства. Включає такі функції захисту:

- ідентифікація інформації, персоналу з допомогою паролевих, карткових, біометричних, програмних засобів і. тп.;
- перевірка системних журналів реєстру персоналу відносно робочого графіку, повноважень, доступів до інформації;
- створення і організація роботи в межах регламенту ;
- відмовостійкість систем (затримка робіт, відмова, відключення, сигналізація) під час спроб несанкціонованих дій.

3. Маскування – захист даних в ЛКМ шляхом використання криптографічних перетвіорень перетворення. При передачі інформації незахищеними лініями зв'язку, криптографічний захист є найголовнішим методом їх захисту.

4. Регламентація – розроблення документації в які прописані посадові інструкції

персоналу та правила робити з конфеденційною інформацією.

5. Примус – користувачі та персонал ЛКМ змушені дотримуватися правил обробки та використання інформації, що захищається під загрозою матеріальної, адміністративної чи кримінальної відповідальності.

Розглянуті засоби захисту інформації реалізуються застосуванням різних засобів захисту, причому, розрізняють технічні, програмні, організаційні, законодавчі і морально-етичні засоби[1].

Організаційними засобами захисту називаються організаційно- правові заходи які регулюють процес створення та експлуатації ЛКМ. Організаційні заходи охоплюють усі структурні елементи ЛКМ на всіх етапах: будівництво приміщень, проектування системи, монтаж та налагодження обладнання, випробування та перевірки, експлуатація.

До законодавчих засобів захисту відносяться законодавчі акти країни, якими регламентуються правила використання та опрацювання інформації обмеженого доступу та встановлюються заходи відповідальності за порушення цих правил.

До морально-етичних відносять правила які формуються традиційно або складаються в міру поширення обчислювальних засобів у цій країні чи суспільстві. Ці норми здебільшого є обов'язковими, як законодавчі заходи, проте недотримання їх веде зазвичай до втрати авторитету, престижу людини чи групи осіб [1].

Заходи захисту інформації в ЛКМ

Захист інформації в ЛКМ це - організація методів і засобів що знижують можливість появи каналів витоку інформації, її спотворення при зберігані і оброрбці на ПК [2].

1. Організаційні заходи захисту – заходи загального характеру, утрудняють доступом до цінної інформації стороннім особам, незалежно від особливостей способу обробки інформації та каналів витоку інформації [2]. Організаційні заходи передбачають:

– Обмеження доступу до приміщень, де відбувається обробка конфіденційної інформації.

– Допуск до вирішення завдань на ПК із обробки секретної, конфіденційної інформації перевірених посадових осіб, визначення порядку проведення робіт на ПК. Зберігання носіїв інформації у ретельно закритих міцних шафах[2,3].

– Призначення однієї або кількох ПК для обробки цінної інформації та подальша робота тільки на цих ПК.

– Встановлення дисплея, клавіатури та принтера таким чином, щоб унеможливити перегляд сторонніми особами змісту інформації, що обробляється.

– Постійне спостереження за роботою принтера та інших пристроїв виведення на матеріальний носій цінної інформації.

– Знищення барвників або інших матеріалів, що містять фрагменти цінної інформації.

– Заборона ведення переговорів щодо безпосереднього змісту конфіденційної інформації особам, які зайняті її обробкою.

2. Організаційно-технічні заходи захисту – заходи, пов'язані зі специфікою каналів витоку та методу обробки інформації, але не потребують реалізації нестандартних прийомів і/або устаткування[2,3]. Організаційно-технічні заходи передбачають:

– Обмеження доступу до корпусу ПК шляхом встановлення механічних запірних пристроїв.

– Знищення всієї інформації на вінчестері ПК під час її відправлення в ремонт із використанням засобів низько рівневого форматування.

– Організацію живлення ПК від окремого джерела живлення або загальної (міської) електромережі через стабілізатор напруги (мережевий фільтр).

– Використання для відображення інформації рідкокристалічних або плазмових дисплеїв, а для друку – струменевих чи лазерних принтерів.

Висновок:

Проведено аналіз системи захисту інформації об’єкту інформаційної діяльності.

Проаналізовані, структуровані та кваліфіковані способи, засоби і заходи захисту інформації

Список використаних джерел:

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К. : Консум. — 2005. — 576 с.
2. Засоби створення шкідливого програмного забезпечення [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://studfile.net/preview/5206321/page:17/.
3. Безпека інформаційно-комунікаційних систем. Шкідливе програмне забезпечення [Електронний ресурс] – Режим доступу до ресурсу: http://virt.ldubgd.edu.ua/pluginfile.php/39805/mod_resource/content/3/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.4.pdf.

Д.О. Ніщеменко
Державний університет інформаційно-комунікаційних технологій, м. Київ

БЕЗПЕКА ТА ЗАХИСТ ОБМІНУ ДАНИМИ ЗА ДОПОМОГОЮ ПРОТОКОЛУ MQTT ДЛЯ КЕРУВАННЯ СИСТЕМАМИ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (IoT) — це концепція, яка описує мережу взаємопов’язаних фізичних пристроїв із вбудованими датчиками, програмним забезпеченням та іншими технологіями для підключення та обміну даними з іншими пристроями та системами через Інтернет [1]. Завдяки обміну даними та Інтернет-зв’язку ці пристрої можуть збирати інформацію, аналізувати її та реагувати на неї в режимі реального часу.

Розробники IoT повинні впроваджувати надійні заходи безпеки. Це передбачає шифрування даних як під час передачі, так і в стані спокою, впровадження надійного контролю доступу, регулярне оновлення програми пристроїв для виправлення вразливостей і забезпечення безпечних протоколів зв’язку.

Іншим важливим питанням, яке потребує уваги, є сумісність. Зі стрімким розширенням IoT на ринок виходить дедалі більше пристроїв від різних виробників, використовують різні протоколи зв’язку, формати даних і стандарти, що може призвести до фрагментації та проблем несумісності. Для реалізації весь потенціал IoT, вкрай необхідно встановити загальні стандарти та протоколи, які забезпечують безперебійний зв’язок і взаємодію між пристроями, незалежно від їх походження.

MQTT (Message Queuing Telemetry Transport) – це спрощений мережевий асинхронний протокол, побудований на основі стеку TCP/IP, використовується для обміну повідомленнями між пристроями за принципом видавець-підписник [2]. Пристрої в системі підключаються до брокера (сервера), щойно певний пристрій в системі публікує дані в тему, брокер надсилає ці дані всім пристроям, що на неї підписані.

Зараз протокол є відкритим стандартом і підтримується популярними мовами програмування за допомогою кількох реалізацій з відкритим вихідним кодом.

Основні сфери використання MQTT — це системи зі слабким сигналом зв’язку, де вимагається економія енергії та мінімізація затримок.

Протокол MQTT є стандартом для обміну даними між IoT-пристроями в умовах обмежених ресурсів. Однак захист даних в MQTT має певні обмеження, що робить його вразливим до атак. Однією з основних загроз є відсутність вбудованого шифрування, що дозволяє зловмисникам перехоплювати дані під час передачі. До того ж, як показали дослідження італійських дослідників у 2020 році, безпека MQTT не є ідеальною. Використовуючи повільні DoS-атаки, вони продемонстрували, що протокол вразливий до затримок у процесі передачі, що може негативно вплинути на продуктивність системи [4].

Для підвищення безпеки MQTT рекомендується використовувати захищений варіант протоколу — MQTTS. Це вдосконалена версія, яка інтегрує Transport Layer Security (TLS) для шифрування з’єднань. TLS забезпечує аутентифікацію, конфіденційність і цілісність даних, створюючи захищений канал між видавцем, підписником і брокером [5].

Шифрування через TLS забезпечує конфіденційність даних, захищаючи інформацію під час передачі між клієнтом і сервером. MQTTS дозволяє автентифікувати не тільки клієнтів, але й сам брокер, що додає додатковий рівень безпеки та мінімізує ризики фальшивих серверів. Механізми TLS допомагають гарантувати, що передані дані не були змінені під час їхнього транспортування.

Попри переваги MQTTS, для забезпечення повноцінного захисту IoT-систем рекомендується застосовувати комплексний підхід, що включає: обмеження прав доступу до тем, використання виявлення аномалій для протидії DoS-атакам, а також регулярний моніторинг і аудит безпеки. Для управління доступом потрібні додаткові засоби, як-от сертифікати або ключі API. Якщо налаштування виконано недостатньо чітко, це може створювати вразливості для мережі та призводити до можливих атак.

Перехід до MQTTS може бути розділений на кілька ключових етапів.

Першим кроком є отримання SSL/TLS сертифікатів від довіреної сертифікаційної установи (CA). Брокер повинен мати сертифікат, який підтверджує його ідентичність та повинен бути налаштований для використання TLS, що включає в себе оновлення конфігураційного файлу, щоб вказати використання захищеного порту, і налаштування шляхів до сертифікатів.

Клієнти повинні бути налаштовані на підключення до брокера через захищений порт. Це може вимагати вказання сертифікату CA, а також клієнтського сертифікату та приватного ключа для аутентифікації. Важливо налаштувати обробку помилок у випадку, якщо підключення не вдається, наприклад, клієнти повинні мати можливість повторно підключатися або сповіщати користувачів про проблеми з безпекою.

Після налаштування важливо протестувати всі з'єднання для перевірки їхньої безпеки та надійності. Це включає в себе перевірку, чи відбувається успішне з'єднання до брокера через MQTTS. Після впровадження необхідно організувати моніторинг для виявлення потенційних загроз безпеці, що включає в себе перевірку журналів доступу, а також активне спостереження за незвичними поведінковими патернами.

Хоча перехід до MQTTS надає численні переваги, він також має свої виклики. Налаштування TLS може бути технічно складним, особливо для великих систем. Неправильна конфігурація може призвести до відмови у з'єднанні або зниження продуктивності. Витрати на отримання сертифікатів, навчання персоналу та зміну архітектури системи можуть бути значними. Не всі MQTT-клієнти можуть підтримувати MQTTS, що може вимагати оновлення програмного забезпечення або зміни в архітектурі системи. Однак, впровадження описаних заходів безпеки є виправданим, адже забезпечить безпеку обміну даних в системі.

Список використаних джерел:

1. Internet of Things (IoT): A vision, architectural elements, and future directions / J. Gubbi та ін. *Future Generation Computer Systems*. 2013. Т. 29, № 7. С. 1645–1660. URL: https://doi.org/10.1016/j.future.2013.01.010 (дата звернення: 02.11.2024).

2. MQTT Version 5.0. *OASIS Standard*. URL: http://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html (дата звернення: 02.11.2024).

3. MQTT Version 3.1.1 becomes an OASIS Standard - OASIS Open. OASIS Open. – Режим доступу до ресурсу: https://www.oasis-open.org/2014/10/30/mqtt-version-3-1-1-becomes-an-oasis-standard/ (дата звернення: 30.10.2024).

4. Vaccari I., Aiello M., Cambiaso E. SlowITe, a Novel Denial of Service Attack Affecting MQTT. *Sensors*. 2020. Т. 20, № 10. С. 2932. URL: https://doi.org/10.3390/s20102932 (дата звернення: 02.11.2024).

5. Securing MQTT Ecosystem: Exploring Vulnerabilities, Mitigations, and Future Trajectories / S. u. A. Laghari та ін. *IEEE Access*. 2024. С. 1. URL: https://doi.org/10.1109/access.2024.3412030 (дата звернення: 02.11.2024).

Д.А. Пустолякова, Н.В. Пустовіт, І.О. Сирота
Національний авіаційний університет, м. Київ

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Інтелектуальні інформаційні технології (ІІТ) (Intellectual information technology, IIT) – це інформаційні технології, які допомагають людині прискорити аналіз політичної, економічної, соціальної і технічної ситуації, а також синтез управлінських рішень.

Використання ІІТ в реальній практиці має на увазі врахування специфіки проблемної області, яка може характеризуватися наступним набором ознак:

- якість і оперативність прийняття рішень;
- нечіткість цілей і інституціальних кордонів;
- множинність суб'єктів, що беруть участь у вирішенні проблеми;
- хаотичність, флюктурованість і квантованість поведінки середовища;
- множинність взаємовпливаючих один на одного чинників;
- слабка формалізованість, унікальність ситуацій;
- латентність, прихованість, неявність інформації;
- девіантность реалізації планів, значимість малих дій;
- парадоксальність логіки рішень та ін.

ІІТ формуються при створенні інформаційних систем та інформаційних технологій для підвищення ефективності управління знаннями, прийняття рішень в умовах, пов'язаних з виникненням проблемних ситуацій.

Інтелектуальна система (ІС, intelligent system) - це технічна або програмна система, здатна вирішувати завдання, що традиційно вважаються творчими, що належать конкретній предметній області, знання про яку зберігаються в пам'яті такої системи.

З усім процесом розробки інтелектуальних інформаційних систем в цілому і ЕС зокрема тісно пов'язана Інженерія знань. Це методологія ЕС, яка охоплює методи видобутку, аналізу і вираження в правилах знань експертів для формування бази правил.

Інтелектуальні інформаційні системи (ІІС) – це комп'ютерна система, що складається з 5 основних взаємодіючих компонентів: мовної підсистеми (механізм забезпечення зв'язку між користувачем і іншими компонентами ІСПР), інформаційної підсистеми (сховище даних і засобів їх обробки), підсистеми управління знаннями (сховище знань про проблемну область, таких як процедури, евристики і правила, і засоби обробки знань), підсистеми управління моделями та підсистеми обробки і вирішення завдань (сполучна ланка між іншими підсистемами).

Класифікація завдань, що вирішуються ІІС:

- *Інтерпретація даних*. Це одне з традиційних завдань для експертних систем. Під інтерпретацією розуміється процес визначення сенсу даних, результати якого повинні бути узгодженими і коректними. Зазвичай передбачається багатоваріантний аналіз даних.
- *Діагностика*. Під діагностикою розуміється процес співвідношення об'єкту з деяким класом об'єктів і/або виявлення несправності в деякій системі. Несправність – це відхилення від норми. Таке трактування дозволяє з єдиних теоретичних позицій розглядати і несправність обладнання в технічних системах, і захворювання живих організмів, і всілякі природні аномалії. Важливою специфікою тут є необхідність розуміння функціональної структури («анатомії») діагностичної системи.
- *Моніторинг*. Основне завдання моніторингу - безперервна інтерпретація даних в реальному масштабі часу і сигналізація про вихід тих або інших параметрів за допустимі межі. Головні проблеми – «пропуск» тривожної ситуації і інверсне завдання «помилкового» спрацьовування. Складність цих проблем полягає в розмитості симптомів тривожних ситуацій і необхідність обліку тимчасового контексту.

- *Проектування*. Проектування полягає в підготовці специфікацій на створення «об'єктів» із заздалегідь визначеними властивостями. Під специфікацією розуміється весь набір необхідних документів-креслень, пояснювальної записки і т.д. Основні проблеми тут – отримання чіткого структурного опису знань про об'єкт і проблеми «сліду». Для організації ефективного проектування і в ще більшому ступені перепроектування необхідно формувати не лише самі проектні рішення, але і мотиви їх прийняття. Таким чином, в завданнях проектування тісно зв'язуються два основні процеси, які виконуються в рамках відповідної ЕС: процес виведення рішення і процес пояснення.
- *Прогнозування*. Прогнозування дозволяє передбачати наслідки деяких подій або явищ на підставі аналізу наявних даних. Прогнозуючі системи логічно виводять вірогідні наслідки з заданих ситуацій. У прогнозуючій системі зазвичай використовується параметрична динамічна модель, в якій значення параметрів «підганяються» під задану ситуацію. Виведені з цієї моделі слідства складають основу для прогнозів з ймовірними оцінками.
- *Планування*. Під плануванням розуміється знаходження планів дій, що відносяться до об'єктів, здатним виконувати деякі функції. У таких ЕС використовуються моделі поведінки реальних об'єктів з тим, щоб логічно вивести наслідки планованої діяльності.
- *Навчання*. Під навчанням розуміється використання комп'ютера для навчання якоїсь дисципліни або предмету. Системи навчання діагностують помилки при вивченні будь-якої дисципліни за допомогою ЕОМ і підказують правильні рішення. Вони акумулюють знання про гіпотетичного «учня» і його характерні помилки, а потім в роботі вони здатні діагностувати слабкості в пізнаннях учнів і знаходити відповідні засоби для їх ліквідації. Крім того, вони планують акт спілкування з учнем залежно від успіхів учня, з метою передачі знань.
- *Управління*. Під управлінням розуміється функція організованої системи, що підтримує певний режим діяльності. Такого роду ЕС здійснюють управління поведінкою складних систем відповідно до заданих специфікацій.

Підтримка прийняття рішень. Підтримка прийняття рішення - це сукупність процедур, що забезпечує особа, яка приймає рішення, необхідною інформацією та рекомендаціями, що полегшують процес прийняття рішення.

Штучна нейронна мережа (ШНМ) – математична модель, а також її програмне або апаратне втілення, побудована за принципом організації та функціонування біологічних нейронних мереж – мереж нервових клітин живого організму.

Висновок:

Проведено аналіз та визначено особливості застосування інтелектуальних технологій в телекомунікаційних мережах.

Подано основні визначення та класифікацію основних задань, що вирішуються за ждопомогою інтелектуальних інформаційних технологій.

Список використаних джерел:

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К.: Консум. — 2005. — 576 с.

2. Романова А.І. Телекомунікаційні мережі та управління. – Київ: ВПЦ “Київський університет”, 2003. 247 с.

3. Швиденко М.З., Матус Ю.В.. Технології комп’ютерних мереж. / Навч.-метод. посібник., — К., Береста, — 2007. — 420с.

Б. С. Рожнітовський
Національний авіаційний університет, м. Київ

СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ ДО ЗОВНІШНІХ ВПЛИВІВ

Обмеження на використання криптографічних засобів у ряді країн світу та виникнення проблеми захисту прав власності на інформацію, представлену в цифровому вигляді зумовлюють популярність досліджень у сфері стеганографії. Методи стеганографії – приховування і передачі інформації через зображення дозволяють не тільки приховано передавати дані (так звана класична стеганографія), але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку, пошуку інформації в мультимедійних базах даних тощо.

При передачі по каналах зв'язку заповнене зображення-контейнер з великою ймовірністю піддається атакам або підпадає під вплив зовнішніх збурень [1,2].

Завади – сигнали або дії, що спотворюють корисний сигнал, який несе основну інформацію у пристроях зв'язку. Вплив завади може призвести до значних помилок у стеганографічній системі [1,2].

Атаки – це будь-яка спроба детектувати, вилучити, змінити приховане стеганографічне повідомлення [8,21]. Одні стеганографічні додатки частіше потерпають від завад у каналах звя'зку, наприклад, стеганосистеми прихованого зв'язку та системи захисту прав на зображення. Інші постійно піддаються атакам з боку користувачів, особливо при використання стеганографіїї з метою відстеження порушника або виявлення випадків неліцензійного тиражування та шахрайства.

Здатність стеганографічних систем протистояти атакам та завадам називається стійкістю або захищеністю, в залежності від умов та мети впливів [1,3].

Класифікація атак на стеганографічні системи

Існує безліч класифікацій атак на стеганографічні системи, але загалом їх можна поділити на [1,3]:

1. Атаки проти вбудованого повідомлення – направлені на

видалення чи псування ЦВЗ шляхом маніпулювання стеганоконтейнером. Виділяють наступні види даних атак: стиснення зображення, додавання шуму, зміна контрастності, застосування лінійних і нелінійних фільтрів (розмитість, підвищення різкості, медіанна фільтрація).

2. Атаки проти стеганодетектора – направлені на те, щоб зробити важким, або неможливим правильну роботу детектора. При цьому водяний знак в зображенні залишається, але губиться можливість його прийому. Виділяють такі атаки, як афінні перетворення (тобто, масштабування, зсуви, повороти), відсічення зображення, перестановка пікселів, друку/копіювання/сканування, квантування кольорів тощо.

3. Атаки проти протоколу вбудовування повідомлення – в основному пов'язані зі створенням помилкових вкладень та ЦВЗ, інверсією водяних знаків, додаванням кількох ЦВЗ, тощо.

4. Атаки проти самого водяного знаку – спрямовані на оцінювання та вилучення ЦВЗ із стеганосистеми, по можливості без спотворення контейнера. У цю групу входять такі атаки, як атаки змови, статистичного усереднення, методи очищення сигналів від шумів, деякі види нелінійної фільтрації та інші.

Дослідження стійкості стеганографічних систем до атак

Для дослідження впливу атак проти стеганографічного детектора розглядаються геометричні атаки, тому що саме їх найчастіше застосовують до зображень середньостатистичні користувачі, переслідуючи особисті цілі. Геометричні атаки математично моделюються як афінні перетворення невідомі детектору. Вони призводять до

втрати синхронізації в детекторі, при цьому водяний знак у зображенні залишається, але втрачається можливість правильного його детектування [1,2,3].

Результати геометричних впливів на здатність правильного детектування ЦВЗ наведені в табл. 1, де тут і в подальшому НЗБ – метод заміни найменш значущого біта, КДБ – метод Кутера-Джордана-Боссена, КЖ – метод Коха-Жао, БМЕЮ – метод Бенгама-Мемона-Ео-Юнга, ДВП – метод на основі вейвлет-перетворення. У відсотках вказана максимально допустима величина змін. Реалізація атак здійснювалася за допомогою програмних засобів Adobe Photoshop і Microsoft Office Picture Manager [2,3].

Таблиця 1

Аналіз стійкості до атак проти стеганографічного детектора

Вид геометричної атаки	в просторовій обл.		в частотній обл.		в обл. перетв.
	НЗБ	КДБ	КЖ	БМЕЮ	ДВП
1. Масштабування	–	–	–	–	–
2. Зміна пропорцій	–	17%	1%	–	–
3. Повороти	–	–	–	–	+
4. Відсічення	–	–	–	–	+
6. Яскравість	–	17%	18%	15%	20%
7. Контрастність	–	52%	55%	5%	60%

Після аналізу зображень опорних зображень, зробимо висновок, що атаки проти стеганодетектора засновані на масштабуванні, повороті і відсіченні зображення призводять до не спрацювання детектора. Жоден з досліджуваних методів не виявив до них стійкості.

Таким чином, найвищий рівень стійкості та захищеності до стеганографічних атак серед методів вбудовування у просторову область показав метод Куттера-Джордана-Боссена. Але навіть він значно програє методам, що використовують область перетворення, при дослідженні впливів атак проти вбудованого повідомлення [1,3].

Висновок:

Проведено аналіз стійкості стеганографічних методів приховування інформації до зовнішніх впливів.

Подано основні визначення та класифікацію атак на стеганодетектора.

Список використаних джерел:

1. Конахович Г.Ф. Комп’ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. - Київ: МК-Пресс, 2006. – 288с.

2. Кузнецов О. О. Стеганографія: навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. - Х.: Вид. ХНЕУ, 2011. - 232с.

17. Вовк О.О. Розроблення методики оцінювання важливості характеристик стеганографічних 3горитмів / О.О. Вовк, А.А. Астраханцев // Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі». – Львів, 2014. – № 805. – С. 52 – 60.

Р.М. Кириченко, К.О. Домрачева, І.А. Паламарчук,
Державний університет інформаційно-комунікаційних технологій, м.Київ

ВДОСКОНАЛЕННЯ АЛГОРИТМІВ МАРШРУТИЗАЦІЇ ТА ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ДОСТУПОМ У ЩІЛЬНИХ БЕЗДРОТОВИХ МЕРЕЖАХ ЯК ОСНОВА ПІДВИЩЕННЯ БЕЗПЕКИ ТА ПРОДУКТИВНОСТІ WI-FI МЕРЕЖ НАСТУПНОГО ПОКОЛІННЯ

Сучасні бездротові мережі стикаються з численними викликами, пов’язаними з обмеженою пропускною здатністю, зростанням затримок і підвищеним рівнем інтерференції. Для покращення продуктивності важливо використовувати інтелектуальні алгоритми маршрутизації, які здатні адаптуватися до змінюваних умов. Такі алгоритми можуть аналізувати трафік у режимі реального часу, виявляючи затори та перенаправляючи дані по менш завантажених каналах.

Проблеми щільних бездротових мереж

У щільних бездротових мережах, таких як спортивні арени чи конференц-центри, існує безліч проблем, які впливають на їх ефективність. По-перше, висока щільність користувачів призводить до збільшення конкуренції за ресурси каналу, що може викликати колізії кадрів. Ці колізії, в свою чергу, зменшують загальну продуктивність мережі, оскільки пакети можуть втрачатися або затримуватися.

По-друге, недостатня інформація про мережеві умови призводить до надмірних перешкод та зменшення пропускної спроможності. У зв'язку з цим, традиційні методи управління доступом і маршрутизації вже не відповідають сучасним вимогам.

Вдосконалення алгоритмів маршрутизації

1. Адаптивні алгоритми маршрутизації

Адаптивні алгоритми маршрутизації здатні динамічно змінювати свої параметри на основі поточних умов у мережі. Це означає, що вони можуть враховувати різні фактори, такі як зміна навантаження, кількість користувачів, їх розташування, а також умови навколишнього середовища, такі як перешкоди і рівень сигналу.

Однією з ключових переваг адаптивних алгоритмів є їхня здатність до самооптимізації. Наприклад, якщо в одній частині мережі спостерігається підвищене навантаження через велику кількість активних користувачів, алгоритм може автоматично перенаправити трафік через менш завантажені канали або точки доступу. Це дозволяє зменшити затримки і підвищити ефективність використання каналу.

Адаптивні алгоритми також можуть використовувати інформацію про якість з'єднання та затримки для оптимізації маршрутів. Вони можуть визначати найкращий шлях для передачі пакетів даних, враховуючи поточну пропускну здатність і швидкість з'єднання. Це особливо важливо в умовах змінних навантажень, де один і той же маршрут може мати різну ефективність у різний час. Застосування таких алгоритмів у бездротових мережах дозволяє знижувати ймовірність колізій та покращувати загальну продуктивність системи.

2. Використання технології MIMO та MU-MIMO

Технології MIMO (Multiple Input Multiple Output) і MU-MIMO (Multi-User MIMO) стали революційними в розвитку бездротових комунікацій. MIMO дозволяє використовувати кілька антен на передавачі та приймачі, що підвищує ефективність передачі даних шляхом одночасної передачі декількох сигналів. Це зменшує ймовірність втрат даних і підвищує швидкість з'єднання.

MU-MIMO, у свою чергу, дозволяє одночасно передавати дані декільком користувачам, що істотно підвищує загальну продуктивність мережі. Завдяки цьому користувачі можуть отримувати дані одночасно, що особливо важливо в середовищах з високою щільністю користувачів, таких як офіси, конференц-зали чи навчальні заклади.

Вдосконалені алгоритми маршрутизації можуть інтегрувати ці технології для забезпечення більш ефективної комунікації між пристроями. Наприклад, алгоритми можуть

автоматично визначати оптимальні маршрути для передачі даних, враховуючи кількість користувачів, їхнє розташування та характеристики сигналу. Це дозволяє максимізувати пропускну здатність мережі та зменшити затримки, забезпечуючи високоякісний зв'язок для всіх користувачів.

Використання MIMO та MU-MIMO також відкриває нові можливості для реалізації нових сервісів, таких як відеоконференції високої чіткості, потокове відео та онлайн-ігри, що вимагають стабільного з'єднання з високою пропускною здатністю. Таким чином, ці технології є важливим елементом у вдосконаленні бездротових мереж наступного покоління, що відповідає зростаючим вимогам до швидкості та надійності.

Централізоване управління доступом

1. Центральні контролери

Централізоване управління доступом за допомогою контролерів дозволяє більш ефективно керувати ресурсами мережі. Контролери можуть збирати дані про стан мережі в реальному часі, що дозволяє здійснювати оперативне реагування на зміни в навантаженні, а також управляти трафіком, що проходить через різні точки доступу.

2. Застосування алгоритмів машинного навчання

Впровадження машинного навчання в алгоритми маршрутизації може значно підвищити їх ефективність. Наприклад, алгоритми можуть навчатися на основі попередніх даних про трафік, визначаючи, які маршрути є найбільш оптимальними в різних умовах. Це дозволить знизити затримки та підвищити швидкість передачі даних, що є критично важливим у ситуаціях з великим навантаженням.

Підвищення безпеки Wi-Fi мереж

1. Впровадження механізмів автентифікації

Забезпечення надійної автентифікації користувачів є критично важливим аспектом безпеки Wi-Fi мереж. Вдосконалені методи автентифікації, такі як WPA3, забезпечують підвищений рівень захисту даних та унеможливлюють несанкціонований доступ до мережі.

2. Системи виявлення та запобігання вторгненням

Інтеграція систем виявлення та запобігання вторгненням (IDS/IPS) в централізоване управління доступом дозволяє миттєво реагувати на потенційні загрози безпеці. Такі системи можуть моніторити трафік у реальному часі та виявляти підозрілі дії.

Висновок

Вдосконалення алгоритмів маршрутизації та централізованого управління доступом у щільних бездротових мережах є ключовими елементами для підвищення безпеки та продуктивності Wi-Fi мереж наступного покоління. Застосування адаптивних алгоритмів маршрутизації, технологій MIMO, централізованих контролерів та машинного навчання дозволяє ефективно управляти ресурсами та зменшувати колізії кадрів. Впровадження механізмів безпеки гарантує захист даних і запобігає несанкціонованому доступу, що робить Wi-Fi мережі більш надійними та продуктивними.

Таким чином, подальше дослідження і розробка нових технологій та алгоритмів стане основою для забезпечення безпеки та ефективності сучасних бездротових мереж.

Список використаних джерел:

1. Климаш Ю.В. Комплексний метод маршрутизації інформаційних потоків у самоорганізованих мережах / 1Ю.В. Климаш, О.М. Шпур, М.В. Кайдан // Вісник Національного університету «Львівська політехніка». Радіоелектроніка та телекомунікації №885 – Львів. – 2017. – С.76-87.

2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. - Pearson Education, Inc., Old Tappan, New Jersey, 2016. – 538 pp.;

Ілля Мойсеєв,
Київський національний університет будівництва і архітектури,
факультет автоматизації інформаційних технологій, кафедра кібербезпеки та
комп'ютерної інженерії спеціальність: 123, Київ, Україна

ПРИВАТНО-ДЕРЖАВНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРЗАХИСТУ

Анотація

Приватно-державне партнерство (ПДП) стає необхідним елементом для забезпечення кіберстійкості держави. У статті аналізуються механізми ПДП в Україні та інших країнах, оцінюється ефективність співпраці державних структур із приватними компаніями для протидії кіберзагрозам, а також розглядаються основні виклики та перспективи розширення ПДП.

Ключові слова

Кібербезпека, приватно-державне партнерство, кіберзагрози, державна безпека, інформаційна безпека.

Вступ

У світі стрімкої цифровізації та зростання кіберзагроз кібербезпека стає пріоритетом для державного та приватного секторів. Кіберінциденти загрожують критичній інфраструктурі, економіці та суспільному життю, вимагаючи об'єднання зусиль для ефективного захисту. ПДП пропонує практичну модель співпраці, що об'єднує ресурси, технології та знання державних і приватних структур, що дозволяє більш ефективно протидіяти сучасним кіберзагрозам.

Дослідження

Аналіз показує, що ефективне ПДП широко застосовується в країнах з розвиненими підходами до кібербезпеки, таких як США та ЄС. Дослідження виявило, що в цих регіонах ПДП стимулюється за рахунок правової бази, стандартизації та технологічного розвитку. В Україні ж, хоча нормативно-правова база для кібербезпеки активно вдосконалюється, проте вона має ряд бар'єрів, що уповільнюють впровадження ПДП. Зокрема:

Конфіденційність: Державні органи і компанії часто обмежені правовими нормами, що регулюють обробку та передачу даних, через що можливості обміну інформацією зменшуються.

Дефіцит кадрів: Брак спеціалістів у сфері кібербезпеки ускладнює реалізацію надійних проектів ПДП. Для подолання цього виклику потрібні інвестиції у підготовку фахівців, зокрема через спільні навчальні програми.

Організаційні та фінансові бар'єри: Державні органи часто мають обмежене фінансування для проектів з кібербезпеки, а різниця у пріоритетах держави та бізнесу створює труднощі для повноцінного співробітництва.

Окрім стандартів ISO/IEC 27001 та 27002, що визнані у світі, українські компанії часто стикаються з необхідністю адаптувати практики відповідно до локальних реалій. Результати аналізу підтверджують, що країни з активними ПДП показують більшу готовність до протидії кіберзагрозам і швидко відновлюються після кіберінцидентів.

Результати дослідження

Результати свідчать, що впровадження ПДП має такі позитивні ефекти:

- Оперативне реагування на кіберзагрози: Державні та приватні організації здатні швидко реагувати на нові загрози завдяки обміну інформацією та технологічним рішенням. Наприклад, банки та телекомунікаційні компанії можуть швидко надати дані про підозрілі дії, попереджуючи широкомасштабні атаки.
- Доступ до інноваційних технологій: Приватний сектор зазвичай володіє новітніми розробками в галузі кіберзахисту, що дозволяє державним структурам захищати критичну інфраструктуру з використанням сучасних технологій без значних додаткових витрат.

- Підвищення компетентності: Спільне навчання та тренування покращують рівень підготовки співробітників обох секторів, розвиваючи навички для вчасного виявлення та нейтралізації кіберзагроз. Зокрема, спільні симуляції кібератак підвищують здатність команд швидко виявляти вразливості.

Аналіз результатів підтверджує, що країни з розвиненими ПДП є більш стійкими до кібератак і демонструють швидше відновлення після інцидентів. Системний обмін знаннями та навичками забезпечує ефективну підготовку як державного, так і приватного сектору, дозволяючи оперативніше реагувати на нові виклики у сфері кіберзахисту.

Висновки

Зміцнення ПДП у сфері кібербезпеки є ключовим для створення кіберстійких суспільств. Міжнародний досвід підтверджує, що для ефективної реалізації ПДП необхідно вдосконалювати правову базу, стимулювати обмін інформацією та інвестувати у професійну підготовку кадрів. Запропоновані підходи можуть підвищити рівень безпеки і забезпечити необхідну синергію для протидії сучасним кіберзагрозам.

Список використаних джерел:

1. Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". Доступно за: https://zakon.rada.gov.ua/laws/show/96/2016#n11.

2. ЄВРОПЕЙСЬКЕ ПРИВАТНО-ДЕРЖАВНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРБЕЗПЕКИ: ПІДХОДИ ДО ФОРМУВАННЯ ТАНОРМАТИВНО-ПРАВОВІ ЗАСАДИ Доступно за: https://niss.gov.ua/sites/default/files/2017-10/Boiko_kiber-3afb5.pdf.

3. Аналітична доповідь Національного Інституту Стратегічних досліджень щодо державно-приватного партерства у сфері кібербезпеки. Доступно за: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberbezpeka.pdf

4. Аналітична доповідь Національного Інституту Стратегічних досліджень: підходи до формування та нормативно-правові засади Доступно за: https://niss.gov.ua/sites/default/files/2017-10/Boiko_kiber-3afb5.pdf.

5. "Partnership for Cybersecurity: Building a National Framework" Доступно за: https://www.csis.org/

Зміст