НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ КОРИСТУВАЧІВ У ЦИФРОВОМУ ПРОСТОРІ»

Виконала здобувачка 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Ігнатенко Анастасія Ігорівна

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.фіз.-мат.н., доцент
Чепурна Олена Євгенівна

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачці Ігнатенко Анастасії Ігорівни

1. Тема роботи: «Методи захисту інформації користувачів у цифровому просторі»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання«15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методи захисту інформації користувачів у цифровому просторі» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 6 рисунків та 21 літературних джерел за переліком посилань. Робота виконана на 42 сторінках загального тексту і 35 сторінках основного тексту.

Метою роботи є аналіз методів захисту інформації користувачів у цифровому просторі.

Визначено види кіберзагроз, включаючи кіберзлочинність, кібершпіонаж, кібертероризм, порушення приватності, соціальний інжиніринг, фішинг та втрати даних, що актуалізує потребу в ефективних методах захисту. Досліджено принципи криптографії, процеси шифрування та дешифрування даних, а також застосування криптографічних протоколів у мережах. Складено програмне забезпечення, необхідне для захисту інформації, включно з антивірусами, фаєрволами та надано певні заходи протидії шкідливим програмам.

Результати даного дослідження можуть бути використані в широкому спектрі областей, включаючи розробку політик безпеки для корпорацій та установ, які прагнуть захистити свої дані та інформаційні системи від сучасних загроз. Зокрема, вони можуть слугувати основою для навчання співробітників з питань кібербезпеки, збільшуючи їх обізнаність щодо потенційних кіберзагроз та методів їхнього усунення.

Можливими напрямками подальших досліджень є розробка нових, більш ефективних криптографічних технологій, які могли би забезпечити кращий захист від зростаючих загроз кібербезпеки.

КІБЕРБЕЗПЕКА, КРИПТОГРАФІЯ, КІБЕРЗЛОЧИННІСТЬ, АНТИВІРУСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЗАХИСТ ДАНИХ.

ABSTRACT

Qualification work on the topic "Methods of protecting user information in the digital space" for the first (bachelor’s) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 6 figures and 21 references in the list of references. The work is performed on 42 pages of the general text and 35 pages of the main text.

The purpose of the work is to analyze the methods of protecting user information in the digital space.

The types of cyber threats are identified, including cybercrime, cyberespionage, cyberterrorism, privacy violation, social engineering, phishing and data loss, which actualizes the need for effective protection methods. The principles of cryptography, data encryption and decryption processes, and the use of cryptographic protocols in networks are studied. The software necessary to protect information, including antiviruses, firewalls, and certain measures to counteract malware, is compiled.

The results of this research can be used in a wide range of areas, including the development of security policies for corporations and institutions seeking to protect their data and information systems from modern threats. In particular, they can serve as a basis for cybersecurity training for employees, increasing their awareness of potential cyber threats and methods to address them.

Possible areas for further research include the development of new, more effective cryptographic technologies that could provide better protection against growing cybersecurity threats.

CYBERSECURITY, CRYPTOGRAPHY, CYBERCRIME, ANTIVIRUS SOFTWARE, DATA PROTECTION.

ЗМІСТ

ВСТУП

У сучасну епоху цифрових технологій та Інтернету значення захисту інформації користувачів стає критично важливим. Кількість даних, які ми щоденно передаємо в цифровому просторі, невпинно зростає, охоплюючи все від банківських операцій до особистого спілкування. Разом з цим, зростає й кількість загроз: від кіберзлочинців до великих корпорацій, що збирають і аналізують дані.

Цифровий простір може здаватися незримим і абстрактним, проте його вплив на реальне життя людей є величезним. Порушення конфіденційності або крадіжка особистих даних може мати серйозні наслідки для індивідуальної безпеки та фінансового становища. Крім того, захист інформації користувачів має велике значення для довіри до цифрових послуг та розвитку цифрової економіки.

Дослідження методів захисту інформації користувачів дозволяє краще зрозуміти, як саме кіберзлочинці можуть отримати доступ до особистих даних, а також які технології та стратегії забезпечують ефективний захист. Це охоплює різноманітні сфери, включаючи криптографію, аутентифікацію, моніторинг безпеки та розробку безпечного програмного забезпечення.

З вищевикладеного не виникає сумнівів, що обрана тема дослідження методів захисту інформації користувачів у цифровому просторі є актуальною на сьогоднішній день.

Мета дослідження полягає в дослідженні та аналізі методів захисту інформації користувачів у цифровому просторі. Дослідження включає в себе огляд сучасних кіберзагроз та ризиків, аналіз основних методів захисту, а також вивчення важливості освіти користувачів у сфері кібербезпеки.

Для досягнення поставленої мети необхідно виконати наступні завдання: визначити сучасні загрози та ризики у цифровому просторі; проаналізувати криптографічні методи захисту інформації; надати програмне забезпечення для захисту інформації.

Об’єктом дослідження є процеси забезпечення безпеки та конфіденційності інформації користувачів у цифровому просторі.

Предмет дослідження це методи та технології захисту інформації користувачів у цифровому просторі.

Практичне значення отриманих результатів полягає у тому, що робота дає інформацію про ефективні методи захисту, які допоможуть користувачам зберегти конфіденційність своїх даних та захистити себе від кіберзагроз. Результати дослідження будуть корисні як для звичайних користувачів, так і для організацій, що прагнуть підвищити рівень захищеності своєї інформації в онлайн середовищі.

1 ОГЛЯД СУЧАСНИХ ЗАГРОЗ ТА РИЗИКІВ У ЦИФРОВОМУ ПРОСТОРІ

1.1 Кіберзлочинність

Кіберзлочинність є однією з найбільш серйозних загроз у сучасному цифровому просторі. Вона включає в себе широкий спектр злочинних дій, які відбуваються в інтернеті та мережах цифрового простору, спрямованих на отримання несанкціонованого доступу до інформації, шахрайство, фінансові маніпуляції та інші злочинні активності. Ці атаки можуть мати різні наміри та наслідки, що ставить під загрозу безпеку користувачів, організацій та навіть держав.

Одним із найпоширеніших видів кіберзлочинності є фішинг, який полягає у використанні підроблених електронних листів або веб-сайтів для отримання конфіденційної інформації, такої як паролі, номери кредитних карток або інші особисті дані. Кіберзлочинці також використовують віруси та шкідливе програмне забезпечення для незаконного доступу до комп’ютерних систем, крадіжки інформації або завдання шкоди пристроям користувачів. Атаки відмови у обслуговуванні (DDoS) спрямовані на перевантаження серверів або мережі та зниження їх доступності для законних користувачів [1].

Ще однією серйозною загрозою є вимагання викупу за даними, коли кіберзлочинці зашифровують файли на комп’ютері жертви та вимагають викуп для їх розблокування. Якщо вимоги не виконуються, це може призвести до втрати важливої інформації або навіть назавжди знищити дані.

Крім перерахованих загроз, важливо зазначити, що кіберзлочинці постійно розвивають свої методи та стратегії, адаптуючись до нових технологій та захисту. Вони активно використовують подвійні атаки та хмарні сервіси, щоб уникнути виявлення та виявити уразливості в системах. Також стає все більш поширеним злам програмного забезпечення (exploit kits), які використовують вразливості в програмному забезпеченні для отримання несанкціонованого доступу до систем.

Порушення кібернетичної інфраструктури є ще однією серйозною загрозою. Кібератаки на критичні інфраструктурні об’єкти, такі як електростанції, водні

споруди, транспортні системи та інші, можуть мати серйозні наслідки для громадської безпеки та економіки.

Також, зловживання штучного інтелекту стає все більшою загрозою в цифровому просторі. Кіберзлочинці можуть використовувати алгоритми штучного інтелекту для виявлення вразливостей, вдосконалення атак та навіть для створення нових видів шкідливого програмного забезпечення, яке може обходити традиційні системи захисту [2].

Оскільки кіберзлочинці постійно еволюціонують та вдосконалюють свої методи, важливо мати постійно оновлені технології та стратегії захисту. Проактивний підхід до кібербезпеки, регулярне навчання та оновлення знань, а також постійна відстеження нових загроз можуть допомогти зменшити ризики та забезпечити безпеку в цифровому просторі.

Додатковою загрозою є інтернет в речах (IoT), оскільки зростає кількість підключених до Інтернету пристроїв, таких як веб-камери, домашні роутери, термостати тощо. Ці пристрої часто мають недостатні заходи безпеки, що робить їх вразливими до атак та зловмисного використання. Наприклад, хакер може використовувати незахищений веб-камеру для вторгнення в приватність користувача або використання її в складі ботнету для здійснення DDoS-атак.

Крім того, соціальні мережі також є місцем, де кіберзлочинці шукають потенційних жертв. Вони можуть використовувати підроблені профілі або шахрайські схеми, щоб отримати доступ до особистої інформації користувачів або шахрайських фінансових операцій.

Іншою серйозною загрозою є кібершпіонаж та кібертероризм. Державні актори та терористичні групи можуть використовувати кіберзлочинність для здійснення шпигунських операцій, збирання розвідувальної інформації або навіть виконання кібератак на критичну інфраструктуру держави або організацій [3].

Загроза кіберзлочинності є постійною і потенційною, тому важливо постійно бути на сторожі та приймати заходи для захисту своєї інформації та пристроїв. Це включає в себе використання надійного антивірусного програмного забезпечення,

встановлення оновлень безпеки, складних паролів та двофакторної аутентифікації, а також підтримку своїх знань про кібербезпеку.

1.2 Кібершпіонаж та Кібертероризм

Кібершпіонаж та кібертероризм представляють собою серйозні загрози в цифровому просторі, що становлять потенційну небезпеку для національної безпеки, промислового секрету, особистої конфіденційності та інфраструктури критичних систем.

Кібершпіонаж – це процес отримання конфіденційної або чутливої інформації з комп'ютерних систем, мереж та інших цифрових пристроїв шляхом використання кібератак та технологій шпигунства. Головною метою кібершпіонажу є отримання доступу до інформації, яка може бути корисною для розвідки, політичної або військової стратегії, конкурентного шпигунства, промислового шпигунства тощо.

Кібершпіонаж може бути здійснений різними суб'єктами, включаючи державні органи, злочинців, конкуруючі підприємства, хакерські групи та інші. Ці суб'єкти можуть використовувати різноманітні методи, такі як віруси, троянські програми, розподілені атаки з використанням мережевих пристроїв (ботнетів), фішинг, соціальний інжиніринг та інші, для здійснення кібершпіонажу [4].

Основні цілі кібершпіонажу можуть включати в себе отримання конфіденційної інформації про військові стратегії, політичні плани, економічні звіти, технологічні розробки, комерційні секрети, персональні дані користувачів тощо. Ця інформація може бути використана для отримання переваги в конкурентній боротьбі, для здійснення шпигунських або дестабілізуючих дій проти інших держав або організацій, або для отримання фінансової вигоди.

Кібершпіонаж може мати різні форми та механізми виконання, включаючи:

Витік конфіденційної інформації – це процес незаконного отримання і розголошення конфіденційних даних або документів з комп'ютерних систем або

мереж. Ця форма кібершпіонажу може мати серйозні наслідки для організацій та осіб, які стають жертвами.

Шпигунське програмне забезпечення є одним зі засобів, які використовуються кіберзлочинцями для незаконного отримання конфіденційної інформації. Це зловмисне програмне забезпечення призначене для таємного відслідковування діяльності користувачів на їхніх комп'ютерах або інших електронних пристроях. Основною метою використання шпигунського ПЗ є отримання доступу до конфіденційної інформації, такої як паролі, особисті дані, фінансові інформації, а також документи і файлів [5].

Використання вразливостей в програмному забезпеченні або операційних системах є одним з основних методів кіберзлочинців для отримання доступу до систем та конфіденційної інформації. Вразливості – це слабкі місця в програмному забезпеченні або операційних системах, які можуть бути використані для несанкціонованого доступу або виконання зловмисних дій.

Кіберзлочинці шукають вразливості в програмному забезпеченні та операційних системах, і коли вони знаходять їх, вони можуть використовувати різні методи для експлуатації цих вразливостей.

«Вибух буфера» – Кіберзлочинці можуть використовувати вразливості у програмах, які не впораються з обробкою великої кількості даних, щоб записати код на вразливий ділянку пам'яті і виконати зловмисний код.

«Вибух стеку» – Це атака, яка використовує вразливості у стековому механізмі операційних систем або програм, щоб виконати зловмисний код або отримати доступ до системи.

«Вибух формата файлу» – Кіберзлочинці можуть створити спеціально сформований файл, який використовує вразливості у програмах для виконання зловмисних дій під час обробки цього файлу.

«Використання вразливих ділянок пам'яті» Кіберзлочинці можуть використовувати вразливості у пам'яті, такі як витік пам'яті або некоректне управління пам'яттю, для отримання доступу до конфіденційної інформації або виконання зловмисних дій.

«Використання вразливостей мережевого стеку» Кіберзлочинці можуть використовувати вразливості у мережевому стеку операційних систем для отримання доступу до системи або виконання атак віддаленого виконання коду.

«Використання анонімних мереж та проксі-серверів» Кіберзлочинці можуть приховати свою ідентичність та місце розташування, використовуючи анонімні мережі та проксі-сервери, щоб уникнути виявлення під час кібершпіонажу.

«Використання розподілених мереж», Кіберзлочинці можуть використовувати ботнети, щоб керувати великою кількістю комп'ютерів або пристроїв, які були заражені шкідливим програмним забезпеченням, та використовувати їх для виконання кібершпіонажу [6].

Ці та інші методи дозволяють кіберзлочинцям ефективно виконувати кібершпіонаж і отримувати доступ до конфіденційної інформації з комп'ютерних систем та мереж.

Кібертероризм – це використання кібератак для здійснення терористичних дій або для поширення страху та паніки серед населення. Терористичні організації можуть використовувати кіберзлочинність для атак на критичну інфраструктуру, включаючи електроенергетичні мережі, банківські системи, транспорт та інші сектори, або для розповсюдження пропаганди та кіберпропаганди. Кібертерористичні атаки можуть мати серйозні наслідки для безпеки громадян та економічної стабільності. Такі атаки можуть призвести до великих матеріальних збитків, порушень нормального функціонування суспільства та загрози життю і здоров'ю людей [7].

Кібертерористичні атаки можуть мати різні форми.

Атаки на критичну інфраструктуру, Злочинні групи можуть намагатися зруйнувати або порушити роботу критичних систем, таких як електростанції, водопостачання, транспортні мережі тощо, що може призвести до серйозних наслідків для суспільства.

Фінансові атаки, Кібертерористи можуть намагатися здійснити атаки на фінансові установи, банківські системи або електронні платіжні системи з метою викликати фінансовий хаос або здійснити крадіжку коштів.

Кіберпропаганда та дезінформація, Кібертерористи можуть використовувати соціальні мережі, вебсайти та інші кіберзасоби для поширення пропаганди, маніпуляції громадською думкою або розповсюдження дезінформації з метою викликати паніку або невпевненість.

Кібератаки на критичні інформаційні системи, Кібертерористи можуть намагатися здійснити атаки на критичні інформаційні системи, такі як урядові мережі, військові системи зв'язку або системи контролю та управління, з метою порушення нормального функціонування цих систем та викликання загрози національній безпеці.

Запобігання кібертерористичним атакам вимагає комплексного підходу, який включає в себе зміцнення кібербезпеки, підвищення обізнаності громадськості про кіберзагрози, співпрацю між державними та приватними секторами, а також розвиток міжнародних механізмів співробітництва у сфері кібербезпеки. Тільки таким чином можна забезпечити ефективний захист від кібертероризму і зберегти безпеку та стабільність в цифровому просторі.

Для захисту від кібершпіонажу та кібертероризму необхідно впроваджувати комплексні заходи кібербезпеки. Це включає в себе підвищення свідомості щодо кіберзагроз, регулярне оновлення та підтримку програмного та апаратного забезпечення, використання систем виявлення та запобігання інцидентам, розвиток та впровадження стратегічних планів кібербезпеки та співпрацю з міжнародними організаціями та іншими державами для обміну інформацією та спільного протидії кіберзагрозам.

У часи постійного розвитку технологій та зростання злочинності в цифровому просторі, важливо підтримувати постійний рівень готовності та вдосконалювати заходи захисту, щоб забезпечити безпеку і стабільність в інтернеті та кіберпросторі загалом.

Додатково, кібершпіонаж та кібертероризм стають все більш важливими в контексті геополітичних конфліктів. Державні актори можуть використовувати кіберзлочинність як засіб ведення гібридної війни або для досягнення своїх політичних цілей. Кібератаки можуть бути спрямовані на державні установи,

політичні організації, а також на населення з метою дестабілізації суспільства та зміни геополітичного статусу-кво.

Зокрема, атаки на виборчі системи та політичні партії можуть порушити демократичні процеси та навіть підірвати довіру громадян до виборчої системи. Крім того, кібератаки можуть бути використані для впливу на громадську думку через розповсюдження дезінформації та фейкових новин.

Іншою складністю є анонімність та важкість визначення атакуючого в кіберпросторі. Це ускладнює проведення розслідувань та виявлення винних осіб, що робить кіберзлочинність більш привабливою стратегією для державних та нетериторіальних акторів.

Для протидії кібершпіонажу та кібертероризму необхідно підтримувати міжнародну співпрацю, встановлювати міжнародні стандарти кібербезпеки та правила міжнародної поведінки в кіберпросторі. Також важливо розвивати та впроваджувати технології штучного інтелекту та машинного навчання для виявлення та відстеження кіберзагроз.

Загальна свідомість та готовність до кібератак також важливі для забезпечення безпеки. Організації та індивідуали повинні регулярно навчатися про кібербезпеку, робити резервні копії даних, використовувати надійне програмне забезпечення та вживати інші заходи захисту, щоб мінімізувати ризики кіберзлочинності [8].

Важливо враховувати потенційні наслідки кібершпіонажу та кібертероризму на економіку та підприємництво. Кібератаки можуть призвести до великих фінансових втрат для компаній та держав, включаючи втрати даних, розголошення конфіденційної інформації, порушення діяльності підприємств та інше. Це може мати далекосяжні наслідки для глобальної економіки та стабільності фінансових ринків.

Ростуча залежність від інформаційних технологій у всіх аспектах життя суспільства робить нас більш вразливими перед кіберзагрозами. Від сучасних медичних систем та електронного урядування до підприємств та особистих

пристроїв, всі аспекти нашого життя переплітаються з цифровим простором, що робить необхідним постійне підтримування високого рівня кібербезпеки.

Наприклад, кібератаки на медичні системи можуть ставити під загрозу життя пацієнтів, викраденням конфіденційних медичних даних або навіть заблокуванням доступу до життєвоважливих медичних пристроїв. Кібератаки на електронні системи голосування можуть порушити демократичні процеси та викликати недовіру до результатів виборів.

Отже, необхідно враховувати широкі наслідки кіберзагроз і розробляти комплексні підходи до їх протидії. Це включає в себе співпрацю між державами, сектором приватного бізнесу та громадськістю, розробку стратегічних планів кібербезпеки та постійне підвищення свідомості щодо кіберзагроз та заходів захисту. Тільки таким чином ми зможемо ефективно протистояти кібершпіонажу та кібертероризму і забезпечити безпеку та стабільність у цифровому світі.

1.3 Порушення приватності

Порушення приватності становить серйозну загрозу для користувачів у цифровому просторі, особливо в умовах зростаючого обсягу збору та обробки особистих даних компаніями. Великі організації, що мають доступ до значних обсягів особистої інформації, можуть стати об’єктом порушень приватності через недбале використання або зловживання цими даними.

Компанії збирають та обробляють великі обсяги особистих даних користувачів для різних цілей, включаючи маркетингові дослідження, персоналізовану рекламу, аналітику та інші. Однак недбале зберігання або обробка цих даних може призвести до їх витоку або неналежного використання.

Порушення безпеки даних може призвести до витоку особистої інформації користувачів через хакерські атаки, внутрішні проблеми з безпекою або інші кіберзагрози. Це може включати витік імен, адрес, електронних поштових скриньок, фінансових даних та інших особистих даних, що може підірвати довіру користувачів та завдати шкоди їхній приватності.

Важливо, щоб компанії вживали належних заходів для захисту особистих даних користувачів, включаючи шифрування, використання безпекових протоколів, регулярні аудити безпеки та впровадження строгих правил доступу до даних.

Компанії повинні також дотримуватися вимог щодо захисту даних, встановлених законодавством про захист персональних даних, таких як Загальний регламент про захист персональних даних (GDPR) в Європейському Союзі або Каліфорнійський Закон про Конфіденційність споживача (CCPA) в США.

Втрата особистих даних через витік або порушення приватності може призвести до втрати довіри користувачів до компанії та її послуг. Тому важливо для компаній будувати довіру шляхом ефективного захисту та обробки особистих даних користувачів.

1.4 Соціальний інжиніринг

Соціальний інжиніринг є процесом маніпулювання людьми з метою отримання конфіденційної інформації або здійснення інших злочинних дій. Це ефективний метод атаки, оскільки використовує людські фактори, такі як довіра, невпевненість або недбалість, для досягнення своїх цілей. Атаки соціального інжинірингу можуть приймати різні форми та включати в себе такі дії.

Наприклад, зловмисники можуть виглядати як представники технічної підтримки або інші авторитетні особи, що запитують паролі або інші конфіденційні дані під виглядом необхідності для вирішення технічних проблем.

Шахраї можуть намагатися переконати людей відправити гроші, використовуючи різні схеми обману, такі як виграш у лотерею, невідкладна допомога або фальшиві історії про нещастя.

Імперсоніфікація авторитетних осіб. Зловмисники можуть виглядати як представники владних органів, фінансових установ або інших авторитетних осіб для отримання доступу до конфіденційної інформації або виконання інших дій.

Шахраї здійснюють телефонні дзвінки з метою обману та вибудовування довіри, наприклад, шляхом надання фальшивої інформації або використання загроз або переляку [9].

Ефективна захист від атак соціального інжинірингу включає в себе навчання персоналу щодо виявлення шахрайських методів, регулярну оновлення політик безпеки та процедур аутентифікації, а також підвищення обізнаності користувачів щодо ризиків інтернет-шахрайства.

1.5 Фішинг користувачів

Фішинг користувачів – це вид атаки, коли зловмисники намагаються отримати конфіденційні дані, такі як логіни, паролі або фінансові інформації, шляхом підробки легітимних комунікацій з користувачами. Це може бути електронний лист, повідомлення в соціальних мережах або вебсайт, які виглядають як легітимні, але насправді створені шахраями з метою обману.

Наприклад, фішингове повідомлення може виглядати як легітимний електронний лист від банку, вебсайту електронної комерції або іншої організації, яка просить вас оновити свої облікові дані або ввести конфіденційну інформацію через посилання, вкладені файли або форми на підробленому вебсайті.

Ось деякі загальні ознаки фішингу, які варто враховувати.

Фішингові повідомлення можуть створювати штучний тиск на користувачів, намагаючись викликати паніку або створити відчуття невідкладності.

Перевірте адресу електронної пошти відправника та джерело повідомлення. Часто фішингові повідомлення приходять від підроблених або неперевірених адрес електронної пошти [10].

Фішингові повідомлення можуть містити орфографічні помилки, незвичайний стиль або неправильно розміщені логотипи організацій.

Будьте обережні з посиланнями або вкладеннями у фішингових повідомленнях. Не натискайте на них, якщо ви не впевнені в їхній автентичності.

Ніколи не надавайте конфіденційні дані через електронну пошту або повідомлення в соціальних мережах, особливо якщо це стосується фінансових даних або облікових записів.

1.6 Втрати даних

Втрата даних становить серйозну загрозу для користувачів та організацій, оскільки може призвести до великих втрат інформації, фінансових збитків та порушення діяльності. Деякі з основних причин втрати даних включають випадкове видалення, атаки вірусів або вимагачів, а також технічні проблеми з обладнанням або програмним забезпеченням. Для запобігання втратам даних і забезпечення безпеки інформації важливо вживати наступні заходи.

Регулярно створюйте копії важливих даних і зберігайте їх в безпечному місці, окрім основної робочої системи. Це допоможе відновити дані у разі їх втрати або пошкодження.

Встановіть та регулярно оновлюйте антивірусне програмне забезпечення для захисту комп’ютерів та інших пристроїв від вірусів та шкідливих програм, які можуть призвести до втрати даних.

Захистіть свої системи від атак вимагачів шляхом регулярного оновлення програмного забезпечення, використання програм для блокування вмісту, обмеження прав доступу та навчання користувачів профілактиці шахрайства.

Забезпечте захист фізичної інфраструктури, де зберігаються сервери та інші системи з важливою інформацією, від несанкціонованого доступу, пожеж та інших ризиків.

Навчіть користувачів основам безпеки інформації, включаючи створення надійних паролів, розпізнавання підозрілих повідомлень та поведінку в разі виявлення аномальних ситуацій.

Забезпечення надійного захисту та регулярне вживання заходів безпеки допоможе уникнути втрати важливих даних та зберегти інформаційну цілісність користувачів та організацій.

Загрози та ризики у цифровому просторі постійно зростають, і важливо, щоб користувачі та організації були уважними та приймали заходи для захисту своєї інформації. Це включає в себе використання сильних паролів, оновлення програмного забезпечення, навчання користувачів правилам кібербезпеки та використання захисту даних за допомогою шифрування та інших технологій захисту. Вживання відповідних заходів захисту та уважність при користуванні цифровими технологіями є ключем до забезпечення безпеки інформації. Завдяки цим заходам, користувачі та організації можуть зменшити ризики кіберзлочинів та забезпечити захист своїх даних у цифровому просторі.

2 КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Основні принципи криптографії

Основні методи криптографічного захисту інформації включають наступні пункти.

Шифрування – процес перетворення звичайного тексту в зашифрований формат за допомогою ключа. Шифрування забезпечує конфіденційність даних, ускладнюючи доступ до них без належного ключа. головна мета шифрування – забезпечити конфіденційність даних, ускладнюючи доступ до них без належного ключа.

Процес шифрування використовується для захисту важливої інформації від несанкціонованого доступу та перегляду. При цьому сам алгоритм шифрування може бути симетричним або асиметричним.

Симетричне шифрування - Використовується один і той самий ключ для як шифрування, так і розшифрування даних. Такий підхід є швидшим, але вимагає безпечного обміну ключами між відправником і одержувачем.

Асиметричне шифрування – Використовує пару ключів: публічний та приватний. Публічний ключ використовується для шифрування даних, тоді як приватний ключ використовується для їх розшифрування. Цей метод не вимагає обміну ключами, але може бути менш ефективним з точки зору швидкості.

Шифрування є важливою складовою криптографічного захисту інформації, і використовується в різних областях, включаючи комунікаційні системи, збереження даних, фінансові та медичні системи тощо [11].

Хешування – процес перетворення даних в хеш-код фіксованої довжини за допомогою хеш-функції. Хеш-код може використовуватися для перевірки цілісності даних: будь-яка зміна в початкових даних призведе до іншого хеш-коду. Основна властивість хеш-функцій полягає в тому, що будь-яка зміна в початкових даних (навіть маленька) призведе до значної зміни у вихідному хеш-коді.

Хеш-функції широко використовуються для перевірки цілісності даних. Наприклад, при передачі файлу можна обчислити хеш-код цього файлу перед

відправкою та відправити разом із файлом. Отримувач може обчислити хеш-код отриманих даних і порівняти його з отриманим хеш-кодом. Якщо хеш-коди збігаються, це означає, що дані не були змінені під час передачі.

Хеш-функції часто використовуються для зберігання паролів у формі хешів замість самих паролів у базі даних. Це забезпечує більшу безпеку, оскільки відновити пароль з хеш-коду неможливо, але можна перевірити відповідність введеного пароля хешу, збереженому в базі даних.

Основні властивості хеш-функцій включають фіксовану довжину вихідного значення, що залишається незмінною незалежно від розміру вхідних даних. Кожній унікальній послідовності вхідних даних відповідає унікальний хеш-код. Важливою характеристикою хеш-функцій є неможливість відновлення вхідних даних з хеш-коду, а також чутливість до змін вхідних даних: навіть невелика зміна призведе до значної зміни в хеш-коді.

Хеш-функції використовуються для зберігання паролів у безпечному форматі, перевірки цілісності даних, шифрування паролів та дігестів повідомлень, індексування даних у хеш-таблицях та інших цілей. Вони є важливим інструментом для криптографічного захисту інформації і застосовуються у широкому спектрі сфер інформаційної безпеки.

Цифровий підпис – механізм, що забезпечує аутентифікацію та незаперечність даних. Використовується для підтвердження авторства документа та гарантує, що документ не був змінений після підпису. Основна мета цифрового підпису - надати можливість отримувачеві перевірити, що документ був створений або затверджений конкретним відправником і не був змінений після підпису [12].

Основні принципи роботи цифрового підпису включають використання асиметричного шифрування, де відправник створює підпис, використовуючи свій приватний ключ, а отримувач може перевірити цей підпис за допомогою відкритого ключа відправника. Якщо підпис вірний, це дозволяє отримувачеві підтвердити автентичність та цілісність документа.

Цифрові підписи широко використовуються у різних сферах, таких як електронна комунікація, фінанси, електронний документообіг, електронна торгівля

та багато інших. Вони дозволяють забезпечити безпеку та надійність обміну даними відправників та отримувачів.

Протоколи захищеної комунікації – це набір стандартів і правил, що використовуються для забезпечення безпеки передачі даних через мережі. Їх основна мета - забезпечити конфіденційність, цілісність і аутентичність даних під час їх передачі між двома або більше вузлами мережі.

Деякі з найпоширеніших протоколів захищеної комунікації включають.

TLS (Transport Layer Security) є стандартним протоколом захищеної комунікації, який забезпечує шифрування, аутентифікацію та цілісність даних між клієнтом і сервером в мережах Інтернету.

SSL (Secure Sockets Layer) є попередником TLS і використовується для тих самих цілей. Проте вважається менш безпечним порівняно з TLS через виявлені уразливості.

IPsec (Internet Protocol Security) – це протокол захищеної комунікації, що працює на рівні мережі OSI. Він забезпечує безпеку та конфіденційність на рівні IP, зашифровуючи і аутентифікуючи пакети даних.

SSH (Secure Shell) - це протокол мережевого протоколу, що використовується для безпечного з’єднання між вузлами мережі через незахищені мережі. Він забезпечує шифрування даних, аутентифікацію та інші функції безпеки.

VPN (Virtual Private Network) – це технологія, яка створює зашифроване з’єднання між користувачем та мережею, забезпечуючи безпеку та конфіденційність даних [13].

Ці протоколи використовуються для різних цілей і можуть застосовуватися в різних областях, включаючи безпеку мережі, захист веб-сайтів, захист електронної пошти, віддалений доступ до систем і багато іншого.

Ключі використовуються для шифрування та розшифрування даних, а також для генерації та перевірки цифрових підписів. Важливо забезпечити безпеку ключів, оскільки вони визначають рівень доступу до зашифрованих даних. Залежно від конкретного застосування, існують різні типи ключів.

Симетричні ключі - використовуються для симетричного шифрування, де той самий ключ використовується для як шифрування, так і розшифрування даних. Ці ключі мають бути обмінені між відправником та отримувачем безпечним каналом перед початком обміну даними.

Асиметричні ключі – використовуються для асиметричного шифрування, де пара ключів (приватний і публічний) використовується для шифрування та розшифрування даних. Приватний ключ залишається конфіденційним, тоді як публічний ключ розповсюджується для шифрування даних або перевірки підпису.

Ключі аутентифікації - використовуються для аутентифікації користувачів або систем у процесі взаємодії. Зазвичай це секретні або відомі тільки сторонам значення, які перевіряються під час аутентифікації.

Ключі генерації випадкових чисел - використовуються для генерації випадкових значень, які можуть використовуватися в криптографічних процесах, таких як створення ключів шифрування.

Важливо забезпечити безпеку ключів, оскільки вони визначають рівень доступу до зашифрованих даних або можуть використовуватися для підтвердження ідентичності користувачів чи систем. Неналежне зберігання або використання ключів може призвести до компрометації безпеки даних.

2.2 Шифрування та дешифрування даних

Шифрування та дешифрування даних – це процес застосування математичних алгоритмів (криптографічних ключів) для перетворення звичайного тексту в зашифрований формат, що робить його незрозумілим для незаконних користувачів. ей процес забезпечує конфіденційність інформації, оскільки шифрований текст неможливо зрозуміти без відповідного ключа для розшифрування.

Шифрування даних включає в себе:

− вибір шифрувального алгоритму, обирається певний алгоритм, який буде використовуватися для шифрування даних, існують різні типи шифрування, такі як

симетричне і асиметричне шифрування.

− генерація ключа, для симетричного шифрування використовується один ключ для шифрування та дешифрування, тоді як для асиметричного шифрування використовуються два ключі: публічний та приватний.

− шифрування даних, звичайний текст перетворюється в зашифрований формат за допомогою обраних алгоритмів та ключів, що робить його незрозумілим для незаконних користувачів [14].

− Використання шифрування даних:

− захист конфіденційної інформації: важливі дані можна зашифрувати перед передачею чи зберіганням, щоб запобігти несанкціонованому доступу.

− безпека в мережах: шифрування даних в мережах допомагає захистити інформацію від перехоплення або модифікації під час передачі.

− забезпечення цілісності даних: деякі методи шифрування також можуть забезпечувати перевірку цілісності даних, що дозволяє переконатися, що вони не були змінені під час передачі.

Шифрування даних є важливим засобом забезпечення безпеки інформації в сучасному цифровому світі, зокрема в онлайн-комунікаціях, банківських операціях, зберіганні конфіденційних даних та багатьох інших сферах.

Дешифрування даних включає в себе:

− отримання зашифрованих даних – шифрований текст отримується для подальшого дешифрування;

− використання ключа: для дешифрування даних необхідно мати відповідний ключ, який був використаний під час шифрування, також для симетричного шифрування це той самий ключ, що використовувався для шифрування, тоді як для асиметричного шифрування потрібно використовувати приватний ключ, який відповідає публічному ключу, що був використаний для шифрування;

− дешифрування даних: за допомогою відповідного ключа та алгоритму дешифрування зашифрований текст перетворюється назад у звичайний, зрозумілий формат [14];

− використання дешифрування даних: отримання конфіденційної інформації, дешифрування дозволяє отримати доступ до захищеної інформації, яка була зашифрована з метою збереження конфіденційності;

− робота з зашифрованими даними, після дешифрування дані можуть бути оброблені або використані так само, як і будь-які інші незашифровані дані;

− забезпечення цілісності даних: деякі методи дешифрування можуть також перевіряти цілісність даних, допомагаючи впевнитися, що вони не були пошкоджені або змінені під час передачі.

Дешифрування даних є важливим етапом у забезпеченні безпеки інформації та забезпеченні доступу до конфіденційних даних у сучасному цифровому світі.

2.3 Використання криптографічних протоколів в мережах

В мережах криптографічні протоколи використовуються для забезпечення безпеки під час обміну даними між вузлами мережі. Деякі з найпоширеніших криптографічних протоколів включають SSL/TLS для захищеного з’єднання між веб-серверами і браузерами, а також IPSec для безпечної передачі даних через відкриті мережі, такі як Інтернет [15].

Ці криптографічні методи допомагають забезпечити конфіденційність, цілісність, аутентифікацію та неденіабельність даних в мережах та зберегти їх безпеку під час передачі та зберігання.

3 ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Антивірусні програми та їх функції

Антивірусне програмне забезпечення призначене для виявлення, блокування та видалення шкідливого програмного забезпечення, такого як: віруси; троянські програми; шпигунське програмне забезпечення тощо.

Основні функції антивірусних програм включають:

− сканування файлів: антивірусне програмне забезпечення сканує файлову систему та детектує наявність потенційно шкідливих файлів.

− виявлення загроз: воно визначає потенційно небезпечні програми, віруси, черви, троянці та інші загрози на основі відомих вірусних сигнатур або алгоритмів виявлення поведінки.

− блокування вторгнень: антивіруси можуть блокувати спроби шкідливого програмного забезпечення вторгнутися до системи, перешкоджаючи їх виконанню.

− видалення або знищення шкідливих програм: після виявлення вірусу антивірусна програма може намагатися видалити або знищити шкідливу програму з інфікованого пристрою.

− оновлення вірусних сигнатур: щоб бути ефективним, антивірусне програмне забезпечення повинно регулярно оновлювати свої вірусні сигнатури для виявлення нових загроз [16].

Вибір антивірусної програми – важливе рішення. Важливо визначити конкретні потреби користувача. Перша категорія антивірусних програм призначена для забезпечення базового захисту. До них відносяться безкоштовні антивірусні програми, такі як Avast Free Antivirus або AVG AntiVirus Free, які пропонують захист від вірусів, програм-вимагачів та інших поширених онлайн-загроз [17] . Антивірусне програмне забезпечення преміум-класу, таке як McAfee Total Protection або Trend Micro Maximum Security, пропонує найвищий рівень захисту, включаючи захист особистих даних і розширений батьківський контроль [18].

Бажано прочитати огляди різних антивірусних програм, які можна знайти в незалежних тестах і відгуках користувачів. Це дозволить користувачеві порівняти різні антивірусні програми і вибрати ту, яка найкраще відповідає його потребам. Важливо з'ясувати, чи сумісний антивірус з відповідною операційною системою. Не всі антивірусні програми сумісні з усіма операційними системами. Тому бажано звернутися до вебсайту розробника антивірусу, щоб переконатися, чи сумісна програма з потрібною операційною системою та завантажувати антивірусне програмне забезпечення з офіційного сайту, щоб уникнути можливості завантаження шкідливого програмного забезпечення.

Після встановлення антивірусного програмного забезпечення бажано оновити антивірусні бази. Вкрай важливо переконатися, що антивірусне програмне забезпечення, яке ви використовуєте, має нові бази визначення вірусів, оскільки це забезпечить оптимальний рівень захисту.

Рекомендується увімкнути функцію автоматичного сканування. Бажано налаштувати антивірусне програмне забезпечення на регулярне автоматичне сканування комп'ютера з метою виявлення та видалення будь-яких вірусів або іншого шкідливого програмного забезпечення. Також необхідно увімкнути захист у режимі реального часу. Захист у реальному часі служить для запобігання зараженню комп'ютерів вірусами та іншими шкідливими програмами.

Рекомендується запланувати резервне копіювання файлів. Бажано регулярно створювати резервні копії важливих файлів, щоб полегшити відновлення даних у разі зараження вірусом.

Крім того, рекомендується проявляти обережність при відкритті електронних листів і завантаженні файлів з невідомих джерел, регулярно оновлювати операційну систему, антивірусне та інше програмне забезпечення.

3.2 Фаєрволи та їх роль у захисті мережі

Фаєрвол (firewall) - це система захисту мережі, яка контролює трафік мережі, фільтрує його та блокує небажаний доступ до комп'ютера або мережі. Основні ролі

фаєрволів у захисті мережі:

1. Фільтрація трафіку: Фаєрволі можуть фільтрувати трафік на основі різних критеріїв, таких як IP-адреса, порти, протоколи тощо. Це дозволяє блокувати небажаний або потенційно небезпечний трафік.

2. Захист від вторгнень: Фаєрволи можуть виявляти та блокувати спроби несанкціонованого доступу до мережі, включаючи атаки відмови в обслуговуванні (DoS) та вторгнення.

3. Доступ до мережних ресурсів: Фаєрволи можуть контролювати доступ до мережних ресурсів, встановлюючи правила доступу для користувачів та пристроїв.

4. Захист від шкідливих програм: Фаєрволи можуть виявляти та блокувати небажану активність, таку як спроби виконання шкідливого програмного забезпечення або передача вірусів через мережу [19].

Фаєрволи також відіграють важливу роль у забезпеченні конфіденційності та захисту даних. Вони можуть запобігати витоку конфіденційної інформації, відслідковуючи та блокуючи підозрілу активність, яка може призвести до крадіжки даних. Це особливо важливо для організацій, що обробляють чутливу інформацію, таку як фінансові дані або особисті дані клієнтів.

Окрім цього, фаєрволи можуть надавати журнали подій та звіти про мережеву активність, що дозволяє адміністраторам мережі аналізувати трафік і виявляти потенційні загрози. Це допомагає у вчасному виявленні та реагуванні на інциденти безпеки, а також у вдосконаленні політик безпеки.

Фаєрволи можуть бути апаратними або програмними. Апаратні фаєрволи зазвичай розташовуються між внутрішньою мережею та інтернетом і забезпечують високий рівень захисту завдяки своїй спеціалізованій архітектурі. Програмні фаєрволи встановлюються на окремих комп’ютерах або серверах і забезпечують захист на рівні пристрою.

Крім того, сучасні фаєрволи часто використовують інтелектуальні технології, такі як машинне навчання та аналіз поведінки, для виявлення нових та невідомих загроз. Це дозволяє значно підвищити ефективність захисту та знизити ймовірність успішних атак.

Узагальнюючи, фаєрволи є критично важливим компонентом системи захисту мережі, забезпечуючи багаторівневий захист від різноманітних загроз та допомагаючи підтримувати безпеку та стабільність мережевої інфраструктури.

Фаєрволи можуть функціонувати на різних рівнях мережевої моделі OSI, що дозволяє їм забезпечувати гнучкий і ефективний захист. Розглянемо деякі технічні аспекти їх роботи.

На рівні мережі (мережевий рівень OSI) фаєрволи можуть здійснювати фільтрацію пакетів, перевіряючи заголовки IP-пакетів на відповідність встановленим правилам безпеки. Цей процес включає аналіз IP-адрес відправника і одержувача, портів, протоколів, а також інших метаданих. Фільтрація пакетів дозволяє блокувати або дозволяти трафік на основі попередньо визначених політик.

На транспортному рівні (транспортний рівень OSI) фаєрволи можуть контролювати з'єднання за допомогою технологій станового інспектування (stateful inspection). Це означає, що фаєрвол відслідковує стан кожного з'єднання і дозволяє трафік тільки для законних з'єднань, відстежуючи контекст з'єднань TCP та UDP. Такий підхід забезпечує більш точний контроль трафіку порівняно з простим фільтруванням пакетів.

На рівні додатків (додатковий рівень OSI) фаєрволи можуть виконувати глибокий аналіз вмісту пакетів за допомогою технології глибокого аналізу пакетів (Deep Packet Inspection, DPI). DPI дозволяє фаєрволам аналізувати не тільки заголовки пакетів, але й самі дані, що передаються. Це дозволяє виявляти і блокувати шкідливі програми, спроби експлуатації вразливостей додатків та інші загрози, що приховані в легітимному на перший погляд трафіку.

Фаєрволи можуть також підтримувати технології віртуальних приватних мереж (VPN), забезпечуючи безпечне з'єднання між віддаленими користувачами та внутрішньою мережею організації. Використання VPN дозволяє шифрувати трафік, захищаючи дані від перехоплення та несанкціонованого доступу.

Додатково, сучасні фаєрволи часто інтегровані з іншими засобами захисту, такими як системи виявлення та запобігання вторгнень (IDS/IPS), антивірусне

програмне забезпечення, системи управління інформаційною безпекою (SIEM) та інші. Це дозволяє створити комплексну систему захисту, яка може ефективно реагувати на широке коло загроз і забезпечувати надійний захист мережевих ресурсів.

Технічні параметри фаєрволів, такі як пропускна здатність, затримка, максимальна кількість одночасних з'єднань, об'єм журналів та інші, можуть суттєво впливати на їх продуктивність і ефективність. Тому вибір фаєрвола повинен здійснюватися з урахуванням специфічних потреб і вимог організації, а також з оцінкою можливостей інтеграції з існуючою інфраструктурою.

3.3 Заходи захисту від шкідливих програм

Додаткові заходи захисту від шкідливих програм включають:

− оновлення програмного забезпечення: регулярне оновлення операційних систем, антивірусного та іншого програмного забезпечення допомагає уникнути використання вразливостей для вторгнень;

− обмеження прав доступу: встановлення обмежень на права доступу користувачів до файлів, папок та інших ресурсів допомагає уникнути неправомірного доступу до даних;

− освіта користувачів: навчання користувачів про загрози безпеки та методи їх уникнення, такі як натискання на шкідливі посилання або відкриття вірусних вкладень в електронних листах;

− регулярні резервні копії: регулярне створення резервних копій важливих даних допомагає відновити інформацію в разі атаки або втрати даних через інші причини;

− використання антивірусного програмного забезпечення та фаєрволів для захисту від шкідливих програм і несанкціонованого доступу;

− використання багатофакторної автентифікації (mfa): впровадження багатофакторної автентифікації для доступу до систем і ресурсів підвищує рівень безпеки, знижуючи ризик несанкціонованого доступу;

− моніторинг та аналіз мережевого трафіку: постійний моніторинг та аналіз мережевого трафіку допомагає виявляти підозрілі дії та можливі атаки на ранніх стадіях;

− інцидент-менеджмент: впровадження процедур для швидкого реагування на інциденти, що включають виявлення, ізоляцію, ліквідацію та аналіз кіберінцидентів.

Додаткові заходи захисту від шкідливих програм включають кілька ключових аспектів. Регулярне оновлення програмного забезпечення є однією з основних стратегій, оскільки своєчасне оновлення операційних систем, антивірусного та іншого програмного забезпечення допомагає уникнути використання вразливостей для вторгнень. Обмеження прав доступу також грає важливу роль: встановлення обмежень на права доступу користувачів до файлів, папок та інших ресурсів допомагає уникнути неправомірного доступу до даних.

Освіта користувачів є ще одним важливим аспектом. Навчання користувачів про загрози безпеки та методи їх уникнення, такі як натискання на шкідливі посилання або відкриття вірусних вкладень в електронних листах, допомагає зменшити ризики. Регулярні резервні копії забезпечують надійний спосіб відновлення інформації в разі атаки або втрати даних через інші причини.

Використання антивірусного програмного забезпечення та фаєрволів забезпечує ефективний захист від шкідливих програм і несанкціонованого доступу. Додатково, впровадження багатофакторної автентифікації (MFA) для доступу до систем і ресурсів підвищує рівень безпеки, знижуючи ризик несанкціонованого доступу. Постійний моніторинг та аналіз мережевого трафіку допомагає виявляти підозрілі дії та можливі атаки на ранніх стадіях.

Нарешті, впровадження процедур інцидент-менеджменту для швидкого реагування на інциденти, включаючи виявлення, ізоляцію, ліквідацію та аналіз кіберінцидентів, є необхідним для ефективного управління безпекою та допомагають підтримувати безпеку комп’ютерів та мереж.

3.4 Програмна реалізація засобів перевірки комп’ютеру

Розглянемо три приклади коду, які демонструють різні підходи до перевірки та забезпечення безпеки комп’ютерних систем, які включають в себе використання бібліотеки hashlib у Python для сканування файлів на наявність шкідливого ПЗ, скрипт Bash для налаштування брандмауера за допомогою iptables, а також застосування алгоритму шифрування AES у C#. Кожен з цих методів має свої особливості та переваги, і їх комбіноване використання може значно підвищити рівень захисту вашої системи.

Перший приклад, написаний на Python, використовує бібліотеку hashlib для сканування вказаного каталогу на наявність шкідливих файлів. Алгоритм хешування MD5 використовується для обчислення хешів файлів і порівняння їх з відомими хешами шкідливих файлів. Цей метод дозволяє оперативно виявляти та видаляти потенційно небезпечні файли, підвищуючи загальний рівень безпеки системи. Рекомендується використовувати цей метод для регулярного моніторингу файлів у критичних каталогах.

Другий приклад демонструє використання скрипта Bash для налаштування правил брандмауера за допомогою iptables – утиліти командного рядку, стандартного інтерфейсу керування роботою міжмережевого екрана (брандмауеру) Netfilter. Скрипт встановлює політику відкидання для вхідних і переадресованих з'єднань за замовчуванням, дозволяє з’єднання через loopback інтерфейс, а також вхідні з’єднання для вже встановлених сесій і SSH. Використання цього скрипта допомагає забезпечити базовий рівень захисту на серверах та робочих станціях, обмежуючи доступ лише до необхідних сервісів.

Третій приклад, написаний на C#, використовує бібліотеку System.Security.Cryptography для шифрування та розшифрування тексту за допомогою алгоритму AES. Цей метод забезпечує високий рівень безпеки для конфіденційних даних, які потрібно захистити при їх зберіганні або передачі. Рекомендується використовувати цей метод для забезпечення конфіденційності та цілісності важливих даних.

Кожен з цих методів може бути використаний як окремо, так і в комбінації, залежно від ваших потреб і рівня загроз. Використання цих підходів допоможе значно підвищити загальний рівень безпеки вашої системи, захищаючи її від потенційних загроз та несанкціонованого доступу.

1. Hashlib

Представлений нижче код призначений для сканування вказаного каталогу на наявність шкідливих файлів. Він використовує алгоритм хешування MD5 для обчислення хешів файлів і порівняння їх з відомими хешами шкідливих файлів. Якщо знайдено файл з відповідним хешем, система виводить попередження про виявлення шкідливого файлу. Це допомагає виявляти та видаляти потенційно небезпечні файли, підвищуючи загальний рівень безпеки вашої системи.

```
import os
import hashlib

# Шлях до каталогу, який потрібно перевірити
directory = "/path/to/directory"

# Відомі хеші шкідливих файлів
known_hashes = [
    "5d41402abc4b2a76b9719d911017c592",
    "7d793037a0760186574b0282f2f435e7",
    # Додайте більше відомих хешів
]

def calculate_md5(file_path):
    hash_md5 = hashlib.md5()
    with open(file_path, "rb") as f:
        for chunk in iter(lambda: f.read(4096), b""):
            hash_md5.update(chunk)
    return hash_md5.hexdigest()

def scan_directory(directory):
    for root, dirs, files in os.walk(directory):
        for file in files:
            file_path = os.path.join(root, file)
            file_hash = calculate_md5(file_path)
            if file_hash in known_hashes:
                print(f"Warning: Malicious file detected:
{file_path}")
```

```
# Сканування каталогу
scan_directory(directory)
```

Цей код ефективно допомагає виявити шкідливі файли у вказаному каталозі, використовуючи порівняння хешів.

2. Bash

Скрипт Bash використовує iptables для налаштування правил брандмауера на системі. Він встановлює політику відкидання вхідних та переадресованих з'єднань за замовчуванням, дозволяє з'єднання через loopback інтерфейс, дозволяє вхідні з'єднання для вже встановлених сесій та SSH (на порті 22), і зберігає налаштування брандмауера для подальшого використання.

```
    #!/bin/bash ю

    # Встановлення політики за замовчуванням
    iptables -P INPUT DROP
    iptables -P FORWARD DROP
    iptables -P OUTPUT ACCEPT

    # Дозволити loopback інтерфейс
    iptables -A INPUT -i lo -j ACCEPT

    # Дозволити вхідні з'єднання для вже встановлених
сесій
    iptables -A INPUT -m state --state ESTABLISHED,RELATED
-j ACCEPT

    # Дозволити вхідні SSH-з'єднання
    iptables -A INPUT -p tcp --dport 22 -j ACCEPT


    # Зберегти налаштування
    service iptables save
```

3. C# та бібліотека Cryptography

Цей код на C# використовує бібліотеку System.Security.Cryptography для шифрування та розшифрування тексту за допомогою алгоритму шифрування AES (Advanced Encryption Standard).

В основній функції Main() спочатку створюється об’єкт AES, після чого викликаються методи шифрування EncryptStringToBytes_Aes та розшифрування DecryptStringFromBytes_Aes. Текст "This is some data to encrypt!" спершу шифрується, а потім розшифровується, і обидва варіанти виводяться на консоль для порівняння.

Метод EncryptStringToBytes_Aes приймає вхідний текст, ключ і вектор ініціалізації (IV). Він створює об’єкт AES з вказаними ключем і IV, створює шифрувальний об’єкт, і використовує його для шифрування вхідного тексту.

Метод DecryptStringFromBytes_Aes приймає шифрований текст, ключ і IV. Він створює об’єкт AES, створює розшифрувальний об’єкт і використовує його для розшифрування шифрованого тексту назад у вихідний.

Цей код демонструє простий приклад використання алгоритму AES для шифрування та розшифрування тексту в мові програмування C#.

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

class Program
{
    static void Main()
    {
        string original = "This is some data to encrypt!";
        using (Aes myAes = Aes.Create())
        {
            byte[] encrypted =
EncryptStringToBytes_Aes(original, myAes.Key, myAes.IV);
            string roundtrip =
DecryptStringFromBytes_Aes(encrypted, myAes.Key, myAes.IV);

            Console.WriteLine("Original: {0}", original);
            Console.WriteLine("Round Trip: {0}",
roundtrip);
        }
    }
```

```
    static byte[] EncryptStringToBytes_Aes(string
plainText, byte[] Key, byte[] IV)
    {
        if (plainText == null || plainText.Length <= 0)
            throw new ArgumentNullException("plainText");
        if (Key == null || Key.Length <= 0)
            throw new ArgumentNullException("Key");
        if (IV == null || IV.Length <= 0)
            throw new ArgumentNullException("IV");
        byte[] encrypted;

        using (Aes aesAlg = Aes.Create())
        {
            aesAlg.Key = Key;
            aesAlg.IV = IV;

            ICryptoTransform encryptor =
aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);

            using (MemoryStream msEncrypt = new
MemoryStream())
            {
                using (CryptoStream csEncrypt = new
CryptoStream(msEncrypt, encryptor, CryptoStreamMode.Write))
                {
                    using (StreamWriter swEncrypt = new
StreamWriter(csEncrypt))
                    {
                        swEncrypt.Write(plainText);
                    }
                    encrypted = msEncrypt.ToArray();
                }
            }
        }

        return encrypted;
    }

    static string DecryptStringFromBytes_Aes(byte[]
cipherText, byte[] Key, byte[] IV)
    {
        if (cipherText == null || cipherText.Length <= 0)
            throw new ArgumentNullException("cipherText");
        if (Key == null || Key.Length <= 0)
            throw new ArgumentNullException("Key");
```

```
        if (IV == null || IV.Length <= 0)
            throw new ArgumentNullException("IV");

        string plaintext = null;

        using (Aes aesAlg = Aes.Create())
        {
            aesAlg.Key = Key;
            aesAlg.IV = IV;

            ICryptoTransform decryptor =
aesAlg.CreateDecryptor(aesAlg.Key, aesAlg.IV);

            using (MemoryStream msDecrypt = new
MemoryStream(cipherText))
            {
                using (CryptoStream csDecrypt = new
CryptoStream(msDecrypt, decryptor, CryptoStreamMode.Read))
                {
                    using (StreamReader srDecrypt = new
StreamReader(csDecrypt))
                    {
                        plaintext = srDecrypt.ReadToEnd();
                    }
                }
            }
        }

        return plaintext;
    }
}
```

Отже, у цьому розділі було розглянуто три різні підходи до перевірки та забезпечення безпеки комп’ютерних систем. Перший передбачає використання Python і бібліотеки hashlib для сканування каталогу на наявність шкідливих файлів за допомогою хешування MD5. Другий підхід реалізовано за допомогою скрипта Bash, який налаштовує правила брандмауера за допомогою iptables, забезпечуючи захист від небажаних вхідних з’єднань. Третій підхід використовує мову програмування C# та бібліотеку System.Security.Cryptography для шифрування і розшифрування даних з використанням алгоритму AES (Advanced Encryption Standard).

Всі ці методи сприяють підвищенню загального рівня безпеки системи, захищаючи її від потенційних загроз та несанкціонованого доступу. Використання хешування для виявлення шкідливих файлів, налаштування брандмауера для контролю вхідних з’єднань та шифрування даних для захисту конфіденційної інформації – це ефективні засоби для забезпечення комп’ютерної безпеки.

ВИСНОВКИ

У сучасному цифровому світі, де технології все більше проникають у різні аспекти нашого життя, кібербезпека стає критично важливою. Основні загрози, такі як віруси, троянські програми, фішинг, DDoS атаки та інші, негативно впливають на безпеку користувачів та організацій. Розуміння цих загроз, а також використання ефективних методів захисту, є ключем до успішного збереження конфіденційності, цілісності та доступності інформації.

Антивірусні програми, файерволи та заходи захисту від шкідливих програм є основними компонентами захисту інформації. Вони забезпечують виявлення, блокування та видалення шкідливих програм, контролюють трафік мережі та захищають від вторгнень, а також допомагають уникнути використання вразливостей та небажаних активностей.

Криптографічні методи грають важливу роль у захисті інформації, забезпечуючи конфіденційність та цілісність даних під час їх передачі та зберігання. Аутентифікація та авторизація користувачів дозволяють контролювати доступ до систем та ресурсів, уникнути несанкціонованого використання інформації та забезпечити безпеку систем.

Використання відповідного програмного забезпечення для захисту інформації, такого як антивірусні програми та файерволи, разом із регулярним оновленням програм та навчанням персоналу щодо безпеки даних, є важливими складовими кібербезпеки. Застосування комплексного підходу до захисту інформації допоможе зменшити ризики кібератак та зберегти конфіденційність та цілісність даних.

Важливо пам’ятати, що жоден захисний захід не є повністю недоліком. Тому важливо використовувати комплексний підхід до захисту інформації, включаючи регулярне оновлення програмного забезпечення, обмеження прав доступу користувачів, освіту та навчання персоналу та регулярне створення резервних копій даних.

Загалом, ефективний захист інформації вимагає постійного моніторингу та вдосконалення стратегій та заходів захисту. Це важливо як для індивідуальних користувачів, так і для підприємств, щоб уникнути потенційних наслідків кіберзагроз та зберегти конфіденційність, цілісність та доступність їхніх даних.

Ретельне розуміння сучасних загроз, використання ефективних методів захисту та впровадження відповідних заходів безпеки дозволять забезпечити надійний рівень кібербезпеки в цифровому просторі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Старик-Блудова А. Ю., Станіна О. Д.Кіберзлочинність та шляхи боротьби з нею. Інформаційні технології в освіті та практиці : матеріали Всеукр. наук.-практ. конф. 18 грудня 2020 Львів, упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2020. С. 100-101.
2. Таран О. В., Гавловський В. Д.Організована кіберзлочинність в україні: проблеми формування офіційної статистики та її аналізу. *Інформація і право*, 2021. № 4(39). С. 193-201.
3. Кізима І. В. Кібертероризм як глобальна проблема людства. Сучасні тенденції розвитку науки та освіти : матеріали Всеукраїньскої науково-практичної інтернет-конференції педагог. та наук.-педагог. працівників, аспірантів, молодих учених. ВСП, 2021. С. 392-397.
4. Нашинець-Наумова А. Ю. Кіберзлочинність. Нова кримінальна загроза. Наукові розвідки з актуальних проблем публічного та приватного права: матеріали IV Всеукраїнської науково-практичної конференції 24 квітня 2021 р. Київ : Київський університет імені Бориса Грінченка, 2021. С. 111-114.
5. Лисенко С. М., Омельяненко В. Ю., Щука Р. В. Метод ідентифікації шпигунського програмного забезпечення в комп’ютерних системах. Технічні науки. *Вісник Хмельницького національного університету*, 2020. №3 (285). С. 43-49.
6. Грищук А. Б., Хімко Я. П. Класифікація шідливого програмного забезпечення. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції 22 грудня 2023, Львів. ЛьвДУВС, 2024С. 45-47.
7. Гавва С. К., Головко С. Г. Сучасний кібертероризм як загроза національній безпеці. Свобода, безпека та незалежність: правовий вимір : матеріали XIII Міжнародної науково-практичної конференції, Київ, 24 лютого 2023 р. Київ, Національний авіаційний університет, 2023. С. 54-56

8. Котляров В. Кібертероризм як загроза міжнародній безпеці. Наукові праці Міжрегіональної Академії управління персоналом. *Політичні науки та публічне управління*, 2023. №5(71). С. 46-54.
9. Погоріла К., Лєсная Ю., Богданова Є., Малахов С. Соціальний інжиніринг, як фактор реалізації інсайдерських загроз. *Scientific Collection «InterConf»*, 2022. (50), 494–501.
10. Інформаційна безпека та інформаційні технології: збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів, ЛДУ БЖД, 2023, 489 с.
11. Пучок М. С., Тищенко Д. О. Особливості криптографічного захисту інформації в електронному документообігу. Модернізація економіки: сучасні реалії, прогнозні сценарії та перспективи розвитку: матеріали V Міжнародної науково-практичної конференції 27-28 квітня 2023 р., м. Херсон. Хмельницький, 2023. С. 125-127.
12. Довганик С. С. Захист від фішингових атак за допомогою електронного цифрового підпису. Technical sciences, 2022. С.122-123.
13. Луговський П.В. Розробка та налаштування захищеного корпоративного поштового сервера. Тернопіль : ТНТУ, 2023. – 74 с.
14. Єрмоленко А. В. Кібербезпека інформаційно телекомунікаційних систем. Шифрування та дешифрування методом підстановки. І. В. Піскачова; Харків, 2023. 68 с.
15. Костюк К. О. Дослідження криптографічних протоколів захисту інформації в мережі Інтернет. Тернопіль: ТНТУ, 2023. 63 с.
16. Стадник Б. С., Ніколюк П. К. Сучасні антивірусні програми. Прикладні інформаційні технології, 2023. С. 72-75.
17. Avast Antivirus. URL: https://www.avast.ua/ru-ua/free-antivirus-download#pc
18. McAfee Total Protection. URL: https://www.mcafee.com/en-us/antivirus/mcafee-total-protection.html
19. Нагорний О. В. Проблеми захисту інформації в комп’ютерних системах та засоби і методи їх вирішення. Modern research in science and education :

матеріали II Міжнар. наук.-практ. конф., Чикаго, 12-14 жовтня 2023 року. США, 2023. С. 171-180.

20. Брандмауэр (Firewall) Comodo . URL: https://www.comodo.com/?af=7639
21. Поляков О. М. Сучасні тренди виявлення та протидії застосуванню шпигунських та шкідливих програм. Інформаційна і національна безпека. Інформація і право, 2023. № 2(45). С. 125-136.