ТЕХНОЛОГІЇ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Лунгол Ольга Миколаївна,
к. пед. н., доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ
Агішева Анна Володимирівна,
викладач інформатики Кропивницького вищого професійного училища

Анотація: Технології створення та застосування систем захисту інформаційно-комунікаційних систем є важливою сферою, що вивчається та розвивається в контексті сучасних викликів цифрового світу. Ця область охоплює різноманітні техніки та методики, спрямовані на забезпечення безпеки інформації в комп'ютерних системах і комунікаційних мережах. Основні аспекти теми включають шифрування даних, аутентифікацію та авторизацію, виявлення та захист від загроз, фізичну безпеку, захист мереж від несанкціонованого доступу та атак, створення політики безпеки в організаціях, захист від соціально-інженерних атак, аналіз загроз і ризиків, захист від витоку даних тощо. Технології в області захисту інформаційно-комунікаційних систем є важливим компонентом в сучасному цифровому світі, де зростає кількість загроз і ризиків для інформації та приватності. Вивчення та розвиток цих технологій є важливим завданням для забезпечення безпеки в інформаційному суспільстві.

Ключові слова: загрози, безпека, захист, шифрування, інформаційно-комунікаційні системи.

Технології створення та застосування систем захисту інформаційно-комунікаційних систем є важливою складовою сучасного світу, де інформація є надзвичайно цінним активом. Ці технології спрямовані на

забезпечення конфіденційності, цілісності та доступності інформації у мережі та комп'ютерних системах. Вони стали невід'ємною частиною багатьох сфер, включаючи корпоративний сектор, урядові органи, освіту, організації громадянського суспільства та правоохоронні структури.

Роботи багатьох сучасних науковців направлені на вивчення та вдосконалення систем захисту інформаційно-комунікаційних систем [1 – 4]. Проаналізувавши відповідіні дослідження, ми виділили основні аспекти технологій створення та застосування систем захисту інформаційно-комунікаційних систем, такі як шифрування даних, аутентифікацію та авторизацію, виявлення та захист від загроз, фізичну безпеку тощо. Розглянемо більш детально кожен із них.

Шифрування інформації являє собою процес перетворення звичайного тексту, відомого як «відкритий текст» у нечитабельний формат за допомогою спеціального алгоритму, відомого як «ключ». Цей процес використовується для захисту конфіденційності даних та перешкоджання несанкціонованому доступу до них. Шифрування вимагає наявності ключа, який є секретним параметром, що використовується для шифрування та розшифрування даних. Ключ визначає, як саме інформація буде перетворена. Існують різні алгоритми шифрування, такі як симетричне шифрування (де один і той же ключ використовується для шифрування та розшифрування) та асиметричне шифрування (де ключі для шифрування та розшифрування відрізняються). Від вибору алгоритму залежить рівень безпеки. Шифрування забезпечує конфіденційність даних, оскільки без ключа неможливо прочитати шифрований текст. Це особливо важливо для захисту особистої та конфіденційної інформації, такої як фінансові дані або медичні записи. Шифрування також допомагає забезпечити цілісність даних. Якщо дані були змінені під час передачі або зберігання, то їх розшифрування буде неможливим, і користувач отримає сигнал, що дані були пошкоджені.

Шифрування може також включати аутентифікацію, тобто перевірку ідентичності користувача чи джерела даних. У мережевому оточенні

шифрування дозволяє захистити дані, що передаються через Інтернет або локальну мережу від несанкціонованого доступу.

Шифрування широко використовується в різних аспектах сучасних технологій, включаючи електронну пошту, месенджери, онлайн-банкінг, бездротові мережі та багато інших аспектів цифрового життя. Шифрування інформації відіграє ключову роль у забезпеченні безпеки в цифровому світі та захисту конфіденційності й цілісності даних. Використання шифрувальних алгоритмів та правильного управління ключами є важливою складовою захисту інформації в сучасному світі.

Серед технологій створення та застосування систем захисту інформаційно-комунікаційних систем також виділяють багаторівневий захист або багаторівневу безпеку – це концепція та практика забезпечення безпеки, яка використовує декілька рівнів заходів та захисних механізмів для захисту системи чи інформації від різних загроз та атак. Ця стратегія базується на ідеї, що жоден окремий рівень захисту не може забезпечити повноцінну безпеку, тому використовуються комбіновані заходи на різних рівнях. Фізичний рівень багаторівневого захисту забезпечує захист фізичного доступу до системи. Він включає в себе заходи, які контролюють фізичний доступ до серверних кімнат, дата-центрів та інших об’єктів. Це може бути біометрична ідентифікація, картковий доступ, камери відеоспостереження тощо. Мережевий рівень багаторівневого захисту включає в себе використання брандмауерів, VPN-з’єднань, інтрузійні системи виявлення та інші засоби для моніторингу та захисту мережі від несанкціонованого доступу та атак. Системний рівень багаторівневого захисту включає в себе регулярне оновлення системи, встановлення антивірусного програмного забезпечення, застосування політик безпеки та обмеження доступу до ресурсів. Додатковий рівень захисту включає в себе додаткові заходи, такі як двофакторна аутентифікація, шифрування даних, контроль доступу на рівні користувача та інші методи для забезпечення безпеки даних та доступу. Особлива увага приділяється захисту даних на різних рівнях. Це може включати в себе регулярні резервні копії, шифрування даних в

спокійному та транзитному стані, аудит доступу до даних та інші методи захисту конфіденційності та цілісності інформації. Багаторівневий захист також враховує аспекти соціальної інженерії та освіту користувачів. Інструктажі, навчання щодо безпеки та усвідомлення загроз допомагають запобігти атакам, які можуть виникнути через психологічні маніпулювання. Важливою складовою багаторівневого захисту є постійний моніторинг систем та реагування на потенційні загрози. Це може включати в себе виявлення несправностей, аналіз журналів подій та автоматизовані системи реагування на атаки.

Багаторівневий захист є важливим аспектом для забезпечення безпеки в інформаційній та кібернетичній сферах. Використання комбінації різних заходів на різних рівнях допомагає ефективно захищати системи та дані від різноманітних загроз та атак.

Аутентифікація і авторизація в системах захисту інформаційно комунікаційних систем являють собою важливі концепти в області кібербезпеки та захисту інформації, які допомагають визначити, хто має доступ до системи та які дії ці користувачі можуть виконувати.

Аутентифікацію трактують як процес перевірки ідентифікації користувача. Вона визначає, чи є користувач тим, за кого він себе видає, і чи має він право доступу до системи. Для аутентифікації можуть використовуватися різні методи, включаючи інформацію, яку користувач знає (наприклад, пароль), фізичні засоби (наприклад, смарт-карту або токен), або фізичну ідентифікація користувача (наприклад, біометричні дані, такі як відбиток пальця або розпізнавання обличчя).

Авторизація – це процес визначення повноважень користувача після того, як він успішно пройшов аутентифікацію. Авторизація визначає, які ресурси, функції чи дії користувач має право виконувати в системі. Авторизація базується на ролях або правах доступу, які призначені користувачеві після аутентифікації. Реалізація може здійснюватися через різні механізми контролю доступу, такі як списки допуску або правила, що обмежують доступ.

Авторизація гарантує, навіть якщо користувач аутентифікується успішно, він має обмежені права та доступ лише до тих ресурсів, до яких він має право. Разом аутентифікація та авторизація допомагають забезпечити безпеку інформації та ресурсів в системі, регулюючи доступ користувачів та визначаючи їх права.

Для забезпечення стабільності і захищеності програмного забезпечення та операційних систем важливого значення набувають оновлення та патчі безпеки. Оновлення – це нові версії програмного забезпечення, які випускаються розробниками для виправлення помилок, поліпшення функціональності та внесення інших змін у програмному продукті. Вони можуть включати оновлення, які не стосуються безпеки, такі як нові функції або зміни інтерфейсу.

Оновлення допомагають забезпечити коректну роботу програм та операційних систем, а також підтримують їхню актуальність та сумісність з іншими компонентами.

Патчі безпеки – це спеціальні оновлення, які видаються для закриття вразливостей у програмному забезпеченні та запобігання зловживанню ними. Патчі безпеки є надзвичайно важливими для запобігання атак на систему та збереження конфіденційності, цілісності та доступності даних. Вони захищають від ризику використання вразливостей для атак та злому безпеки.

Оновлення та патчі спершу тестуються в ізольованих середовищах, щоб переконатися, що вони не спричиняють непередбачуваного збою. Після успішного тестування оновлення та патчі безпеки встановлюються робочих системах. Після встановлення важливо моніторити стан системи та робити регулярні резервні копії для захисту. Багато організацій використовують автоматичні системи управління оновленнями та патчами безпеки для спрощення процесу їх обслуговування. Всі оновлення та патчі безпеки важливо вчасно встановлювати, оскільки вони забезпечують якісну роботу програмного забезпечення й операційних систем.

Важливим аспектом систем захисту інформаційно-комунікаційних систем

є фізичний захист серверних кімнат та дата-центрів від несанкціонованого доступу. Велика кількість витоків даних стається через недбалість або навмисні дії самих співробітників. Важливо навчити персонал правилам безпеки та контролювати їх доступ до даних.

Зазначені технології в області захисту інформаційно-комунікаційних систем є важливим аспектом сучасної цифрової безпеки. Ці технології спрямовані на захист конфіденційності, цілісності та доступності інформації, що зберігається в інформаційних системах. Технології створення та застосування систем захисту інформаційно-комунікаційних систем постійно розвиваються, оскільки загрози для інформаційної безпеки трансформуються та вдосконалюються. Важливо як для організацій, так і для окремих користувачів, вдосконалювати захисні стратегії та використовувати найновіші технології для захисту інформації.

ЛІТЕРАТУРА

1. Габорець О., Лунгол О. Personal data protection issues in the context of modern communication. Штучний інтелект та інтелектуальні системи : II Міжнар. наук.-техн. конф. (м. Київ, 8-9 грудня 2022 р.). Київ, 2022. С. 54–56.
2. Lunhol O., Haborets O. Information security as an integral part of today. Здоров’я і суспільство в умовах війни: Збірник наук. статей. (м. Кропивницький, 18 листопада 2022 р.). Кропивницький : ЦІРоЛ, 2022. С. 389–392.
3. Шаєц Є. Використання ханіпотів для виявлення мережевих атак. Інформаційна безпека та інформаційні технології : IV Міжнар. наук.-практ. конф. (м. Львів, 30 листопада 2022 р.). Львів : Растр-7, 2022. С. 93–95.
4. Lysenko O.V., Haborets O.A., Lunhol O.M. Law enforcement information and analytical support. Current issues in modern science. Issue № 3(9) 2023. Pp. 281–291.