УДК 004.056

АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Плєхова Г. А., доцент, канд. техн. наук, доцент кафедри інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет,
Костікова М. В., доцент, канд. техн. наук, доцент кафедри інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет

Анотація. Досліджені проблеми інформаційної безпеки та захисту інформаційних систем від навмисного чи випадкового втручання. Висвітлюються актуальні проблеми розвитку системи інформаційної безпеки. Інформаційна безпека має першорядне значення у зв'язку із значним поширенням атак, яким постійно піддаються як окремі мережі підприємств, так і національні мережі в цілому.

Ключові слова: інформаційні системи, інформаційна безпека, небезпека, Lorenz, захист інформації.

Широке поширення обчислювальної техніки як засобу обробки інформації призвело до інформатизації суспільства та появі принципово нових, інформаційних технологій. Поява будь-яких нових технологій зазвичай має як негативні, так і позитивні сторони. Тому багато прикладів. Атомні та хімічні технології, вирішуючи проблеми енергетики та виробництва нових матеріалів, породили екологічні проблеми. Інтенсивний розвиток транспорту забезпечує зручну і швидку доставку людей, матеріалів, сировини і товарів у необхідних напрямах, а й матеріальні збитки і жертви при транспортних катастрофах зросли. Інформаційні технології також не є винятком з цього правила, і тому слід завчасно подбати про безпеку при використанні та розробці таких технологій.

Від ступеня безпеки інформаційних технологій сьогодні залежить добробут, а часом життя багатьох людей. Така плата за ускладнення та поширення автоматизованих систем обробки інформації.

Інформаційні технології все більш наполегливо проникають в усі сфери людської діяльності. У сучасному суспільстві важливою проблемою є захист інформації, яка перетворилася на ринку в предмет купівлі-продажу. У зв'язку з цим зараз широко обговорюється інформаційна безпека. Завдання кожної організації створити таку систему захисту, яка була б стійка до втручання сторонніх осіб. Це передбачає безпеку мереж та всієї інфраструктури, захист програмного забезпечення та баз даних, регулярний аудит інформаційних систем. На цю тему видано чимало наукових статей та методичних посібників.

Так у підручнику [1] розглянуті концептуальні засади інформаційної безпеки, національні інтереси в інформаційній сфері, стратегія розвитку та формування єдиного інформаційного простору України, загрози безпеці держави та її громадянам в інформаційній сфері, технології інформаційно-психологічного та інформаційного впливу й захисту від цих впливів, система забезпечення інформаційної безпеки України, особливості функціонування та функції її суб'єктів.

Проблема інформаційної безпеки має давнє походження і стала особливо значущою у наш час, коли використання інформаційно-телекомунікаційних технологій відбувається вже практично у всіх житті суспільства. Розгляду питань інформаційної безпеки приділяють величезну увагу як вітчизняні, так і закордонні дослідники.

Доктор Вільям Столінгс зробив унікальний внесок у розуміння широкого спектру технічних розробок у галузі комп'ютерної безпеки, комп'ютерних мереж та

комп'ютерної архітектури. У [2] пропонується вичерпне та уніфіковане пояснення кращих практик та стандартів, які є перевіреними та узгодженими методами реалізації кібербезпеки.

Перед розгортанням нових технологій у виробничому середовищі необхідно розглянути їх аспекти безпеки. Програмно-визначені мережі (*SDN*) та віртуалізація мережевих функцій (*NFV*) – це дві нові технології, які використовуються, наприклад, для підвищення керованості, безпеки та гнучкості корпоративних/виробничих/хмарних *IT*-середовищ. У [3] представлений аналіз безпеки кількох програмно-визначуваних мереж (*SDN*) та додатків віртуалізації мережевих функцій (*NFV*) з використанням середовища моделювання загроз *Microsoft STRIDE*.

Проблема інформаційної безпеки в останні роки стала дуже актуальною і розглядається як одне із пріоритетних державних завдань.

Метою роботи є визначення напрямів удосконалення забезпечення інформаційної безпеки у взаємозв'язку з інформаційною діяльністю, з огляду на реальні й потенційні загрози, а також ключових інструментів її забезпечення.

Для досягнення поставленої мети необхідно визначити актуальні проблеми розвитку системи інформаційної безпеки.

Комп'ютерні мережі характерні тим, що проти них роблять так звані віддалені атаки. Порушник може перебувати за тисячі кілометрів від об'єкта, що атакується, при цьому нападу може зазнавати не тільки конкретний комп'ютер, але й інформація, що передається по мережевих каналах зв'язку.

Формування режиму інформаційної безпеки – комплексна проблема. Заходи щодо її вирішення можна поділити на п'ять рівнів:

1. Законодавчий (нормативні акти, закони, стандарти тощо).

2. Морально-етичний (різні стилі поведінки співробітників або цілої організації).

3. Адміністративний (дії загального характеру, що вживаються керівництвом організації).

4. Фізичний (електро та електронно-механічні, механічні перешкоди на можливих шляхах проникнення потенційних порушників).

5. Апаратно-програмний (система заходів спрямованих на безпеку організації та зменшення вірогідності та шкоди від загроз) має відповідати наступним принципам: захист тим ефективніший, чим простіше користувачеві з ним працювати; вартість засобів захисту має бути меншою, ніж розміри можливої шкоди; можливість відключення в екстрених випадках.

Фахівці, які працюють в сфері адміністратора з кібербезпеки повинні розуміти свої дії у разі атак на систему та алгоритм дій при відповідних атаках. Адміністратор захисту системи не повинен підлягати контролю системи. Тобто він не може бути серед тих, кого ця система контролюватиме. Система захисту має надавати докази коректності своєї роботи. Особи, які здійснюють інформаційну безпеку системи несуть особисту відповідальність.

При захисті об'єктів потрібно систему розділяти на групи. Таким чином ми можемо захистити частину системи при проникненні та порушенні захисту в якоїсь її частині.

Коли ми будуємо надійну систему з надійним захистом то вона має бути повністю протестована та узгоджена. Більш гнучким та ефективним захист стає, якщо він може мати параметри які допускають зміну параметрів при необхідності зі сторони менеджера з кібербезпеки. Крім того потрібно враховувати в системи захисту що при використанні системи користувачі будуть робить помилки при користуванням системою.

Таким чином найбільш критичні та важливі рішення мають прийматися людиною. Існування механізмів захисту має бути приховано від користувачів, робота яких перебуває під контролем.

Незважаючи на те, що сучасні ОС для персональних комп'ютерів, мають власні підсистеми захисту, актуальність створення додаткових засобів захисту зберігається. Справа в тому, що більшість систем не спроможні захистити дані, що перебувають за їх межами, наприклад, при мережевому інформаційному обміні.

Апаратно-програмні засоби захисту можна розбити на п'ять груп:

1. Системи ідентифікації (розпізнавання) та аутентифікації (перевірки справжності) користувачів.
2. Системи шифрування дискових даних.
3. Системи шифрування даних, що передаються мережами.
4. Системи аутентифікації електронних даних.
5. Управління криптографічними ключами.

Системи ідентифікації та аутентифікації користувачів – ці функції системи дозволяють обмежити доступ користувачів які випадково або незаконно питаються проникнути в комп'ютерну систему. Користувачам які мають доступ в систему, потрібно підтвердити його особистість, перевірити її справжність і потім надати чи не надати користувачеві можливість роботи з системою.

При побудові цих систем виникає проблема якості ідентифікації користувачів та вибору інформації для здійснення процедури ідентифікації та аутентифікації. Для цього формують такі типи: секретна інформація, яку має користувач (секретний ключ, пароль, персональний ідентифікатор тощо), користувач повинен запам'ятати цю інформацію або для неї можуть бути застосовані спеціальні засоби зберігання; фізіологічні параметри людини (малюнок райдужної оболонки ока, відбитки пальців тощо) або особливості поведінки (особливості роботи на клавіатурі тощо).

Системи, засновані на першому типі інформації, вважаються традиційними. Системи які використовують фізіологічні параметри людини – біометричні системи. Зараз є тенденція випереджаючого розвитку біометричних систем ідентифікації.

Системи шифрування дискових даних існують для того, щоб зробити інформацію марною для противника, використовується сукупність методів перетворення даних, звана криптографією (від грец. kryptos – прихований і grapho – пишу). Системи шифрування можуть здійснювати криптографічні перетворення даних тільки на рівні файлів або на рівні дисків. До програм першого типу можна віднести архіватори типу *RAR* та *ARJ*, які дозволяють використовувати криптографічні методи захисту архівних файлів. Прикладом систем другого типу може бути програма шифрування *Diskreet*, що входить до складу популярного програмного пакета *Norton Utilities, Best Crypt*. Крім того системи шифрування дискових даних можливо розпізнати за методом їх функціонування. За способом функціонування системи шифрування дискових даних ділять на два класи: системи «прозорого» шифрування; системи, що спеціально викликаються для здійснення шифрування на диск, що захищається, а система захисту в процесі запису виконує його шифрування [4]. Коли використовуються системи прозорого шифрування то в таких системах криптографічні перетворення йдуть в режимі реального часу. Користувач непомітно для себе перетворює інформацію в криптографічні шифри и таким чином здійснюється шифрування «на льоту». Наведемо приклад, користувач підготував документ в текстовому редакторі. Далі він записує документ на диск, що захищається, а система захисту в процесі запису виконує його шифрування. [4]

Системи другого класу зазвичай є утиліти. При шифруванні утиліти їх необхідно спеціально викликати для виконання шифрування. Архіватори є прикладом таких утиліт із вбудованими засобами парольного захисту.

Більшість систем, які пропонують встановити пароль на документ, не шифрують інформацію, а тільки забезпечують запит пароля при доступі до документа. До таких систем належить *MS Office*, 1С та багато інших.

Розрізняють два основні способи шифрування даних, що передаються мережами: канальне шифрування та кінцеве (абонентське) шифрування.

У разі канального шифрування захищається вся інформація, що передається каналом зв'язку, включаючи службову. Цей спосіб шифрування дозволяє (маючи вбудовану процедуру шифрування на канальному рівні) використовувати апаратні засоби що в свою чергу робить систему більш продуктивній [4]. Однак цей підхід має і суттєві недоліки:

- Шифрування службових даних ускладнює механізм маршрутизації мережевих пакетів та вимагає розшифрування даних у пристроях проміжної комунікації (ретранслятор, шлюзи и тощо).

- Шифрування службової інформації може призвести до появи статистичних закономірностей у шифрованих даних, що впливає на надійність захисту. Крім того вона накладає обмеження на використання криптографічних алгоритмів.

- Абонентське шифрування дозволяє зробити дані конфіденційними коли вони передаються між двома абонентами. І тут захищається лише зміст повідомлень, вся службова інформація залишається відкритою. Головним недоліком є можливість з можливість аналізувати інформацію об абонентах. Такої інформації може бути інформація про обсяг даних, що передаються, яку структуру мають повідомлення та інформацію об абонентах.

Системи аутентифікації електронних даних використовують при обміні даними мережами, тут виникає проблема автентифікації автора документа і самого документа, тобто. встановлення автентичності автора. Важливо також зробити та перевірити відсутність змін в отриманому документі. Здійснення автентифікації даних робиться з застосуванням коду автентифікації повідомлення (імітівставки) або електронного підпису.

Імітівставка виробляється з відкритих даних за допомогою секретного ключа. Це спеціальне шифрування з використанням до якого додається секретного ключа та передається каналом зв'язку в кінці зашифрованих даних. Імітівставка перевіряється одержувачем за допомогою секретного ключа шляхом повторення процедури, виконаної раніше відправником, над отриманими відкритими даними.

Електронний цифровий підпис є відносно невеликою кількістю додаткової аутентифікуючої інформації, що передається разом з текстом, що підписується. Відправник формує цифровий підпис, використовуючи секретний ключ відправника. Отримувач перевіряє підпис, використовуючи відкритий ключ відправника.

Таким чином, для реалізації імітівставки використовуються принципи симетричного шифрування, а для реалізації електронного підпису – асиметричного шифрування.

Засоби управління криптографічними ключами це безпека будь-якої криптосистеми визначається криптографічними ключами. У разі ненадійного керування ключами зловмисник може заволодіти ключами та отримати повний доступ до всієї інформації в системі чи мережі.

Розрізняють такі види функцій управління ключами: генерація, зберігання та розподіл ключів.

Способи генерації ключів для симетричних та асиметричних криптосистем різні. Розглянемо генерації ключів симетричних криптосистем. В таких системах використовуються апаратні та програмні засоби генерації випадкових чисел. Генерація ключів для асиметричних криптосистем більш складна, оскільки ключі повинні мати певні математичні властивості.

Функція зберігання передбачає організацію безпечного зберігання, обліку та видалення ключової інформації. Для забезпечення безпечного зберігання ключів застосовують їхнє шифрування за допомогою інших ключів. Такий підхід призводить до

концепції ієрархії ключів. У ієрархію ключів зазвичай входить головний (тобто майстер-ключ). Майстер-ключ використовують для шифрування ключів та як ключ шифрування даних. Генерація та зберігання майстер-ключа є критичним питанням криптозахисту. [5]

Розподіл - найвідповідальніший процес у керуванні ключами. Цей процес повинен гарантувати скритність ключів, що розподіляються, а також бути оперативним і точним. Між користувачами мережі ключі розподіляються двома способами: за допомогою прямого обміну сеансовими ключами; використовуючи один або кілька центрів розподілу ключів. [5]

Нова операція з викупу, відома як атакувальна система *Lorenz*, націлена на організації в усьому світі за допомогою індивідуальних атак, які вимагають сотні тисяч доларів викупу. Програма-вимагач *Lorenz* почала діяти у квітні 2021 року і з тих пір накопичила зростаючий список жертв, чиї вкрадені дані були опубліковані на сайті витоку даних. Шифратор *Lorenz* є таким же, як і попередня операція, відома як *ThunderCrypt*. Як і інші атаки програмного забезпечення, *Lorenz* порушує мережу та поширюється на інші пристрої, доки вони не отримують доступ до облікових даних адміністратора домену *Windows*. Поширюючись по всій системі, програма-вимагач збиратимуть не зашифровані файли із серверів жертв, які вони завантажують на віддалені сервери під їхнім контролем. Ці вкрадені дані потім публікуються на спеціальному сайті для витоку даних, щоб тиснути на жертв, щоб вони заплатили викуп або продали дані. На сайті витоку даних *Lorenz* перераховано дванадцять жертв, дані оприлюднені для десяти з них. Коли команда *Lorenz* публікує дані, вона робить трохи інакше, ніж інші групи. Щоб змусити жертв сплатити викуп, *Lorenz* спочатку надає дані для продажу іншим суб'єктам загроз або можливим конкурентам. Минає час, вони починають випускати захищені паролем *RAR*-архіви, що містять дані жертви. Зрештою, якщо викуп не сплачується, а дані не купуються, *Lorenz* випускає пароль для архівів витоку даних, щоб вони були загальнодоступними ля всіх, хто завантажує файли. Іншою цікавою характеристикою, якої немає на інших сайтах витоку даних, є те, що *Lorenz* продає доступ до внутрішньої мережі жертви разом з даними. Для деяких суб'єктів загроз доступ до мереж може бути більш цінним, ніж самі дані.

Зі зразків програм-вимагачів *Lorenz*, учасники загроз налаштовують виконуваний файл шкідливого програмного забезпечення для конкретної організації, на яку вони націлені.

В одному зі зразків, наданих *BleepingComputer*, програма-вимагач видасть такі команди, щоб запустити файл під назвою ScreenCon.exe з того, що, здається, є контролером домену локальної мережі.

Під час шифрування файлів програма-вимагач використовує шифрування *AES* і вбудований ключ *RSA* для шифрування ключа шифрування. Для кожного зашифрованого файлу до імені файлу буде додано розширення *.Lorenz.sz*40. Наприклад, файл з іменем 1.*doc* буде зашифрований і перейменований на 1.*doc.Lorenz.sz*40.

На відміну від інших програм-вимагачів, орієнтованих на підприємства, зразок Lorenz, не вбиває процеси або не закриває служби Windows перед шифруванням.

Кожна папка про викуп на комп'ютері буде записуватися під назвою *HELP_SECURITY_EVENT.html,* яка містить інформацію про те, що сталося з файлами жертви. Вона також міститиме посилання на сайт витоку даних *Lorenz* і посилання на унікальний платіжний сайт *Tor*, де жертва може побачити свій запит на викуп. Кожна жертва має спеціальний платіжний сайт Tor, який містить вимогу викупу в біткойнах і форму чату, в якому жертви можуть домовитися зі зловмисниками. Зі записів про викуп, які бачив *BleepingComputer*, вимоги *Lorenz* про викуп варіюються від 500 000 до 700 000 доларів. Попередні версії програм-вимагачів включали вимоги викупу на мільйон доларів, але неясно, чи були вони пов'язані з тією ж операцією.

Зараз програму-вимагач аналізують на наявність слабких місць, і

BleepingComputer не радить жертвам платити викуп, поки не буде визначено, чи може безкоштовний дешифратор відновити файли безкоштовно. Вже створений дешифратор, який надає можливість частково відновити вкрадені дані.

Таким чином, інформація – це ресурс. Втрата конфіденційної інформації завдає моральної чи матеріальної шкоди. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією, зводяться до її розголошення, витоку та несанкціонованого доступу до її джерел. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена лише комплексним системним захистом інформації. Комплексна система захисту має бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту має спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування у повсякденних умовах, у критичних ситуаціях. Різноманітність умов, що сприяють неправомірному оволодінню конфіденційною інформацією, викликає необхідність використання не менш різноманітних способів, сил та засобів для забезпечення інформаційної безпеки.

Способи забезпечення інформаційної безпеки мають бути орієнтовані на запобіжний характер дій, що спрямовуються на завчасні заходи запобігання можливим загрозам комерційним секретам. Забезпечення інформаційної безпеки досягається організаційними, технічними та організаційно-технічними заходами, кожне з яких забезпечується специфічними силами, заходами та засобами, що мають відповідні характеристики.

Список літератури

1. Остроухов В.В., Присяжнюк М.М., Фармагей О.І., Чеховська М.М. та ін. Інформаційна безпека: підручник. Київ: Видавництво Ліра-К, 2021. 412 с.

2. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley, 2019. 800 p.

3. Sagare A.A., Khondoker R. Security Analysis of SDN Routing Applications. In: Khondoker, R. (eds) SDN and NFV Security. Lecture Notes in Networks and Systems, vol. 30. Cham: Springer, 2018. pp. 1-17. DOI: https://doi.org/10.1007/978-3-319-71761-6_1.

4. Канали втрати конфіденційної інформації. *Канали втрати конфіденційної інформації – Канали витоку інформації sites.google.com.* URL: https://sites.google.com/site/kanalivitokuinformaciie/klasifikacia-kanaliv-vitoku-informaciie/kanali-vtrati-konfidencijnoie-informaciie (дата звернення 21.10.2022).

5. Апаратно-програмні засоби захисту інформації. *Апаратно-програмні засоби захисту інформації – Студопедія studopedia.com.ua.* URL: https://studopedia.com.ua/1_221082_aparatno-programni-zasobi-zahistu-informatsii.html (дата звернення 21.10.2022).