МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ

НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КІБЕРБЕЗПЕКА: АКТУАЛЬНІ ПИТАННЯ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ»

13 – 16 червня 2024 р.

с. Світязь

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
STATE SCIENTIFIC AND RESEARCH INSTITUTE OF CYBERSECURITY TECHNOLOGIES AND INFORMATION PROTECTION
FACULTY OF AERONAUTICS, ELECTRONICS AND TELECOMMUNICATIONS FACULTY OF COMPUTER SCIENCES AND TECHNOLOGIES
SCIENTIFIC CYBER SECURITY ASSOCIATION OF UKRAINE

PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

«CYBER SECURITY: CURRENT ISSUES AND WAYS TO SOLVE THEM»

June, 13 – 16, 2024
Svitiaz, Ukraine

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КІБЕРБЕЗПЕКА: АКТУАЛЬНІ ПИТАННЯ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ»

13 – 16 червня 2024 р.
с. Світязь, Україна

УДК 35.316: 004.9 (043.2)

Кібербезпека: актуальні питання та шляхи їх вирішення: Тези науково-практичної конференції; с. Світязь, 13 – 16 червня 2024 р., Національний авіаційний університет. – К.: Вид-во НАУ, 2024. – 25 с.

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

ЗМІСТ

УДК 004.05:351.81

Б.Д. Халмурадов, Л.С. Чубко, Н. В. Журавель, В.В. Нечипорук
Національний авіаційний університет, м. Київ

КОНВЕРГЕНЦІЯ КІБЕРНЕТИЧНОГО ТА ФІЗИЧНОГО ВИМІРІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Середовище ризиків, що впливають на критичну інфраструктуру, складне й невизначене; загрози, вразливості й наслідки продовжують розвиватися. Критична інфраструктура, яка вже давно піддається ризикам, пов'язаним з фізичними загрозами та стихійними лихами, зараз дедалі більше піддається кіберризикам; ця тенденція зумовлена зростальною інтеграцією інформаційно-комунікаційних технологій з операціями критичної інфраструктури, а також тим, що супротивники зосереджуються на використанні потенційних кібервразливостей. Загрозливе середовище динамічне й містить низку ризиків для інфраструктурних систем з боку національних супротивників і конкурентів, екстремальних погодних явищ, тероризму та насильницьких злочинів. Ці ризики є більш численними, складними, розпорошеними географічно та між різними зацікавленими сторонами, їх складно зрозуміти й управляти ними. Інфраструктурні системи та критичні функції, які вони забезпечують, є системами систем зі складними взаємозалежностями й потенціалом для каскадних збоїв у разі їх порушення.

З операційної точки зору, для ефективного функціонування критично важлива інфраструктура в усіх секторах дедалі більше покладається як на фізичні активи, так і на кіберсистеми. Сучасні загрози час-то є гібридами, які використовують фізичну інфраструктуру, інформаційні технології (IT) та операційні технології (OT) як шляхи підходу злочинців. Наприклад, електроенергетичні системи включають як фі-зичні ресурси для виробництва та передачі електроенергії (наприклад, електростанції, опори ліній електропередачі, лінії електропередачі та розподілу, підстанції, центри управління), так і кіберсистеми для управління ними (наприклад, системи диспетчерського контролю та збору даних (ДКЗД) для управління віддаленими операціями, розподілені системи управління для контролю процесів на електростанціях, інтелектуальні технології для обліку та звітності про стан). Ці фізичні й кібернетичні елементи мають чітко виражену вразливість до різних за-гроз і небезпек та можуть спричинити цілу низку наслідків, якщо їх порушити. Вони також збільшують складнощі, пов'язані з виявленням та аналізом інфраструктурних залежностей і взаємозалежностей.

Вплив залежностей і взаємозалежностей на стійкість інфраструктури.

Зростаюча залежність і взаємозалежність між системами критичної інфраструктури, особливо залежність від інформаційно-комунікаційних

технологій, збільшує потенційну вразливість до фізичних і кіберзагроз, а також потенційні наслідки, пов'язані з компрометацією базових систем або мереж. Залежність — це односпрямований зв'язок між двома активами, коли операції одного активу впливають на операції іншого. Наприклад, водоочисна станція може залежати від послуг зв'язку, які підтримують системи ДКЗД, необхідні для управління роботою станції. Взаємозалежність — це двосторонній зв'язок між двома активами, коли операції обох активів впливають одна на одну. Взаємозалежність — це фактично поєднання двох залежностей, тому розуміння взаємозалежності вимагає аналізу односторонніх залежностей, які її складають. Наприклад, водоочисна станція може потре-бувати зв'язку для своєї ДКЗД-системи, і, зі свого боку, надавати воду, яку використовує система зв'язку для охолодження обладнання.

Хоча безпека може бути ефективною у вирішенні певних аспектів ризику, спричиненого залежностями й взаємозалежностями, самих лише рішень безпеки недостатньо для вирішення проблем залежностей і взаємозалежностей, зважаючи на їхню зовнішню належність до інфраструктурної системи. Наприклад, функції кібербезпеки для систем ОТ, підключених до Інтернету, є ефективним підходом до захисту від потенційних кіберзагроз для операцій, які виникають через залежність від зовнішніх інтернет-сервісів. Однак ці рішення не можуть вирішити проблему збоїв у роботі самого інтернет-провайдера. Суб'єкти господарювання можуть принаймні підготуватися до проблем, від яких вони, можливо, не зможуть убезпечити себе; ці дії втілюють риси стійкості. Таким чином, розвиток стійкості має важливе значення для управління широким спектром ризиків, які несуть у собі залежності та взаємозалежності. Відповідно, залежності та взаємозалежності мають сильний вплив на стійкість інфраструктури, а оцінка стійкості інфраструктури значною мірою залежить від розуміння та оцінки цих залежних зв'язків, а також від заходів, що вживаються для пом'якшення наслідків їхнього потенційного порушення.

УДК 621.396

О.П. Нечипорук., О.М. Супрун., Журавель С.В.
Національний авіаційний університет, м. Київ

АНАЛІЗ ПРИНЦИПІВ РОБОТИ БЕЗДРОТОВИХ СИСТЕМ ПЕРЕДАЧІ ДАНИХ В УМОВАХ ДЕСТРУКТИВНИХ ВПЛИВІВ

На теперішній час спостерігається стрімке зростання бездротових систем передачі даних, які активно впроваджуються в різні сфери людської діяльності. Однією з таких перспективних сфер є контроль територій різ-

них об'єктів, в яких використовуються системи, що забезпечують збір інформації з розподілених по території об'єкта датчиків з радіозв'язуванням.

Бездротові системи передачі даних порівняно з дротовими системами передачі даних мають такі переваги: простота організації, менші витрати на побудову та експлуатацію, можливість застосування за відсутності дротових ліній зв'язку та в надзвичайних ситуаціях, можливість оперативної зміни структури і параметрів систем, велика зона покриття та деякі інші.

Зазначені переваги визначають перспективність розвитку бездротових систем передачі даних.

Водночас, у зв'язку з активним впровадженням бездротових технологій, з одного боку, і розвитком ринку недорогих засобів деструктивного впливу на радіоканал, поширенням промислового шпигунства, збільшенням кількості протиправних дій з боку третіх осіб, з іншого боку, забезпечення скритності радіоканалу від деструктивних впливів є одним із пріоритетних завдань під час побудови нових і вдосконалення наявних бездротових систем передачі даних.

До основних видів деструктивних впливів належать такі дестабілізуючі чинники: перехоплення, перегляд, підміна, радіоелектронне придушення. Слід зауважити, що ці дестабілізуючі фактори можуть застосовуватися не тільки окремо, а й у комплексі.

Комплексні деструктивні впливи, що впливають на бездротову систему передачі даних одночасно, можуть дестабілізувати її роботу в достатній мірі, і для їхньої реалізації наразі відомо досить багато методів і технологій.

Розглянемо практичну реалізацію описаних вище деструктивних впливів на радіоканал для того, щоб показати, що рівень потенційного деструктивного впливу на нього завжди є досить високим. Так відомі методи часткового розкриття зашифрованої за допомогою криптографічних методів захисту (КМЗ) інформації, наприклад алгебраїчні та статистичні методи криптоаналізу, а також диференціальні та лінійні методи. Так само відомо багато технологій, спрямованих на придушення радіосигналів, які досить успішно можуть порушити роботу як радіоканалу на основі простих сигналів, у якому передана інформація прихована за допомогою КМЗ, так і радіоканалу, заснованого на використанні шумоподібних сигналів (ШПС).

Так само досить поширеним є перехоплення радіосигналу за допомогою оптимального приймача. ШПС потенційно можна перехопити за допомогою різноманітних радіотехнічних пристроїв (наприклад, цифрового аналізатора спектра), які спираються на енергетичні показники сигналу (база сигналу і відношення сигнал/шум). Так само ці пристрої застосовні для перехоплення і радіосигналу на основі простих сигналів, в якому в якості методу забезпечення скритності використовується КМЗ.

Порівняльна оцінка різних видів завад на радіолінію на основі псевдовипадкової перебудови робочої частоти показує, що загороджувальні завади є більш ефективними порівняно з оптимальними. Загороджувальні перешкоди можна представити за допомогою такого виразу:

$$P = U_{тш}(t)\cos[\omega_{p1}t + \varphi_{p1}(t)],$$

де $U_{тш}(t)$ – закон зміни обвідної перешкоди, $\varphi_{p1}(t)$ – закон зміни фази перешкоди, $\omega_{p1}(t)$ – закон зміни фази завади, ω_{p1} – середня частота завади.

Проаналізувавши дані можна зробити наступні висновки: проблема забезпечення скритності радіоканалу є актуальною і потребує нових рішень через те, що наявні рішення не завжди можуть впоратися із завданням щодо забезпечення скритності радіоканалу від деструктивних впливів.

УДК 004.42

О.М. Супрун[1], В.В. Лукашенко[2], О.О.Супрун[3]
[1,2]Національний авіаційний університет, м. Київ
[3]Київський національний університет імені Тараса Шевченка

ОСОБЛИВОСТІ СТЕГАНОКОНТЕЙНЕРА НЕПРЯМОЇ ПОСЛІДОВНОСТІ

Вступ. Серед методів стеганографічних перетворень найбільш пріоритетними й використовуваними на практиці є методи вбудовування інформації в цифрове зображення-контейнер. Дані методи характеризуються простотою моделей реалізації вбудовування, поширенням різних класів цифрових контейнерів в інформаційному середовищі, значним обсягом критичної інформації, яку можливо вбудувати в цифрові зображення різних класів, мінімальною кількістю обчислювальних операцій для здійснення алгоритмів вбудовування й вилучення інформації [1].

Основні підходи до вбудовування інформації в зображення-контейнер. Стеганографічні методи вбудовування інформації в зображення-контейнер використовують алгоритми безпосереднього і непрямого стеганографічного вбудовування (Рис. 1).

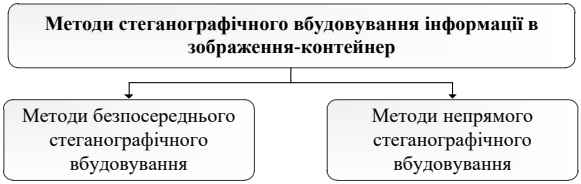

Рис. 1. Класифікація стеганографічних підходів для вбудовування інформації

Реалізація безпосереднього вбудовування можлива за рахунок особливостей системи людського ока. Завдяки тому, що зір людини не здатен розрізняти незначні зміни кольору і яскравості, цифрові зображення володіють психовізуальною надмірністю: в зображенні є області, усунення або заміна яких залишається візуально непомітною для людини.

Найпоширенішими методами безпосереднього вбудовування є методи вбудовування в найменш значимий біт колірних компонент пікселів зображення-контейнера: метод заміни найменш значимого біта, метод псевдовипадкового інтервалу, метод псевдовипадкової перестановки.

Для усунення недоліків непрямого стеганографічного вбудовування пропонується розробити підхід, який дозволить використовувати для прихованого вбудовування не тільки психовізуальну, а й структурну надмірність зображення-контейнера. Реалізація стеганографічного вбудовування на основі розроблюваного підходу має забезпечити умови:

1. Забезпечити вбудовування прихованого повідомлення обсягом V_{mes} не менш заданого обсягу $V_{mes}^{(mp)}$:

$$V_{mes} \geq V_{mes}^{(mp)} \quad (1)$$

2. Забезпечити мінімальний рівень $h_{стег}$ внесених візуальних спотворень, що не перевищують певний пороговий рівень ε:

$$h_{стег} \leq \varepsilon \quad (2)$$

3. Забезпечити мінімальну кількість операцій $N_{опер}$, необхідних для реалізації прямого і зворотного стеганографічного перетворення.

В якості такого підходу пропонується формувати стеганоконтейнер непрямої послідовності на основі набору спеціалізованих функцій.

Список використаних джерел

1. O. Yudin, R. Ziubina, O. Suprun, S.Buchyk, O. Frolov, N. Barannik, "Efficiency Assessment of the Steganographic Coding Method with Indirect Integration of Critical Information": Proceeding of the International Conference

on Advanced Trends in Information Theory (ATIT 2019), Kyiv, Ukraine, 18.12.19-20.12.19, 2019. IEEE Catalog Number: ISBN 978-1-72-81-61-44-0/19/$31.00©2019IEEE, pp.36-40.

О. Весельська, Р. Зюбіна, О. Фролов "Систематизація та класифікація наявних стеганографічних методів приховування інформації", Наукоємні технології, Том 30, № 2, с.187-194, 2016.

УДК 004.056.8

Н.В. Заїка, М.Ю. Комаров, І.В. Мартинюк, Г.В. Мартинюк
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, м. Київ

АНАЛІЗ АТАК НА АКТИВИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ. Ресурси, які можуть бути виділені для захисту активів об'єктів критичної інфраструктури (ОКІ), не безмежні, тому дуже важливо проаналізувати, як найкраще витратити зазначені ресурси, щоб звести можливі атаки на апаратуру ОКІ до мінімуму. В цьому може допомогти моделювання різного виду загроз, так як під час проведення зазначеного моделювання визначаються вразливі активи та потенційні атаки, які можуть відбуватися на об'єктах.

Аналіз проблематики. На ОКІ розрізняють такі атаки, як апаратні, програмні атаки на обладнання та гібридні.

Апаратні атаки зазвичай націлені на вразливості апаратної частини комп'ютерних систем, таких як процесори, фізична пам'ять, чіпи безпеки тощо. Це можуть бути атаки з використанням фізичного доступу до пристрою, злому захисту чіпів або використання спеціалізованого обладнання, можуть включати доступ до порту налагодження Joint Test Action Group (JTAG). Поверхня атаки може бути розширена від печатної плати до мікросхеми, використовуючи методи декапсуляції та мікрозондування.

Програмні атаки на апаратні засоби - це зловмисне використання програмного забезпечення для отримання несанкціонованого доступу до системи або даних. Вони можуть включати експлойти вразливостей програмного коду, впровадження шкідливого програмного забезпечення через вебсайти, електронну пошту тощо.

Існують два підкласи програмних атак на обладнання: введення помилок і атаки через побічні канали (непрямі шляхи доступу до інформації).

Введення помилок - це навмисне введення пристрою у стан збою. Саме введення помилок не є атакою як такою, проте результат такого введення може мати негативні наслідки. Введення помилок змушує пристрій

працювати за межами його нормальних робочих параметрів, а результат атаки досягається шляхом маніпуляцій з його фізичними параметрами. Наприклад, зловмисники можуть отримати доступ до пристрою, обійшовши захист перевірки підпису прошивки (firmware).

Атаки через побічні канали базуються на використанні непрямих шляхів доступу до інформації, що зберігається або оброблюється апаратурою. До таких атак відносяться атаки, які спрямовані на помилки проектування, конфігурації, реалізації або на функції, якими можна скористатися, щоб обійти безпеку системи. Для цього використовується аналіз інформації про зміни поведінки систем та обладнання ОКІ.

Сучасні гібридні атаки на ОКІ включають в себе етап зі створення комплексу дій для подолання або обходу систем захисту активів ОКІ. Наприклад, до таких атак можуть бути включені дії з отримання інформації про програмні вразливості систем ОКІ та слабкі місця в системі фізичного контролю доступу, використання сучасних програмно-апаратних комплексів та застосування методів соціального інжинірингу. Після накопичення достатньої кількості даних, зловмисники використовують виявлені вразливості для атаки або для фізичного проникнення до ОКІ.

Захист активів на ОКІ повинен враховувати всі можливі види атак і наслідки, які виникають після успішного проведення даних атак. Для запобігання більшості атак рекомендовано проводити оновлення програмного забезпечення, будувати комплексну системи захисту інформації на ОКІ, проводити навчання персоналу, створювати плани відновлення, проводити тестування та аудит стану кібербезпеки на ОКІ.

Висновки. У роботі представлено класифікацію атак на ОКІ: апаратні, програмні атаки на обладнання та гібридні атаки. Для кожного з зазначених видів атак наведено приклади їх виникнення та шкоду, які вони можуть завдати. Також наведено рекомендації для запобігання даним атакам.

Список літератури

1. Sam Newman. Building Microservices 2E. – O'Reilly Media, Inc. – 2021. – 624 p.

2. Colin O'Flynn and Jasper van Woudenberg. The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. – San Francisco, No Starch Press Inc. – 2022. – 560 p.

УДК 004.056.5

Н.В. Пащенко
ПрАТ «Данон Кремез», м. Кременчук

ПРОВЕДЕННЯ ТЕСТІВ НА ПРОНИКНЕННЯ, ЕТАПИ ПРОВЕДЕННЯ, НАЙПОШИРЕНІШІ ПРОБЛЕМИ, ШЛЯХИ ВИРІШЕННЯ

Досвід проведення тестів на проникнення. Коли ми говоримо про безпеку даних компанії, ми маємо використовувати не лише традиційні інструменти, а і більш сучасніші. Саме пентест дає можливість оцінити будь-якому бізнесу стійкість інформаційної інфраструктури до потенційних загроз, виявити слабкі місця в IT-середовищі. Тести внутрішніх систем, хмарних зовнішніх рішень. Залучення сторонніх організацій до проведення тестів на проникнення. Отримання реалістичної картини слабких місць, які потрібно виправляти.

Етапи проведення: все починається з вибору постачальника - наявність відповідних сертифікатів, які підтверджують кваліфікацію пентестера, досвід роботи. Визначити структуру проведення пентесту на проникнення. Як відомо, тести на проникнення можуть бути виконані трьома способами: Black Box, Gray Box, White Box. Ми дійшли висновку, що більш ефективний результат ми отримуємо, коли поєднуємо їх. Наприклад, пару днів Black Box, а решта часу Gray Box. Оптимальна тривалість тесту 14 календарних днів. Таким чином ми розуміємо, на скільки система вразлива, коли зловмисник має мінімальний набір інформації, та що може зробити, маючи трохи більше інформації (отримання адміністського привілейованого доступу, зміна даних). Навіть досвідчені IT спеціалісти та розробники можуть не помітити підставну фальшиву сторінку та вести там свої данні. Початок пентесту - збір необхідної інформації. Потім - застосування соціальної інженерії, брутфорс. На основі зібраних даних пошук точок входу в мережу або в систему. Пошук вразливостей, їх застосування. По завершенню надається звіт про виявлені слабкі місця та вразливості, які можуть бути використані зловмисниками. Бажано організувати зустріч, щоб пентестер зробив демо всього виявленого. Далі пентестер надає детальний звіт всіх дій та рекомендації щодо усунення цих вразливостей. Складання та контроль виконання плану дій. Видалення/закриття всіх наданих доступів для проведення так званої атаки.

Переваги: професійна оцінка актуального рівня захищеності IT-систем, мереж. Виявлення слабких місць, вразливостей, перш ніж про них дізнаються зловмисники. Рекомендації по їх усуненню. Тест на проникнення дає також можливість перегляду стратегії кіберзахисту. Водночас під час пентесту є можливість перевірити реакцію та послідовність дій на кібератаки внутрішніх команд, та за необхідності оновити політики, ско-

регувати послідовність дій внутрішніх команд. Водночас це і перевірка IT команд постачальників, які надають компаніям-замовникам послуги, або системи, що є не меш важливим.

Найпоширеніші проблеми: ґрунтуючись на досвіді професійних пентестерів можемо виділити наступні найпоширеніші проблеми. Обізнаність з кібербезпеки співробітників компаній. Як ми знаємо понад 90% кібератак починаються саме з одного фішингового листа. Слабке керування паролями: використання одного паролю для декількох систем, не стійкі паролі, незмінені адмінські паролі за замовчуванням, як для обладнання так і для систем. Зберігання у відкритому доступі, це файли WORD, txt, OneNote і т.д. Неправильне налаштування пристроїв, систем. Використання незахищених протоколів (HTTP), невірне налаштування файерволів і навіть невірне налаштування систем захисту Кібербезпеки.

Шляхи вирішення: регулярні програми з підвищення обізнаності співробітників. Проведення регулярних Phishing simulation з обов'язковим зворотнім зв'язком. Регулярний перегляд політик з кібербезпеки. Регулярне проведення тестів на проникнення. Контроль виконання плану дій, який був створений за результатами проведеного тесту на проникнення.

Тест на проникнення дуже потужний, ефективний інструмент, мета якого підвищити загальний рівень безпеки будь-якого бізнесу. Фактично, кожен бізнес сьогодні є потенційно вразливим та вимагає більшого захисту та більшого тестування. Кожен день виникає велика кількість нових кіберзагроз. Тому тестування на проникнення є своєрідним «щепленням» від майбутніх загроз. Рекомендовано регулярно проводити пентести хоча б один раз на два роки для кожної системи аби бути більш захищеним від цілеспрямованої атаки.

УДК 004.78 (043.2)

Є.Б. Артамонов, Ю.Ю. Головач, Т.І. Залозний,
Д.В. Крант, А.В. Радченко, К.М. Радченко
Національний авіаційний університет, м. Київ.

ПІДХОДИ ДО ВИЗНАЧЕННЯ КОРИСТУВАЧІВ ПРОГРАМНИХ КОМПЛЕКСІВ ЗА ПОВЕДІНКОВИМИ ФАКТОРАМИ

Сьогодні програмні комплекси відіграють ключову роль практично у всіх сферах діяльності, відстеження та аналіз поведінки користувачів стають дедалі більш актуальними завданнями. З огляду на постійне зростання кіберзагроз і необхідність забезпечення безпеки та персоналізації з'являється необхідність в розробці і використанні додаткових методів ідентифікації користувачів, одним з яких є оцінка поведінкових факторів.

Існує кілька розповсюджених підходів до визначення користувачів програмних комплексів за поведінковими факторами:

– шляхом аналізу кліків, послідовностей дій, поведінкових маршрутів, що дозволяє виявити типові стилі взаємодії з системою і попередити модуль безпеки, якщо у користувача ці стилі починають різко відрізнятись від попередніх;

– шляхом аналізу метаданих, таких як час та частота взаємодії з системою, використані функції в системі, що також дозволяє виявити патерни використання системи і побудувати «профіль» користувача.

Пропонується використовувати методи аналізу графів та оцінки схожості шляхів на графі для визначення «профіля» поведінки користувача. Такий підхід дозволяє використати вже апробовані методи, які мають довгу історію використання:

– коефіцієнт Жаккара (Jaccard Coefficient), який вимірює об'єднання та перетин множин вершин на шляхах і обчислює схожість як відношення розміру перетину вершин до розміру об'єднання вершин шляху [1];

– косинусна схожість (Cosine Similarity), де кожен шлях користувача у векторному форматі, а значення компоненти вказує на наявність чи відсутність цієї вершини на шляху [2];

– відстань Левенштейна (Edit Distance), яка обраховує кількість простих операцій для перетворення одного вектора в інший (вставка (додавання символу в рядок), видалення (видалення символу з рядка), заміна (аміна одного символу на інший)) [3];

– вбудовування графів (Graph Embeddings), який об’єднує низку різних методів, таких як DeepWalk, Node2Vec, LINE (Large-scale Information Network Embedding), Graph Convolutional Networks (GCNs), Graph Attention Networks (GATs).

Для того, щоб використовувати методи аналізу графів, потрібно виконати декілька кроків, які включають перетворення даних про поведінку користувачів у графові структури:

Крок 1: збір даних про поведінку користувачів (переглянуті сторінки та об’єкти на сторінці, вимірювання часу, який користувач проводить на кожній сторінці чи над активним об’єктом, фіксація кожного кліка, завантаження файлів, заповнення форм тощо);

Крок 2: перетворення даних на графову структуру, яка містить вузли (кожна сторінка та об'єкт на сторінці), ребра (переходи користувача між вузлами, вага ребер (кількість переходів або час, проведений до переходу на інший вузол);

Крок 3: створення профілю поведінки (побудова графів для кожного користувача для різних кейсів (зазвичай, кейси-маркери), виділення основних шляхів користувача на графі.

Висновки

Використання графових методів для аналізу поведінки користувачів на сайті дозволяє отримати глибокі інсайти та створити більш персоналізований користувацький профіль. Але для цього треба використовувати спеціалізовані методи збору даних і вести логування всіх дій користувача.

Розглянуті методи дозволяють перетворити графи поведінки користувачів у векторні представлення, що можуть бути використані для ідкнтифікації, класифікації та кластеризації користувачів через метрики схожості патернів поведінки.

Використані джерела

1. Abdullah, Sura & Sura, Mazin & Makttof, Mohammed. (2020). Modifying Jaccard Coefficient for Texts Similarity. Opcion. 32. 2899-2921.

2. Shaw, Jim & Yu, Yun William. (2022). Theory of local k-mer selection with applications to long-read alignment. Bioinformatics, 38(20):4659–4669.

3. Valeriano, Eugene. (2024). Deduplication Methods Using Levenshtein Distance Algorithm. Journal of Electrical Systems. 20. 997-1006. 10.52783/jes.3480.

УДК 004.056.5

І.В. Гринчій
ТОВ «Данон Дніпро», м. Київ

КІБЕРБЕЗПЕКА У ДАНОН. ОСНОВНІ ПРОЦЕСИ ТА ЇХ ОРГАНІЗАЦІЯ

Компанія Данон – міжнародна команнія з центральним офісом у Парижі. Три бізнеси: Молочна продукція та Продукція рослинного походження, Спеціалізоване харчування: Дитяче та Медичне, Вода. 100 тис співробітників по всьому світу у 130 країнах.

В Україні Група компаній «Данон» вже більше 20 років є виробником і дистриб'ютором широкого асортименту продуктів харчування. Виробничі потужності компанії представлені двома заводами: «Данон Дніпро» (у м. Херсон - наразі діяльність призупинена) і «Данон Кремез» (у м. Кременчук). Продукція компанії випускається під такими торговими брендами: «Активіа», «Живинка», «ПростоНаше», «Ростишка», «Деліссімо», «Paw Patrol», «Alpro», «Danone».

Напрямок дитячого харчування представлений в Україні брендами «Nutrilon» та «Milupa».

Напрямок клінічного харчування представлений наступними продуктовими гілками: «Nutrison», «Nutridrink», «Cubitan», «Infatrini», «Nutrini», «Lophlex», «Nutri», «Anamix», «KetoCal».

ІТ команда, що відповідає за питання кібербезпеки поділяється на дві частини: Глобальну на Локальну.

Задачі Глобальної команди:

- розробка документації: глобальних політик, стандартів
- побудова та оптимізація основних процесів, що стосуються ІТ кібербезпеки
- підбір, закупівля, налаштування та подальше управління рішеннями для захисту кінцевих точок та інформаційної безпеки
- моніторинг активностей у внутрішній мережі компанії
- перевірка відповідності ПЗ внутрішнім стандартам компанії
- пошук, аналіз та пріоритезація вразливостей, розслідування інцидентів з кібербезпеки

Задачі Локальної команди:

- адаптація політик та стандартів під особливості кокретного ринку (тобто країни)
- допомога у розслідуванні інцидентів, комунікація та залучення інших департаментів.
- Підготовка локальної документації (політики, стандарти, посібники).
- впровадженя та виконання Програми обізнаності користувачів.

Активна та регулярна комунікація між двома частинами команди - необхідний елемент успішної взаємодії. Окрім взаємодії у стандартних процесах, організовані регулярні щотижневі зустрічі усіх представників ІТ Cybersecurity для навчання та обміну інформацією з тем, повязаних з кібербезпекою у Данон та світі.

Основні процеси у сфері Кібербезпеки:

Інцидент менеджмент. За наявності підозрілої повіденки систем Ініціатор оформлює запит будь яким чином: телефонний дзвінок на локальну або глобальну команду, електронний лист будь кому з команди кібербезпеки, лист на виділену поштову скриньку CERT.

Робота над вразливостями. Глобальна команда виконує сканування на вразливості інформаційних системи та мереж, обладнання та веб-сайтів, включаючи зовнішні, повідомляє про знайдені вразливості локальним командам. Локальна команда - контроль виправлення вразливостей, Комунікації з бізнесом та ІТ командами, відповідальними за виправлення. Ведення реєстру вразливостей, збір статистики. Цей процес є під пильним контролем внутрішніх аудиторів, які проводять щорічну оцінку.

Оцінка ризиків. Проводиться для нових проектів та існуючих, особливо**,** критичних систем (виконується періодично)

Тести на проникнення. Перевірка систем та мереж на наявність вразливостей зі спробами зламу, несанкціоноване отримання доступу до систем чи мереж, отримання адміністративного доступу або можливості

самовільного розширення існуючого доступу. Зазвичай виконуються силами сторонніх організацій, що мають відповідну кваліфікацію.

Програма обізнаності користувачів. Це одна із найважливіших та водночас найскладніших задач, оскільки людина є найслабшою ланкою у системі безпеки компанії. Інструменти, які допомагають вирішувати це питання:

- Комунікації - пости у внутрішній мережі
- Виступи на загальних зборах співробітників
- Тренінги з кібербезпеки (електронні та онлайн)
- Фішинг симуляції
- Заходи обізнаності з кібербезпеки – місяць Жовтень.

Підтримка обізнаності користувачів інвормаційних мереж та систем, а надто, ІТ персоналу, що має привілейований доступ, адміністративні можливості– є ключовим напрямком діяльності команд з Кібербезпеки.

Не має значення, наскільки захищені ваші мережі та системи, наскільки складні вимоги до паролів, наскільки добре ви виявляєте та закриваєте основні вразливості, якщо користувач з легкістю переходить за лінками, отриманими від зловмисників, та дарує йому свої особисті дані (логін - пароль), завантажує або встановлює шкідливі програми чи їх фрагменти, або програми вимагачі (Ransomware).

В наш час мало просто озброїтись сучасними системами та технологіями для захисту інформаційних систем та мереж. Дуже важливо пояснити усім, хто дотичний до вашої інформаційної структури (співробітники компанії, підрядники, постачальники послуг) про необхідність бути максимально пильним, коли мова йде про особисті дані, такі як логіни та паролі, бути обережними з повідомленнями, які вони отримують по будь яких каналах (пошта, смс, робочі та особисті месенджери, та навіть телефонні дзвінки).

УДК 004.8

О.М. Тачиніна, С.О. Кашкевич
Національний авіаційний університет, м. Київ,

ПРИНЦИПИ ПОБУДОВИ ІНФОРМАЦІЙНИХ МЕРЕЖ З МОЖЛИВІСТЮ ДО САМООРГАНІЗАЦІЇ

Синергетичні принципи все частіше впроваджуються в інформаційні технології. Технічні системи стають глобальними та розподіленими, а завдання, які вони виконують, стають все більш складними. Незважаючи на значні успіхи в галузі елементів технічних систем, включаючи нові технології, середовища передачі даних, збільшення продуктивності, швидкості, частот тощо,

питання управління в таких системах все ще залишаються відкритими. Кібернетика частково вирішує цю проблему, розробляючи методи та засоби для автоматизації управління в технічних системах, побудованих на основі зворотного зв'язку.

Самоорганізація є характерною рисою будови і функціонування всіх природних систем, вершиною яких є людина. Загальні черги самоорганізації також простежуються і в неживій природі. Тим не менш, немає сумнівів, що людський організм також є найдосконалішою системою. За синергетичною концепцією, самоорганізація можлива лише у відкритих системах, що знаходяться далеко від термодинамічної рівноваги. Такі системи інтенсивно обмінюються енергією, речовиною та інформацією з навколишнім середовищем.

Іншою характеристикою природних систем які самоорганізовуються, є наявність у їх поведінці так званих точок біфуркації. Під точкою біфуркації в синергетиці розуміється стан максимального хаосу або безладу в системі, що відповідає подальшій стрибковій зміні її функціонування. На відміну від систем живої та неживої природи, де коливання можуть мати абсолютно непередбачуваний характер і фізичну основу, зміни в штучній технічній системі можуть відбуватися на трьох рівнях: зміни значень параметрів елементів; зміни в функціях, що реалізуються елементами; зміни в структурі системи.

У зв’язку з цим технічні системи можуть мати три види самоорганізації: параметричну, функціональну та структурну. Завдання параметричної самоорганізації в загальному вигляді може бути поставлена і розв'язана як багатокритеріальну оптимізаційну задачу з обмеженнями .

Для реалізації процесів параметричної самоорганізації можуть бути використані різні методи параметричної оптимізації. Вибір методу здійснюється на основі аналізу виду оптимізованої функції в кожній конкретній ситуації. Функціональна самоорганізація, яка полягає у виборі функцій, що реалізуються елементами, є найменш формалізованою задачею, яка найбільше залежить від конкретної системи. Відповідно до синергетичного підходу, параметрична та функціональна самоорганізація можуть бути віднесені до еволюційному періоду розпаду системи, оскільки, на думку авторів, в загальному випадку вони призводять до менш кардинальних змін у системі, ніж структурна самоорганація, яку в даному контексті було розглянуто як точку біфуркації в разі її успішного завершення.

Структурна самоорганізація здається найскладнішою, і зміни, які вона вносить в систему, повинні бути ретельно обгрунтовані. Запропоновано підхід, заснований на поступовому збільшенні вартості зміни системи та кількості внесених змін: самоорганізація типів елементів; реконфігурація системи; додавання/видалення елементів.

Реконфігурація також не змінює кількісного складу елементів системи, і система повинна намагатися перемістити частину елементів на більш вигідні позиції з точки зору збільшення цільового функціоналу. Переміщення повин-

но враховувати всі можливі обмеження: фізичну спроможність, кількість вільних комірок, економічну доцільність тощо. Додавання та видалення елементів до системи є вершиною процесу самоорганізації в технічних системах і відбувається після невдачі всіх попередніх методів. Аналіз реальних технічних систем показує, що видалення елементів з системи майже ніколи не призводить до збільшення цільової функції, оскільки система в цьому випадку, навпаки, щось "втрачає", можливо, зменшується.

Отримані теоретичні результати можуть бути використані в подальшому для розробки програмного забезпечення системи управління складними розподіленими технічними об'єктами, що функціонують в тому числі в умовах автономності та невизначеності навколишнього середовища.

УДК 004.4

Б.Ю.Вінтенко[1], Т.В. Смірнова[2], О.А, Смірнов[2]
[1]Черкаський державний технологічний університет, м. *Черкаси*
[2]*Центральноукраїнський національний технічний університет, м. Кропивницький*

АНАЛІЗ ВИМОГ ДО КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНОЇ СИСТЕМИ УПРАВЛІННЯ АЕС

Метою даного роботи є дослідження складу та структури програмного забезпечення КСУ АЕС, що використовується для виконання функцій аварійного та попереджувального захисту (АЗ-ПЗ) виробництва ПАТ НВП «Радій».

Згідно з приведеними особливостями, в модулях КСУ використовуються програмовані логічні інтегральні схеми (ПЛІС) високого ступеню інтеграції. При створенні проектів ПЛІС використовуються три основні технології: розробка графічних схем технологічних алгоритмів, написання коду мовою опису цифрових схем (наприклад, VHDL), а також написання програмного коду мовами високого рівня (С та С++), що виконується емулятором мікропроцесора, для виконання функцій обробки сигналів, діагностування, обміну інформацією тощо. У верхньому рівні КСУ використовується ПЗ, написане мовою програмування С++, що виконується під керуванням ОС Windows. Відповідно до даних особливостей є очевидним, що кожний компонент, який містить ПЗ, може містити потенційні вразливості, і через те потребує дотримання вимог під час розробки ПЗ та експлуатації КСУ.

Як зазначається в роботі, програмно-апаратна платформа для побудови КСУ поділяється на верхній та нижній рівень.

До складу верхнього рівня входять робочі станції, що виконують наступні функції: прийом технологічної та діагностичної інформації від вер-

хнього рівня; відображення технологічної інформації про виконання функцій безпеки, стан вхідних та вихідних параметрів, роботу алгоритмів; відображення діагностичної інформації про стан технічних засобів; архівування прийнятої інформації; передача реєстраційної інформації до інформаційно-обчислювальної системи енергоблоку (ІОС).

До складу нижнього рівня входять шафи з типовими функціональними модулями. Найважливіші функції, які виконують дані модулі, наступні: прийом значень аналогових або дискретних сигналів (модулі БВА, БВД); виконання логіки технологічних алгоритмів формування захисту (модулі БФЗ); видача керуючих аналогових та дискретних сигналів (модулі БОС, БДС); діагностування апаратних засобів (модулі БДН); корекція параметрів роботи алгоритмів, що можуть змінюватися оператором (модуль МКУ).

КСУ КЗ-ПЗ складається з двох комплектів, кожен з яких складається з трьох незалежних каналів захисту (шафи ШФС), що взаємно резервують один одного. До складу кожного каналу входить кросова вихідна шафа (КШВ), що об'єднує вихідні сигнали каналів за мажоритарною схемою «2 з 3». Також до складу КСУ входять комп'ютерні шафи (основна та резервна) та інженерні робочі станції. Обмін інформацією між ПЗ КСУ відбувається за допомогою оптичних ліній зв'язку.

Результати дослідження

Аналіз створеного графу обміну інформації дозволяє зробити наступні висновки: до складу ПЗ, що передає передає інформацію, входять всі компоненти; до складу ПЗ, що передає передає інформацію в односторонньому напрямку хоча б одним каналом, входять компоненти БВА, БВД, БОС, БДС, БФЗ, БДН, InfoServer; до складу ПЗ, що приймає інформацію, входять компоненти БДН, БФЗ, БОС, БДС, МКУ, DiagServer, InfoServer, Monitor, Diagnostics; ПЗ, що приймає інформацію від ПЗ зони нижчого рівня: відсутнє, тому немає необхідності в додаткових перевірках.

Таким чином, з точки зору напрямків передачі інформації та її контролю ПЗ має оцінюватися наступним чином: для всіх компонентів ПЗ – передача з додаванням інформації для перевірки її достовірності з боку приймача: версія, розмір, контрольна сума тощо; для компонентів ПЗ БВА, БВД, БОС, БДС, БДН, БФЗ, InfoServer – використання для окремих каналів протоколів даних, що можуть працювати лише в односторонньому порядку, без відповідей з боку приймача; для компонентів ПЗ БФЗ, БОС, БДС, МКУ, DiagServer, InfoServer, Monitor, Diagnostics – контроль цілісності прийнятих пакетів, ігнорування пакетів невірного формату; для компонентів ПЗ БФЗ, МКУ – перевірка коректності параметрів, що прийняті, з технологічної точки зору (перевірка входження значення уставки до допустимого діапазону).

В прикладі, що наводиться, передбачається повне виконання всіх необхідних вимог щодо обміну інформацією.

УДК 004.056.5 (043.2)

А.Д. Пінчук, Р.С. Одарченко, О.О. Полігенько
Національний авіаційний університет, м. Київ

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ КЛАСИФІКАЦІЇ КІБЕРЗАГРОЗ В ІКТ

ІКТ системи стикаються з низкою фізичних і кіберзагроз, які можуть бути зловмисними, ненавмисними або природними. Класифікації кіберзагроз допомагають ідентифікувати та зрозуміти характеристики та джерела кіберзагроз. Вони допомагають виявити, зрозуміти та оцінити кіберзагрози, а отже, рекомендувати або впровадити належні та відповідні рішення та засоби контролю безпеки, щоб захистити системи, активи та послуги, а також бути стійкими до кібератак.

Загалом, підходи до класифікації кіберзагроз можна категоризувати у два головних класи:

- методи класифікації на основі технік кібератак;
- методи класифікації на основі впливу кіберзагроз.

Методи класифікації на основі технік кібератак. У даній категорії можна виділити наступні методи класифікації: модель трьох ортогональних вимірів, гібридна модель, пірамідальна модель класифікації загроз інформаційній безпеці.

Модель трьох ортогональних вимірів була запропонована у [1] Лукасом Руфом та ін., її мета була покращити розуміння загроз та полегшити існуючі моделі. Дана проблема вирішена шляхом введення тривимірної моделі, які ділить весь простір на три ортогональні виміри, що позначають мотивацію (причини створення загрози, що в свою чергу ділиться на навмисну та випадкову), локалізацію (походження загрози, внутрішня чи зовнішня) та агента (той, хто створює загрозу для певного активу ІКТ системи, що може бути представлений людьми, технологіями та форс-мажорними обставинами).

Гібридна модель також має назву як «Модель С3» була запропонована у [2]. Дана модель розглядає три критерії: частота загроз безпеці (частота виникнення загроз), сфера дії загрози (сфера, на яку впливає загроза), джерело загрози (типи джерел загроз безпеці).

Пірамідальна модель [3] представляє класифікацію навмисних загроз безпеці в гібридній моделі. Класифікація відбувається на основі трьох факторів: попередні знання кіберзлочинця про систему (наскільки багато знає зловмисник про систему від апаратної і програмної складової до спів-

робітників і т.д.), критичність (критичність складової системи, на яку може вплинути загроза), втрати (відображає всі втрати, які можуть статися в системі або в організації, на основі тріади CIA).

Методи класифікації на основі впливу кіберзагроз. Для даної категорії можна розглядати такі моделі як STRIDE та ISO.

Модель STRIDE розробили Microsoft, яка застосовується на рівні мережі, хоста та програми [4-5]. Вона дозволяє охарактеризувати відомі загрози відповідно до цілей кібератак чи мотивації кіберзловмисника. Абревіатура позначає наступні категорії: Spoofing identity, Tampering with data, Repudiation, Information disclosure, DoS та Elevation of privilege. Загалом, даний підхід заснований на цілях спроби проникнення в свідомість кіберзловмисника, оцінюючи кіберзагрози.

Модель ISO являє собою еталонну модель, засновану на стандарті ISO 7498-2, та складається з 5 основних впливів загроз безпеці [6]: знищення інформації та/або інших ресурсів, спотворення або модифікації інформації, крадіжка, вилучення або втрата інформації та/або інших ресурсів, розкриття інформації та переривання надання послуг.

Більшість існуючих класифікацій кіберзагроз в ІКТ обмежуються використанням від одного до трьох критеріїв для класифікації, а інші представляють не вичерпний перелік кіберзагроз, тобто не всі кіберзагрози охоплені класифікацією, а категорії не є взаємовиключними. Враховуючи мінливість кіберпростору та постійну зростаючу кількість і критичність кіберзагроз, цього може бути недостанім. Тому є необхідність розробки принципово нової гібридної моделі класифікації кіберзагроз, яка б могла вирішити дану проблему.

Список використаної літератури

1. Ruf L, AG C, Thorn A, GmbH A, Christen T, Zurich Financial Services AG, Gruber B, Credit Suisse AG., Portmann R, Luzer H, Threat Modeling in Security Architecture - The Nature of Threats. ISSS Working Group on Security Architectures, http://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture_Threat-Modeling_Lukas-Ruf.pdf
2. Gerić, S., & Hutinski, Ž. (2007). Information system security threats classifications. Journal of Information and organizational sciences, 31(1), 51-61.
3. Alhabeeb M, Almuhaideb A, Le P, Srinivasan B. Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops: 2010. p. 208-213.
4. Swiderski F, Snyder W. Threat Modeling. Microsoft Press; 2004.

5. Meier J, Mackman A, Vasireddy S, Dunner M, Escamilla R, Murukan A. Improving we application security: threats and counter measures. Satyam Computer Services, Microsoft Corporation; 2003.
6. ISO. Information Processing Systems-Open Systems Interconnection-Basic Reference Model. Part 2: Security Architecture, ISO 7498-2; 1989.

УДК 004.056.55:681.3.06

М.Ю. Мирошніченко
Київський національний університет імені Тараса Шевченка, м. Київ

МЕТОД ЕЛЕКТРОННОГО ПІДПИСУ З ВИКОРИСТАННЯМ ПОСТКВАНТОВОГО АЛГОРИТМУ

Електронний підпис є одним з ключових елементів у системах забезпечення автентичності, цілісності та невідворотності інформації. Метод електронного підпису, заснований на одному з перспективних постквантових алгоритмів є стійким до квантових атак і може бути використаний для захисту конфіденційної інформації в умовах швидкого розвитку квантових технологій. Пришвидшити та полегшити процес міграції класичної криптографії до постквантової можна за допомогою існуючих стандартизованих складових, що супроводжують процес генерації підпису.

Зростання кіберзагроз також підкреслює актуальність розробки цього методу. Кількість і складність атак на інфраструктуру, системи управління, фінансові та державні установи постійно збільшується. Використання надійних криптографічних методів допомагає забезпечити захист інформації від несанкціонованого доступу та зловмисних дій, що є критично важливим у сучасних умовах. Ці методи дозволяють створювати системи, які є стійкими до новітніх кіберзагроз.

Метою даної роботи є аналіз найбільш перспективних постквантових алгоритмів електронного підпису та метод електронного підпису на базі одного з цих алгоритмів, який забезпечує високий рівень захисту від потенційних квантових атак. Для досягнення цієї мети передбачається детальне вивчення вибраного алгоритму, аналіз його стійкості до різних типів атак.

Атаки на постквантовий електронний підпис включають кілька основних типів, спрямованих на злам алгоритмів, стійких до квантових обчислень. Одним із найпоширеніших методів є атаки на основі лінійної алгебри, які намагаються виявити слабкі місця у математичних структурах, таких як решітки, на яких базуються постквантові алгоритми. Ці атаки можуть використовувати складні математичні обчислення для розкриття криптографічних ключів.

Іншим типом є атаки через побічні канали, які використовують фізичні властивості обчислювальних процесів, такі як час виконання, споживання енергії або електромагнітне випромінювання, для отримання конфіденційної інформації. Ці атаки можуть бути дуже ефективними, оскільки вони не залежать від математичної складності алгоритму, а натомість експлуатують практичні аспекти його реалізації.

Нарешті, атаки на реалізацію алгоритмів можуть бути спрямовані на виявлення помилок або вразливостей у програмному забезпеченні чи апаратному забезпеченні. Ці атаки можуть використовувати баги або недостатньо захищені ділянки коду для отримання доступу до криптографічних ключів або інших захищених даних.

Для забезпечення високого рівня безпеки у постквантовій криптографії було обрано метод електронного підпису Falcon. Основною перевагою Falcon є його стійкість до атак квантовими комп'ютерами завдяки використанню алгебраїчних решіток у криптографічних обчисленнях. Falcon також відзначається ефективністю, що дозволяє його застосування на пристроях з обмеженими ресурсами. Завдяки оптимізованій структурі, метод забезпечує високий рівень продуктивності і безпеки, що робить його привабливим вибором для сучасних систем захисту інформації.

Функцію гешування Купина-256 було обрано через її високий рівень криптостійкості та ефективності. Купина-256 відповідає сучасним вимогам безпеки, що робить її надійним інструментом для захисту даних у постквантових умовах. Вона забезпечує ефективне обчислення хешу, що необхідно для генерації електронних підписів. Крім того, Купина-256 була стандартизована відповідно до ДСТУ 7564:2014, що підтверджує її надійність та відповідність сучасним криптографічним стандартам.

Апаратні генератори випадкових чисел (ГВЧ) мають переваги над програмними завдяки використанню фізичних явищ для генерації чисел, що забезпечує вищу якість випадковості та безпеку. Апаратні ГВЧ не залежать від продуктивності процесора і менш вразливі до програмних атак. Було обрано ГВЧ "Гряда-3" завдяки його здатності генерувати високоякісні випадкові числа на основі фізичних датчиків шуму. "Гряда-3" відзначається високою швидкістю генерації та криптостійкістю, що робить його оптимальним вибором для криптографічних застосувань. Використання Гряда-3 підвищує стійкість системи до статистичних атак і забезпечує надійний захист конфіденційної інформації.

У роботі обґрунтовано вибір ключових компонентів для створення надійної системи електронного підпису, здатної протистояти загрозам, що виникають у постквантову еру.

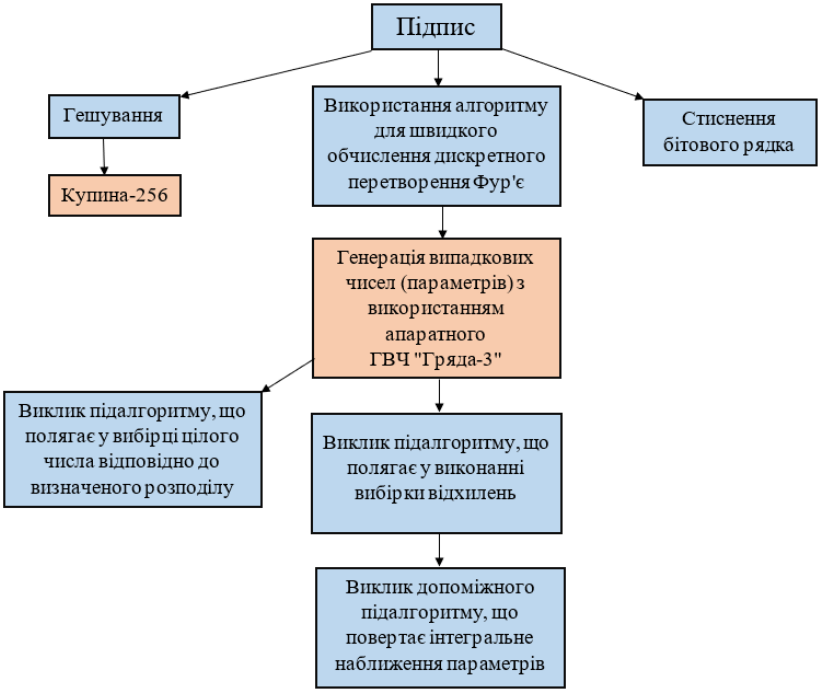

Рисунок 1.1 – Метод електронного підпису на основі алгоритму Falcon

Алгоритм електронного підпису Falcon був обраний завдяки його стійкості до квантових атак і високій продуктивності, що робить його придатним для широкого спектру застосувань, включаючи пристрої з обмеженими ресурсами. Функція гешування Купина-256, стандартизована відповідно до ДСТУ 7564:2014, забезпечує надійну криптографічну безпеку і ефективність обчислень.

Крім того, використання апаратного генератора випадкових чисел Гряда-3 гарантує високий рівень випадковості та безпеки, що значно знижує ризик атак на систему. Завдяки фізичним принципам роботи, ГВЧ Гряда-3 забезпечує надійний захист від статистичних атак, що підвищує загальну безпеку криптографічної системи. Таким чином, обрані рішення дозволяють створити високоефективну і безпечну систему електронного підпису, здатну протистояти сучасним і майбутнім загрозам інформаційної безпеки.

НАУКОВЕ ВИДАННЯ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КІБЕРБЕЗПЕКА: АКТУАЛЬНІ ПИТАННЯ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ»

13 – 16 червня 2024 р.

с. Світязь

Головний редактор Одарченко Р.С.
Комп'ютерна верстка Пінчук А.Д.
Контактний e-mail: conference_scsa@ukr.net

Електронна версія тез конференції зроблена спеціально для розміщення на сайті
Наукової асоціації кібербезпеки України
https://scsa.org.ua/