доступ до якої заборонено, або розкриття інформації в результаті невірного налаштування сайту або веб-сервера.

5. Логічні атаки спрямовані на експлуатацію функціоналу сайту. Додаток може вимагати від користувача коректного виконання кількох послідовних дій для виконання певного завдання. Зловмисник може обійти або використовувати ці механізми у своїх цілях.

Таким чином, при розробці веб-додатку необхідно планувати його архітектуру таким чином, щоб уникнути можливих ризиків та загроз.

Список використаних джерел

1. Сєвєрінов О.В. Аналіз сучасних методів атак на електронні ресурси органів управління / О.В. Сєвєрінов, В.О. Шевцов, А.С. Сокол-Кутиловська // Системи озброєння і військова техніка. – Х: ХНУПС. - 2017. – Вип. 1(49). – С. 65-68.
2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.

Сєвєрінов О. В., к.т.н. доцент,
Щербина Д. В., студент (ХНУРЕ)

АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ ПОРОГОВИХ ПІДПИСІВ

У даний час в системах управління критичної інфраструктури все більше уваги приділяють проблемам захисту інформації. Одним з питань при цьому є використання порогових підписів. Тому актуальних питанням є проведення аналізу алгоритмів порогового підпису, їх порівняння з іншими схемами групових підписів та можливості практичного використання у інформаційних системах.

Схема підпису k з n – це протокол, який дозволяє будь-якій підмножині k гравців з n генерувати загальний підпис, але це виключає створення дійсного підпису, якщо в протоколі бере участь менше, ніж k гравців [1].

Проведенний аналіз показав, що практичне застосування групових підписів (підпис k з n) стримується широким колом їх недоліків:

1. відсутність жорстких доказів безпеки навіть у випадковій моделі оракулів;

2. генерація та (або) верифікація частки підпису є інтерактивною, крім того, вимагає синхронної мережі зв'язку;

3. розмір окремої частки підпису лінійно збільшується зі збільшенням кількості гравців.

Вирішення цих недоліків можливе при використанні порогових підписів. Пороговий підпис – це простий криптографічний метод генерації розподіленого ключа і підпису до нього, який має властивості [1]:

1. виключення можливості підробки часткового секрету, який по своїй суті є підписом;

2. створення та перевірка частки підписів повністю неінтерактивні;

3. розмір окремої частки підпису обмежений невеликим постійним значенням.

Ще одним недоліком схем розділення секрету є їх принципово одноразове використання, оскільки при реконструкції загального секрету, сам секрет стає відомим усім учасникам, що його відновлювали. Порогова криптографія дозволяє здійснювати більш багаторазовий підхід – згідно з яким достатній кворум учасників може погодитися використовувати секрет для виконання криптографічних обчислень, не обов'язково реконструюючи секрет у процесі.

Основна властивість порогових підписів полягає в тому, що приватний ключ ніколи не потрібно реконструювати. Навіть після багаторазового підписання ніхто не дізнається жодної інформації про приватний ключ, який дозволив би кожному окремо підписувати рішення без групування [2].

Проведений аналіз показав, що порогові підписи є більш гнучкими, порівнюючи з мультипідписами, у можливості змінювати політику доступу. Їх використання дозволяє застосувати багатосинхронну політику контролю доступу у здійсненні та завіренні деякого спільного рішення, що врешті буде публічно розголошено.

На практиці порогові підписи використовуються в блокчейн-клієнтах (наборах команд виконуваних повною нодою) для зміни процесу генерації створення ключів і підписів. Застосування саме даного підходу дозволяє вносити зміни для всіх команд, пов'язаних з розподіленими обчисленнями і приватним ключем.

Децентралізовані додатки, рішення масштабованості другого рівня, атомарні свопи, мікшування, успадкування та інші функції, які можуть бути реалізовані в рамках блокчейн технології все частіше заміняються криптографією на основі порогових підписів. Це дозволяє замінити дорогі і ризиковані всередині ланцюгові операції зі смарт-контрактами на більш дешеву і надійну альтернативу.

Таким чином, схеми порогових підписів є більш гнучкими та менш громіздкими, порівнюючи зі схемами підпису k з n.

В даний час порогові підписи активно використовуються у блокчейн-клієнтах, як потужний аналог мультипідписів, та у різноманітних корпоративних бізнес рішеннях.

Список використаних джерел

1. A. Boldyreva, «Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme,» in Public key cryptography – PKC

2003. Springer, 2002, pp. 31-46.
2. V. Shoup, «Practical threshold signatures,» in Advances in Cryptology – EUROCRYPT 2000. Springer, 2000, pp. 207-220.

Білий Б. Б. (ДНУЗТ)

УДОСКОНАЛЕННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ РОЗФОРМУВАННЯ-ФОРМУВАННЯ ЗАЛІЗНИЧНИХ СОСТАВІВ

У доповіді представлені результати досліджень і розробок, призначених для створення інтелектуальної інформаційної технології розформування-формування РФ багатогрупних складів. Основним завданням, яке забезпечує розробку інтелектуальної системи, є створення Бази знань шаблонів (БЗнШ) [2], які описують оптимальні процеси РФ составів певної структури. На основі зіставлення структур деякого вхідного в транспортну систему багатогрупного составу з шаблонами БЗнШ вибирається раціональна модель процесу РФ, без виконання операцій повного перебору варіантів.

У доповіді розглядається можливість використання шаблонів формування составу. Шаблон формування составу [2] - це структура узагальненого опису упорядкованих даних, що кодують інформацію про номери груп вагонів, за допомогою якого однозначно встановлюється список послідовності етапів по переміщенню вагонів на виділені для розформування-формування (РФ) шляху. Шаблон полегшує розуміння принципів формування і розформування составів, а також систематизує алгоритми цих процесів. Інтелектуальна технологія РФ дозволяє уникнути перерахунку схем сортування для подібних составів, а також для составів які відрізняються дійсними номерами груп (ДНГ)[1], але при цьому збігаються за скороченими логічними номерами груп (СЛНГ)[2].

У доповіді представлена базова структура інтелектуальної інформаційної технології формування багатогрупних составів доповнень детальної моделлю процесу пошуку шаблонів в базі знань. Систему пошуку шаблонів дозволяє працювати не тільки з декількома вагонів або групами вагонів, а визначати черговість составів на одному напрямі слідування. Також завдяки зберіганню в БЗнШ є можливість відстежувати хронологію переміщення вагону в составі і між составами. Пошук шаблону формування составу виконується шляхом порівняння СЛНГ вхідного составу з безліччю СЛНГ, які зберігаються в БЗнШ, а також шляхом його перетворення до раціонального виду. Перетворення шаблону в раціональний вид - це перетворення СЛНГ в логічні номери груп (ЛНГ)[1] з урахуванням кількості вагонів у структурі ЛНГ. Особливістю цього алгоритму пошуку є те що крім повних збігів він буде враховувати невеликі відмінності в структурі составу від збереженого шаблону в БЗнШ або генерувати новий шаблон комбінуючи існуючі в БЗнШ шаблони.

У доповіді запропонований інноваційний підхід до вирішення проблеми вдосконалення технологій і засобів формування многогрупних составів на сортувальних станціях. У дослідженні запропоновані структура і моделі інтелектуальної інформаційної технології, яка використовує для формування составів весь досвід реалізації цих процесів. Можливість переходу від окремого завдання формування составу технічно здійснюється за рахунок встановлення її зв'язку з раніше виконаними розрахунками шляхом створення баз даних і баз знань шаблонів структур составів і раціональних процедур РФ.

Список використаних джерел

1. Сковрон И. Я. Оптимизация выбора схемы формирования многогруппных составов //Восточно-Европейский журнал передовых технологий. – 2012. – №. 1 (3). – С. 20-26.
2. Скалозуб В. В., Белый Б. Б. Структура інтелектуальної інформаційної технології формування багатогрупних составів //Транспортні системи та технології перевезень. – 2019. – № 17. С. 62 – 69.

Meleshko V. V. (Ukrzaliznytsia)

UDC 621.331

DISTRIBUTION OF THE TRACTION CURRENT HARMONICS IN RAILS

В роботі розроблено математичну модель розподілу гармонік тягового струму в тяговій мережі при декількох транспортних засобах у фідерній зоні. Ця модель являє собою еволюцію і спрощення моделей, представлених раніше. Робота виконана з метою доказу електромагнітної сумісності нових поїздів, оснащених електронними статичними перетворювачами з існуючими лініями електропостачання і була використана при їх випробуваннях.

Keywords: *traction current harmonics, modelling, electromagnetic compatibility.*

To ensure the electromagnetic compatibility (EMC) of new types of rolling stock with signaling and radio communication systems, they are subjected to an acceptance procedure that includes the EMC tests in accordance with European and national regulatory standards and norms.

The aim of the work is to establish mathematical and computer model for distribution of traction current harmonics in AC direct feeding traction network with