УДК 004

М.Середа, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОЕКТУВАННЯ СЕРВІСІВ АВТЕНТИФІКАЦІЇ

У статті розроблено програмне забезпечення, яке призначено для системи проектування сервісів автентифікації. Метою розробки є дослідження та програмна реалізація системи проектування сервісів автентифікації. Об'єктом дослідження є процес проектування сервісів автентифікації. Предметом дослідження є методи проектування сервісів автентифікації. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи проектування сервісів автентифікації. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, автентифікація

Постановка проблеми. Проблема з паролями полягає в тому, що над ними дуже легко втратити контроль. Люди передають свої паролі іншим людям. Люди записують їх, а інші читають. Люди надсилають їх електронними листами, і ці листи перехоплюються. Люди використовують їх для входу на віддалені сервери, і їхні комунікації прослуховуються. Паролі також легко вгадати. І коли щось із цього трапляється, пароль більше не працює як маркер автентифікації, оскільки ви ніколи не можете бути впевнені, хто вводить цей пароль.

У даній магістерській роботі буде розглянута автентифікація з використанням електронних ключів, більш конкретно з використанням як ключ USB-накопичувача.

Сервіс автентифікації, який описаний у даній роботі, Secure WEB-Logon – це апаратна «двофакторна автентифікація», яка вирішує проблему пароля. USB-ключ Сервіс автентифікації – це апаратний ключ, який замінює незахищений метод входу «Ідентифікатор користувача + пароль» для рішень Інтернету або внутрішньої мережі. Аутентифікація виконується за допомогою шифрування даних всередині безпечного апаратного забезпечення Сервіс автентифікації. Зашифрований маркер автентифікації змінюється щоразу, коли надходить запит на вхід, щоб переконатися, що перехоплений маркер не можна використовувати двічі.

Єдиний варіант – скористатися спеціально розробленою в результаті виконання магістерської роботи системою автентифікації з використанням електронних ключів.

Основна перевага розробленої системи системи полягає в мінімальній перебудові IT-інфраструктури організації, мінімальні витрати на адміністрування, одночасної автентифікації в службах каталогу Windows і NetWare, підвищеної безпека мережі за рахунок використання "сильних" паролів і зберігання їх у захищеній пам'яті електронних ключів.

Крім цього, істотно знижується "людський фактор", оскільки користувач просто не знає пароля, тому не може його нікому передати або записати на папірці.

Безпека підсистем автентифікації не може бути перевірена експериментально в ході випробувань на функціонування. Крім того, через достаток криптографічних алгоритмів і різноманіття завдань автентифікації ці системи найчастіше проектуються «з нуля», що збільшує трудомісткість розробки. Алгоритмізація процесу проектування й обґрунтування прийнятих рішень дозволять уникнути типових помилок, а також порівнювати різні варіанти побудови алгоритмів автентифікації й вибирати найкращий з них.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи проектування сервісів автентифікації.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи проектування сервісів автентифікації.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем проектування сервісів автентифікації.
– Дослідження системи проектування сервісів автентифікації.
– Програмна реалізація системи проектування сервісів автентифікації.

Об'єктом дослідження є процес проектування сервісів автентифікації.

Предметом дослідження є методи проектування сервісів автентифікації.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод проектування сервісів автентифікації.

Розроблено вітчизняний продукт проектування сервісів автентифікації, який має більш широкі можливості, на відміну від існуючих аналогів.

Виклад основного матеріалу.

Сервіс автентифікації – надійна система безпеки для захисту вашого програмного забезпечення від несанкціонованого відтворення.

Сервіс автентифікації для USB-портів

Функціонально модулі Сервіс автентифікації серій MLU і MKU для USB-інтерфейсу ідентичні модулям ML і MK для підключення LPT, а також забезпечують захист програмного забезпечення для ноутбуків і ПК, які не мають паралелі. інтерфейс принтера.

USB-ключі Сервіс автентифікації підтримують HID-режим, що означає, що системний драйвер USB не потрібен.

Сервіс автентифікації для паралельних портів

Модулі Сервіс автентифікації серій ML і MK для інтерфейсу принтера просто підключаються до інтерфейсу LPT, де вони функціонують ідеально, не створюючи проблем для периферійних пристроїв, таких як принтер, сканер тощо, які підключені нижче.

Під час розробки особлива увага приділялася прозорій поведінці, високому ступеню безпеки завдяки використанню процесора RISC, простому підключенню до програмного забезпечення та високій надійності при практичному використанні.

Сервіс автентифікації Secure WEB-Logon базується на двох компонентах:

1. Сервіс автентифікації-ключ і WEB-Client – програма на стороні клієнта.

2. WEB-сервер на стороні постачальника

Коли користувачеві потрібно ввійти на сервер, сервер надсилає довільний запит. Користувач повинен підключити USB-ключ Сервіс автентифікації і ввести особистий PIN-код.

Запит сервера, PIN-код користувача та деякі інші блоки даних будуть зашифровані всередині захищеного матричного ключа. Потім зашифрований маркер результату надсилається назад на сервер.

Конфіденційна інформація, наприклад ключ шифрування, безпечно зберігається в ключі Сервіс автентифікації і на сервері, але ніколи не передається між сервером і клієнтом.

Сервіс автентифікації Secure WEB-Logon можна використовувати з усіма WEB-браузерами і не базується на файлах cookie, плагінах або аплетах Java.

На стороні клієнта програма WEB-клієнт (EXE) використовується для передачі запитів сервера на ключ Сервіс автентифікації.

Щоб мати можливість протестувати тут Сервіс автентифікації Secure WEB-Logon, вам потрібен ключ Сервіс автентифікації!

Виконайте наступні кроки:

1. Створіть WEB-клієнтську програму за допомогою інструменту «Сервіс автентифікації WEB-Logon Wizard».

2. Запустіть програму WEB-Cleint і підключіть Сервіс автентифікації до ПК.

Коли Сервіс автентифікації підключено до USB-порту, автоматично запускається Інтернет-браузер із WEB-сайтом.

3. Зареєструйте на сайті входу параметри вашого ключ і PIN-код на ваш вибір для цього тесту.

4. Після реєстрації продовжте, натиснувши [Вхід] за допомогою підключеного ключа та зареєстрований PIN-код.

Сервіс автентифікації пропонує все, що для вас найважливіше:

– Кросплатформенність (Windows, Linux, Mac) без власних USB-драйверів.

– Істотно зменшує ваші зусилля з підтримки, оскільки він працює одразу після підключення без встановлення будь-яких USB-драйверів.

– Абсолютна надійність (10 років гарантії).

– Доступні кілька розмірів пам'яті.

– Програмний API, інструменти та підтримка безкоштовні.

– Найвища якість за розумною ціною.

– Сертифікований ISO.

– Два різних розміри корпусу (довгий або короткий) з однаковими технічними характеристиками за однаковою ціною.

Дуже відповідні інструменти для керування вашими ліцензіями:

– Просте впровадження API у ваших 16-, 32- та 64-розрядних програмах.

– Автоматичний захист файлів EXE.

– 64-розрядний API для Windows і Linux уже доступний.

– Віддалене оновлення: легко оновлюйте ключі безпосередньо у своїх клієнтів. Також доступний як інтеграція API у вашу систему керування клієнтами.

– Безпечний WEB-вхід для автентифікації користувача у ваших Інтернет- та Інтранет-додатках.

– Управління мережевими ліцензіями без додаткової плати.

– Той самий ключ можна використовувати локально або в мережі.

– Ліцензування мережі на основі TCP/IP доступне як приклад із відкритим кодом.

– Той самий ключ можна використовувати для захисту програмного забезпечення та/або WEB-автентифікації.

Сервіс автентифікації пропонує вищий ступінь безпеки:

– Шифрування відбувається повністю всередині апаратного забезпечення.

– Сучасна техніка, яка використовується для «Анти-Клонування-Безпека».

– Захист файлів EXE від налагодження та зворотного проектування. Також виконувані файли .NET v1.0, 1.1 і 2.0 підтримуються та захищені технологією «Anti-Process-Dump».

– Anti-Hacker-Lock ключ перестане працювати під час атаки.

– 128-бітне шифрування та дешифрування даних.

– Зберігання 128-бітних ключів, визначених вами, які неможливо прочитати з ключа.

– Використання «одноразових ключів», які дійсні лише для однієї послідовності шифрування/дешифрування.

– До 16 різних 128-бітних алгоритмів шифрування.

– Пам'ять серії MK/MKU захищена від запису та може бути змінена лише за наявності захисного ключу MasterKey-Dongle.

Технологія OTP

У сучасному цифровому середовищі, що швидко розвивається, безпека залишається головним пріоритетом для будь-якої платформи. Для забезпечення безпечної роботи користувача та захисту конфіденційних даних клієнтів необхідна надійна система

автентифікації користувачів. У цій вичерпній технічній статті ми розробимо вдосконалену систему автентифікації користувачів, яка використовує перевірку на основі OTP (одноразового пароля) для входу користувача та використовує JWT (веб-токени JSON) для авторизації користувачів. Крім того, ми запровадимо керування доступом на основі ролей, щоб надати користувачам доступ до певних ресурсів на основі їхніх призначених ролей і областей ролей. Ми також вивчимо обмеження швидкості та кешування OTP, щоб захистити систему від атак грубої сили та оптимізувати керування OTP.

Розуміння JWT, OTP і доступу на основі ролей користувача

JWT (веб-токени JSON):

JWT – це компактний, URL-безпечний формат маркера, який надійно представляє претензії між двома сторонами. Підпис забезпечує цілісність токена. JWT не мають статусу, і їх можна перевірити, не покладаючись на серверне сховище. Вони широко використовуються для автентифікації та авторизації в сучасних веб-додатках завдяки своїй ефективності та безпеці.

OTP (одноразовий пароль):

OTP – це одноразовий пароль з обмеженим часом, який зазвичай надсилається користувачеві через SMS, електронну пошту чи інші безпечні канали. Він забезпечує додатковий рівень безпеки, гарантуючи, що пароль користувача дійсний лише протягом короткого періоду часу та не може бути використаний повторно. OTP зазвичай використовуються для двофакторної автентифікації (2FA) і процесів скидання пароля. Використовуючи вхід на основі OTP, система автентифікації додає додатковий захід безпеки для перевірки ідентичності користувачів.

Доступ на основі ролей користувача:

Контроль доступу на основі ролей користувача визначає дозволи та обмеження, надані користувачам на основі їхніх призначених ролей. Кожна роль пов’язана з певними привілеями, які визначають, до яких дій і ресурсів може отримати доступ користувач. Цей підхід допомагає застосувати принцип найменших привілеїв, гарантуючи, що користувачі можуть отримати доступ лише до ресурсів, необхідних для виконання їхніх завдань. Впроваджуючи доступ на основі ролей користувача, система може ефективно та безпечно керувати контролем доступу, запобігаючи несанкціонованому доступу та потенційному витоку даних.

Мета реалізації

Поєднання JWT, OTP і доступу на основі ролей користувача слугує для створення надійної та безпечної системи автентифікації користувачів.

1. Токени JWT забезпечують безперебійний і безпечний метод авторизації користувачів, забезпечуючи доступ до ресурсів лише дійсним користувачам із підтвердженими претензіями. Природа без збереження стану усуває потребу в сховищі на стороні сервера, що робить його масштабованим і ефективним.

2. Вхід на основі OTP додає додатковий рівень безпеки, зменшуючи ризик несанкціонованого доступу через зламані паролі. Одноразові паролі обмежені за часом і можуть використовуватися лише один раз, покращуючи автентифікацію користувачів.

3. Доступ на основі ролей користувача гарантує, що користувачам надаються відповідні дозволи на основі їхніх ролей. Цей детальний контроль доступу обмежує доступ до критично важливих ресурсів, захищаючи конфіденційні дані та запобігаючи можливому зловживанню.

Інтегруючи ці технології, онлайн-платформи можуть підвищити рівень безпеки, завоювати довіру користувачів і захистити їхні цінні активи. Система автентифікації захищає від поширених загроз, таких як атаки грубої сили, неавторизований доступ і вразливість паролів, створюючи безпечне та надійне середовище для впевненої взаємодії користувачів.

Уразливості технологій ОТР

Технологія одноразових паролів вважається досить надійною. Однак об'єктивності заради відзначимо, що й у неї є свої недоліки, яким піддані всі системи, що реалізують принцип ОТР у чистому виді.

Деякі атаки застосовні тільки до окремих способів реалізації технології одноразових паролів. Для приклада можна знову взяти метод синхронізації по таймері. Як ми вже говорили, час у ньому враховується не з точністю до секунди, а в межах якогось установленого заздалегідь інтервалу. Це необхідно для обліку можливості розсинхронізації таймерів, а також появи затримок у передачі даних. І саме цим моментом теоретично може скористатися зловмисник для одержання несанкціонованого доступу до віддаленої системи. Для початку хакер "прослуховує" мережний трафік від користувача до сервера автентифікації й перехоплює відправлені "жертвою" логін і одноразовий пароль. Потім він відразу блокує його комп'ютер (перевантажує його, обриває зв'язок і т.п.), а сам відправляє авторизаційні дані вже від себе. І якщо він встигне зробити це так швидко, щоб інтервал автентифікації не встиг змінитися, то сервер визнає його за зареєстрованого користувача.

Розробка структурної схеми

Спершу розглянемо питання розробки методології формування процесу автентифікації. Найважливішою частиною підсистеми автентифікації є сукупність алгоритмів автентифікації, які задають набір захисних функцій, що визначають, що й при яких умовах може бути захищено.

Таблиця 1 – Упорядкованість захисних функцій автентифікації

Координати захисних функцій	**Упорядкованість**
Тип автентифікації	автентифікація повідомлення ⊇ упізнавання
Число сеансів на одному ключі	багаторазова автентифікація ⊇ однократна автентифікація
Тип використовуваного каналу зв'язку (можливість діалогу)	бездіалогова автентифікація ⊇ діалогова автентифікація
Довіра до верифікатору	недоверенный верифікатор ⊇ довірений верифікатор
Якість зв'язку (при однократної автентифікації потрібне надійне доведення інформації)	некритичність надійного доведення інформації ⊇ необхідність надійного доведення інформації
Наявність служби єдиного часу (необхідно для захисту від повторів або затримок інформації при бездіалогової автентифікації)	необов'язковість єдиного часу ⊇ наявність єдиного часу
Відносний обсяг переданої службової інформації (відношення обсягу переданих даних до ентропії	менший відносний обсяг службової інформації ⊇ більший відносний обсяг службової інформації

У роботі до складу алгоритмів автентифікації включені:

– власно протоколи автентифікації;

– швидкі алгоритми, що реалізують обчислення у відповідних математичних структурах;

– допоміжні алгоритми, що впливають на безпеку;

– алгоритми вибору параметрів підсистеми автентифікації;

– алгоритми керування ключами, включаючи зміну параметрів підсистеми автентифікації.

Стандартні алгоритми автентифікації не завжди задовольняють вимогам, пропонованим до критичних інформаційно-телекомунікаційних систем, тому з'являється необхідність проектування оригінальних алгоритмів автентифікації.

Безпека цих алгоритмів традиційно ґрунтується на складності рішення математичного завдання, для вибору якого в ході проектування пропонується трьохрівневасистематизація завдань.

До першого рівня віднесені класи уніфікованих математичних завдань (КУМЗ), у якості яких запропоноване розглядати наступні типи завдань, орієнтованих на побудову алгоритмів автентифікації:

– завдання про виконуваність (до якої зводяться завдання розкриття ключа, обіги й обчислення колізій хеш-функції);
– завдання визначення структури й порядку кінцевої групи;
– завдання обчислення індексу елемента кінцевої абелевої групи;
– завдання про укладання ранця;
– завдання обчислення морфізма між об'єктами категорії.

До другого рівня віднесені масові основні математичні завдання вибору (ОМЗ), отримані в результаті параметризації КУМЗ за допомогою математичних структур, що визначають область математики, до якої відноситься ОМЗ, а також класи зв'язаних завдань, до яких зводиться ОМЗ. Крім завдань вибору при дослідженні безпеки використовуються також додаткові завдання розпізнавання й пошуку.

До третього рівня віднесені приватні математичні завдання, що відповідають масовій ОМЗ.

Проектування алгоритмів автентифікації (рисунок 1) пропонується формально визначати як процес побудови ланцюжків відображень:

– {Класи уніфікованих математичних завдань} × {уніфіковані криптографічні примітиви} →{мінімізований набір захисних функцій} → {узагальнені протоколи автентифікації};

– {Класи уніфікованих математичних завдань} × {математичні структури} → {Основні математичні завдання} ∪ {додаткові завдання};

– {Основні математичні завдання} × {узагальнені протоколи автентифікації} → {алгоритми автентифікації} → {швидкі обчислювальні алгоритми};

– {Основні математичні завдання} ∪ {додаткові завдання} → {алгоритми генерації параметрів підсистеми автентифікації} → {частки математичні завдання} → {алгоритми керування ключами}.

Уніфіковані криптографічні примітиви містять у собі: симетричне шифрування, шифрування з відкритим ключем, безключову й ключову хеш-функцію, цифровий підпис, діалогові й бездіалогові докази з нульовим розголошенням знань, секретні гомоморфізми. Безлічі математичних завдань і криптографічних примітивів варто розглядати в їхньому розвитку.

При проектуванні алгоритмів автентифікації потрібно прогнозувати як зниження складності математичного завдання, так і ріст продуктивності обчислювальної техніки, що дозволяє вирішити це завдання, а також розвиток інших (не зв'язаних безпосередньо з обчисленнями) можливостей порушника, спрямованих на зниження безпеки.

Швидкість $s(t,T)$ падіння стійкості $S(t)$ на інтервалі часу $(T,\ T+t)$ запропоновано визначати по формулі:

$$s(t,\ T) = (\log S(T) - \log S(T+t))/(t \log S(T)).$$

Показано, що складність завдань падає приблизно з постійною швидкістю. Отримані оцінки дозволяють прогнозувати зниження складності й визначати час життя ключа.

Завдання, покладені в основу безпеки алгоритмів автентифікації, пропонується класифікувати по трьох типах: вибір, розпізнавання, пошук. У ході проектування звичайно

потрібно обґрунтувати складність завдання вибору й знайти або оцінити рішення завдань розпізнавання й пошуку.

Математичні структури, використовувані при проектуванні алгоритмів автентифікації в умовах довіреного верифікатора, як правило, не мають ефективно розв'язні алгебраїчні властивості й розрахункові статистичні характеристики. Це викликає необхідність введення додаткових завдань і обумовлює їхню складність.

Для автентифікації в умовах недовіренного верифікатора використовуються математичні структури з розпізнаваними алгебраїчними властивостями (групи, кільця, категорії) і відповідні ОМЗ.

На підставі аналізу особливостей застосування ОМЗ сформульовані вимоги до ОМЗ і відповідних класів зв'язаних завдань (КЗЗ), до яких поліномиально зводиться завдання порушення безпеки.

Для параметризації й рішення завдання проектування алгоритмів автентифікації пропонується чотирьохрівнева схема (рисунок 2), що характеризується, крім традиційного технічного рівня, наявністю математичного, криптографічного й сертифікаційного рівнів.

Математичний рівень є найбільш специфічним, у значній мірі визначає трудомісткість проектування, вимагає високої наукової кваліфікації виконавців і із цієї причини не може бути ефективно розпаралелений.

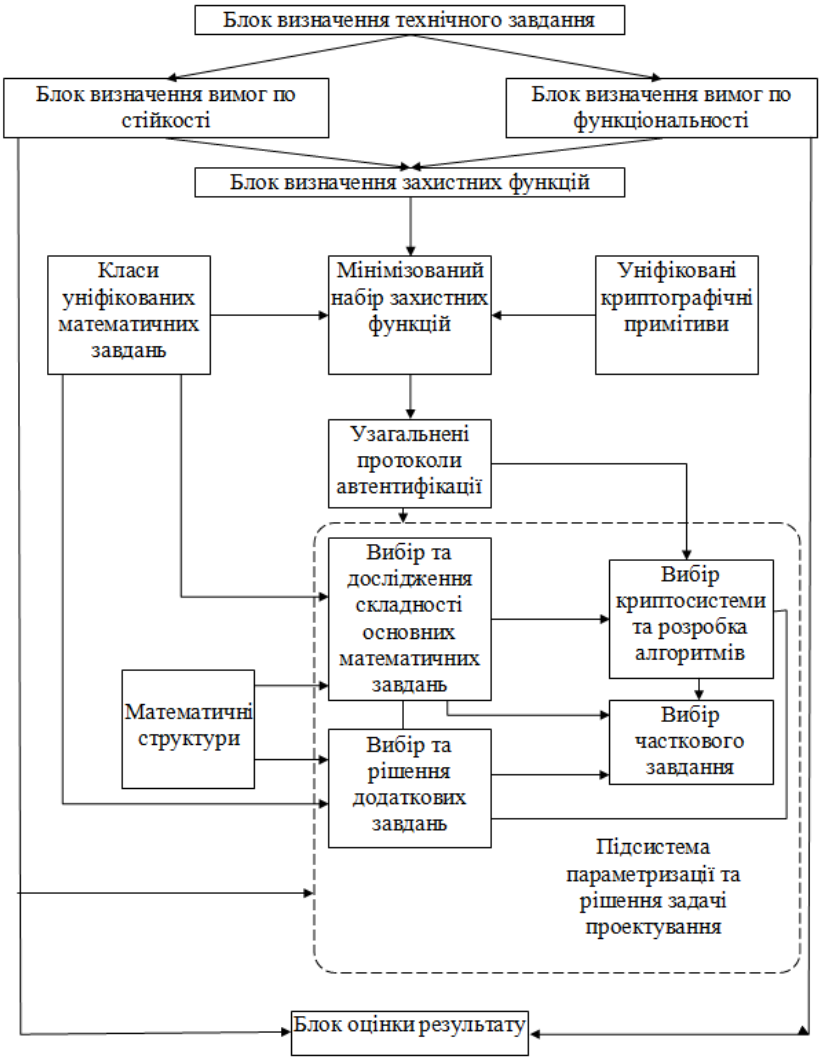

Рисунок 1 – Структурна схема системи проектування алгоритмів автентифікації

Розглянувши запропоновану методологію побудови систем автентифікації перейдемо до практичної побудови системи автентифікації з використанням наведених вище теоретичних відомостей.

За основу системи автентифікації візьмемо автентифікацію з одноразовим паролем з застосуванням USB-ключа.

Структурна схема такої системи наведена на рисунку 1.

З неї ми бачимо, що існують дві сторони процесу автентифікації. З однієї сторони це ЕОМ з операційною системою, у якій встановлений драйвер USB-ключа. З іншої сторони це користувач з USB-ключем, який потребує процесу автентифікації для доступу до системи.

На стороні ПЕОМ, крім драйвера USB-ключа, існує:

- Блок генерування частини одноразового паролю.
- Блок автоматичної генерації паролю.
- Блок перевірки ПІН-кода доступу до USB-ключа користувача.
- Блок синхронізації по часу.
- Блок підрахунку кількості повторів.
- Блок журналювання.
- Блок вибору методу автентифікації.
- БД користувачів з визначенням їх прав доступу.

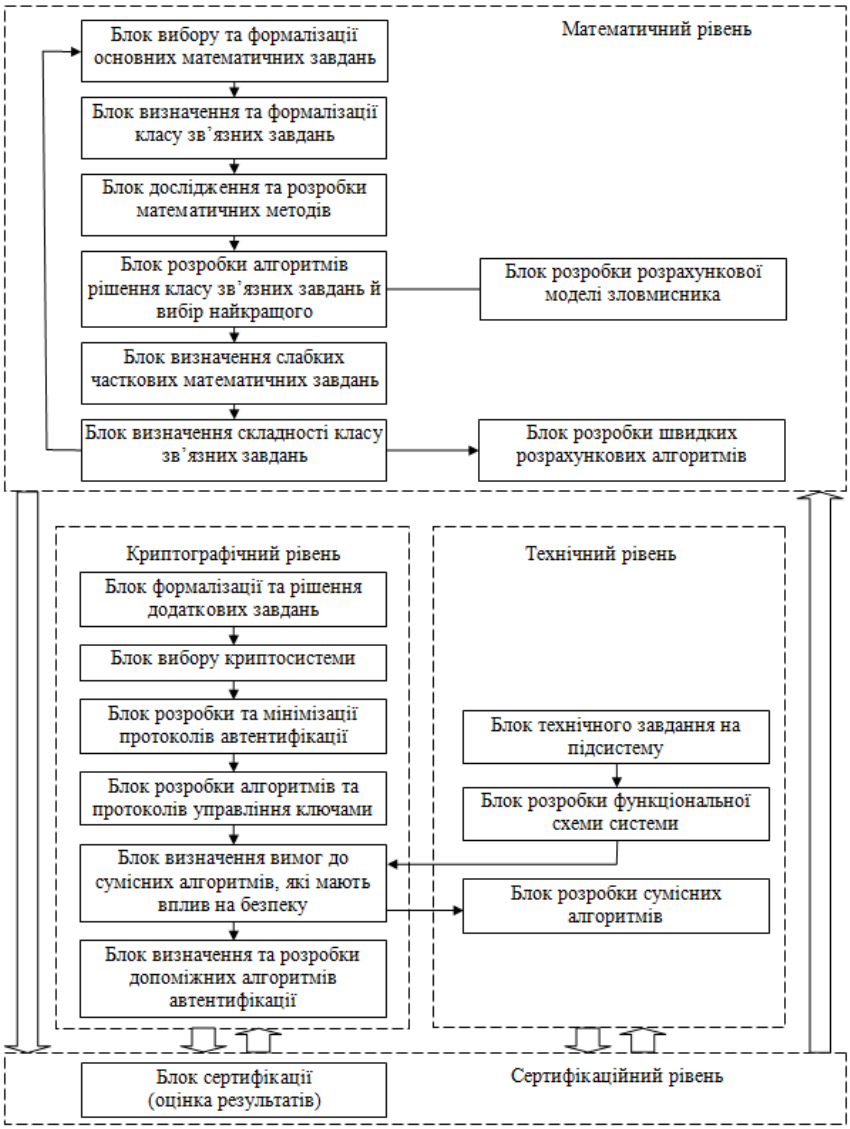

Рисунок 2 – Структурна схема системи параметризації та рішення завдання проектування

На стороні флеш-накопичувача існує:

- Блок криптографічних перетворень.
- БД параметрів користувача.

Процедура автентифікації відбувається наступним чином:

1. На ПЕОМ встановлюється драйвер USB-ключа.

2. Користувач під’єднує при вході у систему USB-ключ, для початку процедури автентифікації.

3. Система видає запит ПІН-коду доступу до USB-ключа.

4. Після введення ПІН-коду, видається вікно у якому потрібно ввести логін та пароль, необхідний для виконання процедури автентифікації й допуску користувача до системи.

5. Після введення паролю, на його основі формується у блоці генератора ключів пароль, частина якого відсилається до флеш-накопичувача.

6. Програмне забезпечення, встановлене на флеш-накопичувачі, згідно заданих таємних криптографічних алгоритмів перетворює цю частину ключа й надсилає відповідь.

7. На ПЕОМ відбуваються аналогічні перетворення, які заносяться у зашифрованому вигляді, до БД користувачів, та паролів.

8. Отримані з флеш-накопичувача дані порівнюються, з тими, які записані у БД.

9. Якщо дані співпадають, то користувач отримує доступ до системи з наданими йому правами. У іншому випадку, надається відмова у доступі.

Кількість повторів обмежується трьома спробами. Усі дії заносяться до журналу подій (у лог-файл). У випадку підозрілих дій видається сигнал адміністраторові ПЕОМ.

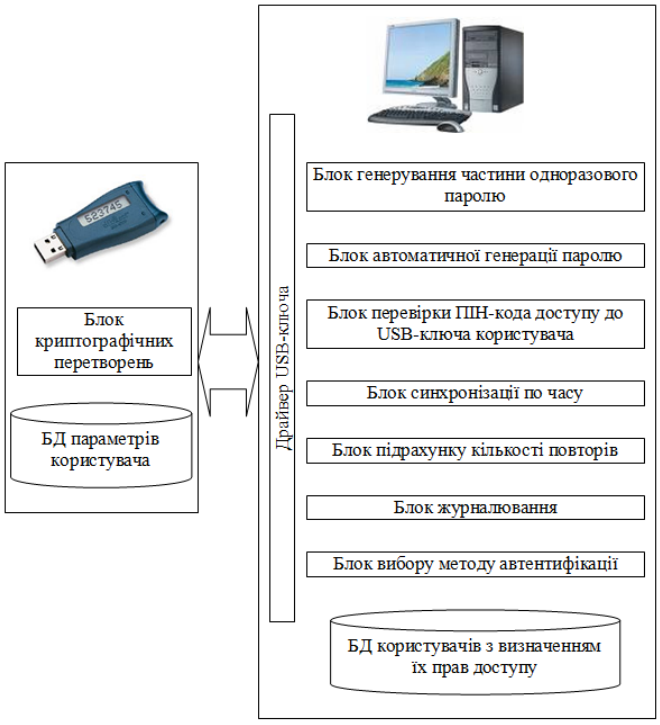

Рисунок 3 – Структурна схема системи автентифікації з використанням USB-ключа

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проектування сервісів автентифікації. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем проектування сервісів автентифікації. Досліджена система проектування сервісів автентифікації. На основі отриманих результатів досліджень створена програмна реалізація системи проектування сервісів автентифікації. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання проектування сервісів автентифікації. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143 (Scopus).
2. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207. (Scopus).
3. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58. (Scopus).
4. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256. (Scopus).
5. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114. (Scopus).
6. Smirnov O.A., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346. (Scopus).
7. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131. (Scopus).
8. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14. (Scopus).
9. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84. (Scopus).
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587. (Scopus).
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136. (Scopus).
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379. (Scopus).
13. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43. (Scopus).
14. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645. (Scopus).
15. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus).
16. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407. (Scopus).
17. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019. (Scopus).
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019. (Scopus).
19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629. (Scopus).
20. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 873-884. (Scopus).