ПРЕЗЕНТАЦІЯ ДИПЛОМНОЇ РОБОТИ НА ТЕМУ: РОЗРОБКА ЗАСОБУ ДЛЯ ЗАХИСТУ ПРОГРАНМОГО ЗАБЕЗПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО ВИКОРИСТАННЯ

Виконав: студент групи ЗІ-15сп
Маєвський Максим Іванович
Керівник роботи:
Куперштейн Л.М.

Мета роботи

Мета дипломної роботи полягає покращенні захисту програмного забезпечення від несанкціонованого використання. Для досягнення мети необхідно об’єднати існуючі методи захисту від несанкціонованого доступу в одному засобі, що дозволить створити ефективніший засіб захисту від несанкціонованого використання.

Відповідно до мети завданнями дипломної роботи є:

- проаналізувати літературні джерела за напрямком дослідження;
- виконати аналіз методів захисту програмного забезпечення;
- запропонувати методи та алгоритми захисту програмного забезпечення;
- розробити модуль, що реалізує запропоновані методи;
- протестувати розроблене програмне забезпечення.

Аналіз стану проблеми

На сьогодні, в зв’язку з поширенням інформаційних технологій в суспільстві, набуває актуальності проблема захисту інтелектуальної власності програмного забезпечення (ПЗ). Основною метою захисту є: захист від несанкціонованого використання, заборона доступу до функціоналу програми, протидія протиправному втручанню в код програмного засобу. Одним з перспективних напрямків є введення процедури аутентифікації та авторизації користувача у системі.

Порівняльний аналіз аналогів

- Одним з найбільш відомих аналогів є сервер авторизації vGate R2[3]. Сервер авторизації - це основний компонент vGate R2, який здійснює авторизацію і аутентифікацію користувачів, без якого не можна буде адмініструвати середу VMware vSphere, якщо він раптом вийде з ладу. Він виконує наступні функції:
- - централізоване управління СЗІ vGate;
- - аутентифікація користувачів і комп'ютерів;
- - розмежування доступу до засобів управління віртуальною;
- - інфраструктурою;
- - реєстрація подій безпеки;
- - зберігання даних;
- - реплікація даних з основного на резервний сервер авторизації.
- Це платний програмний продукт, вартість якого за один екземпляр програми становить близько 14 000 гривень.

Порівняльний аналіз аналогів

- Jasig - інший не менш відомий аналог. Jasig CAS (Central Authentication Service) - це веб-додаток, написаний на Java[4]. Щоб почати ним користуватися, майже нічого не треба робити. Потрібно лише завантажити, налаштувати, запустити та налаштувати клієнтів. Додаток безкоштовний для використання та має відкритий вихідний код.

Порівняльний аналіз аналогів

- Kerberos – ще один аналог серверу аутентифікації, розроблений у 1980-у році в Массачусетському технологічному інституті[5]. Його функціонал полягає у забезпеченні авторизації користувачів у мережі за допомогою унікального електронного ключа, що є у кожного з них. Тобто він є посередником між усіма клієнтами та сервером, що виконує основний функціонал. Це безкоштовна система, яку можна завантажити з офіційного сайту.

Аналіз методів розв’язання поставленої задачі

Поняття аутентифікації та авторизації.

Аутентифікація - процедура перевірки автентичності, наприклад[14]:

- перевірка справжності користувача шляхом порівняння введеного їм логіна з паролем, збереженим в базі даних користувачів;

- підтвердження справжності електронного листа шляхом перевірки цифрового підпису листи з відкритого ключа відправника;

- перевірка контрольної суми файлу на відповідність сумі, заявленої автором цього файлу.

Авторизація – це надання певній особі або групі осіб прав на виконання певних дій; а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій.

Методи аутентифікації

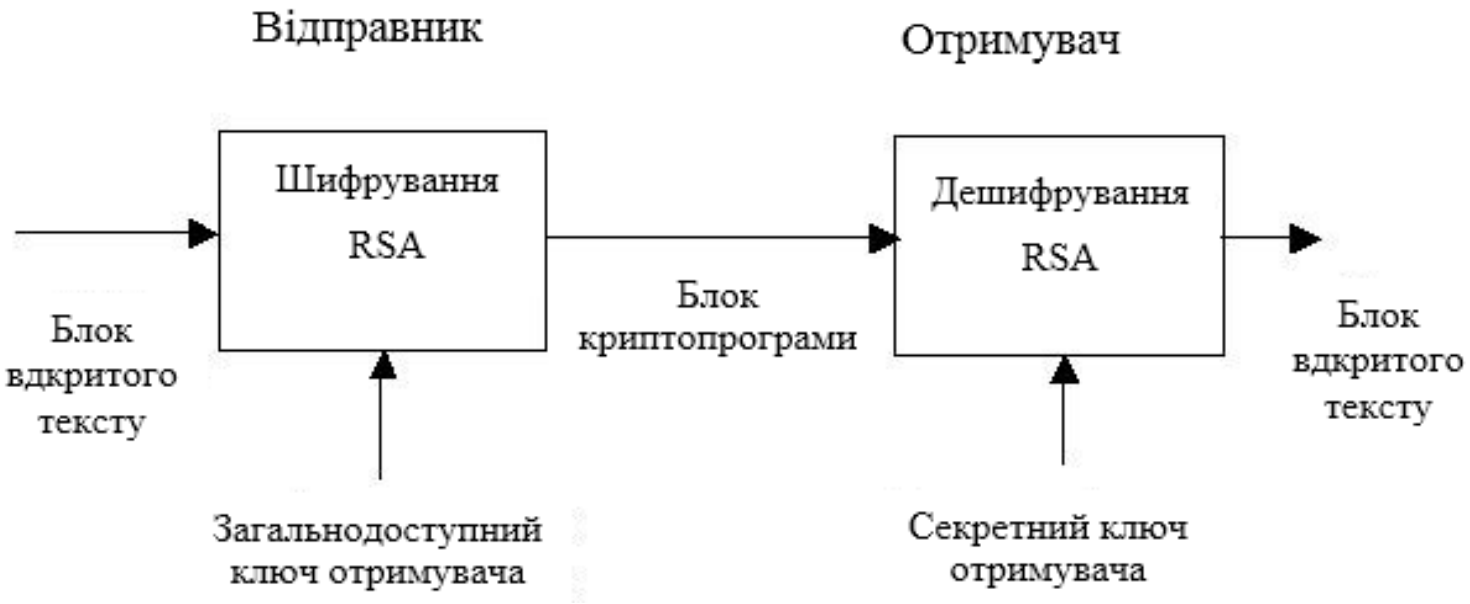
- **за допомогою електронного підпису;**
- **за допомогою введення зв'язки логін-пароля;**
- **за одноразовими паролями;**
- **за допомогою SMS ;**
- **біометрична аутентифікація;**
- **за допомогою GPS ;**
- багатофакторна аутентифікація.

Порівняння існуючих засобів захисту програмного забезпечення

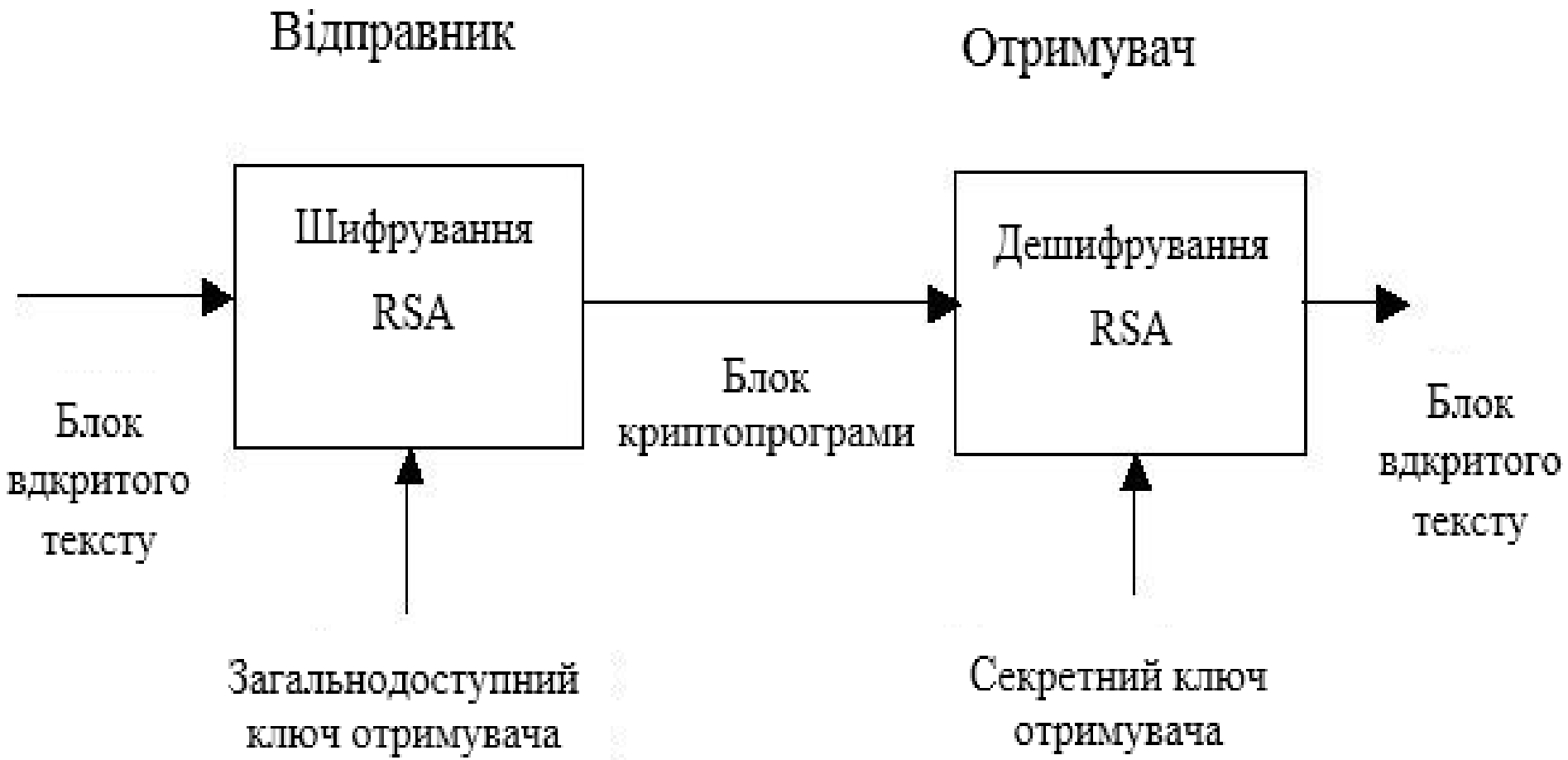
Засіб захисту	Переваги	Недоліки
Демо-версії програмного забезпечення	Неможливість використання можливостей через відсутність коду їх реалізації	Необхідно створювати окрему версію продукту
Захист обмеженням часу	Проста реалізація	Легко піддається взлому
Захист з використанням серійного номера	Проста реалізація	Залежить від фізичної конфігурації комп'ютера, незручний для користувача
Використання унікальних ідентифікаторів носія програмного продукту	Надійність роботи, так як дані зберігаються у зашифрованому вигляді на пристрої (наприклад, оптичному диску), та не можуть бути змінені	Залежність від фізичних параметрів комп'ютера та носія програмного продукту
Навісні захисти	Комбінують декілька існуючих способів захисту	Існує багато утиліт для обходу більшості з існуючих захистів
Захист за допомогою електронних ключів	Дуже складні для взлому	Висока вартість
Захист за допомогою аутентифікації користувача	Існує можливість комбінувати різні засоби перевірки автентичності	Можливість фізичної крадіжки даних користувача

RSA-шифрування

- RSA належить до так званих асиметричних алгоритмів, у яких ключ шифрування не збігається з ключем дешифрування[21]. Один з ключів доступний всім (так робиться спеціально) і називається відкритим ключем, інший зберігається тільки у його господаря і невідомий нікому іншому. За допомогою одного ключа можна робити операції тільки в одну сторону. Якщо повідомлення зашифровано за допомогою одного ключа, то розшифрувати його можна тільки за допомогою іншого. Маючи один з ключів неможливо (дуже складно) знайти інший ключ, якщо розрядність ключа висока.

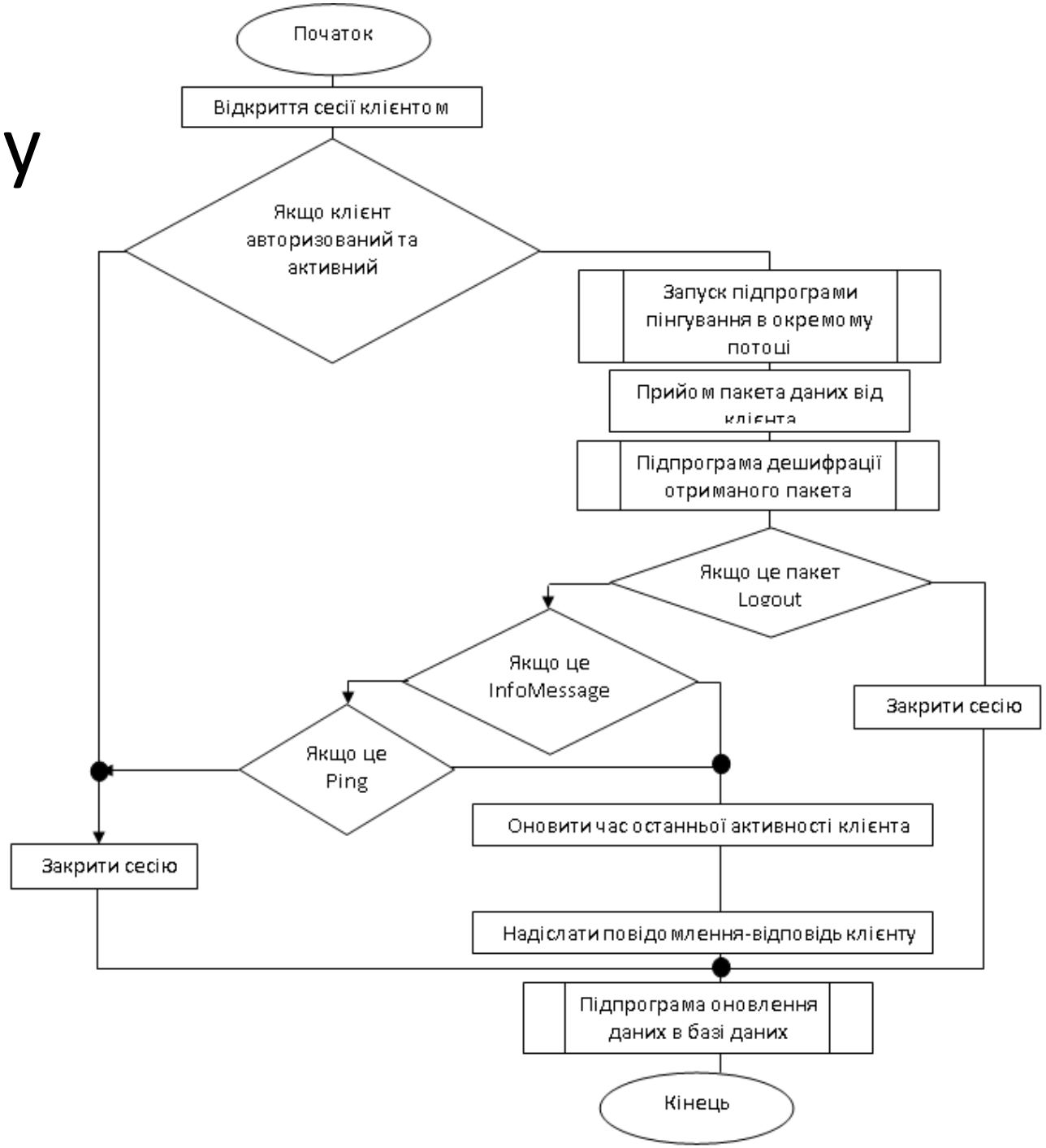


Узагальнена схема програмного комплексу



Загальний алгоритм роботи аутентифікації на сервері авторизації

Алгоритм роботи засобу захисту



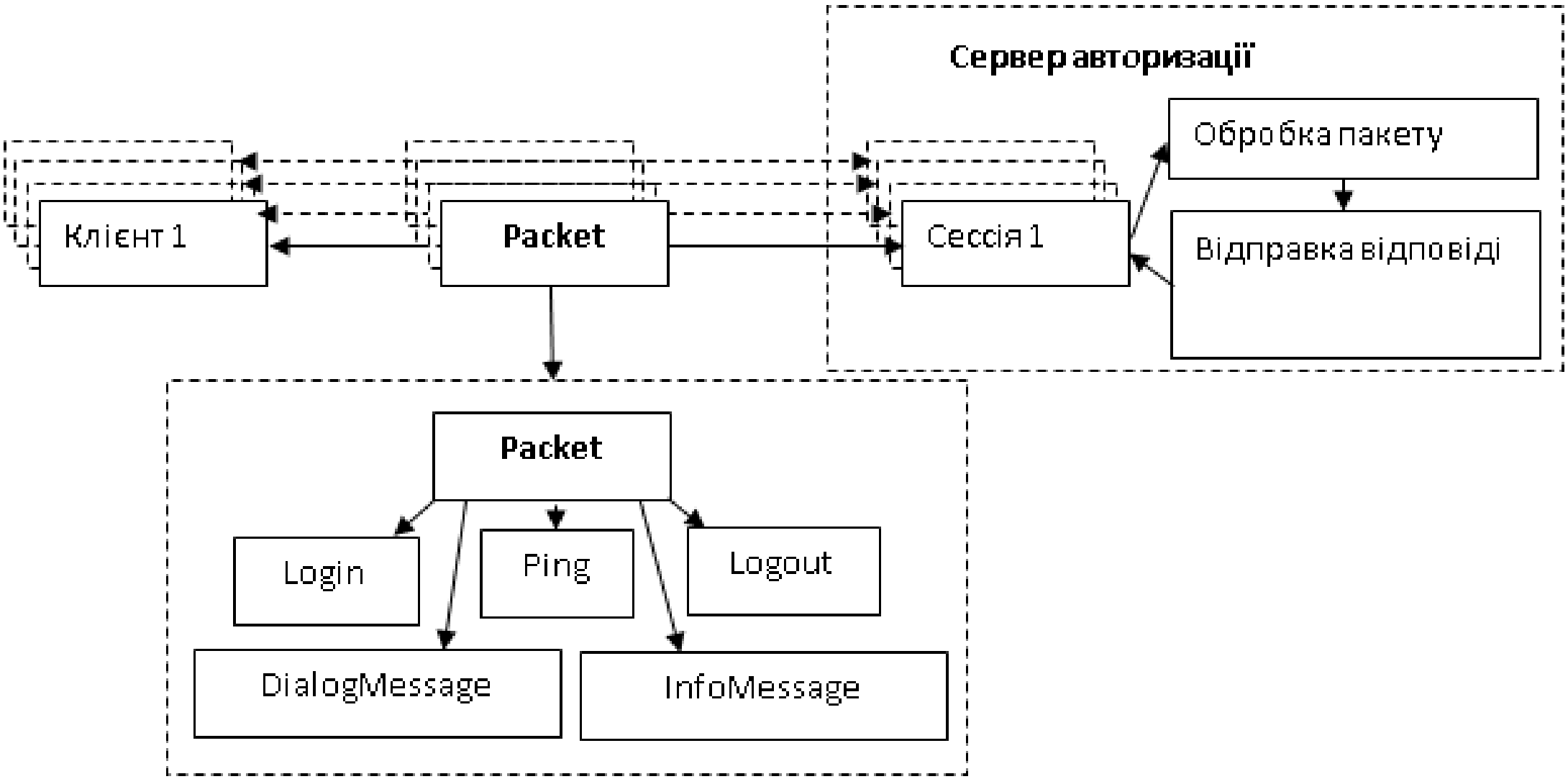
Пакети даних програмного засобу

- Типи пакетів даних у розробленому протоколі:
- Login – для передачі ключа авторизації та отримання зворотної інформації з сервера про успішність операції.
- Logout – для передачі команди про відключення клієнта від сервера.
- Ping – для визначення активності клієнта та відключення від сервера, у разі відсутності відповіді.
- DialogMessage – для передачі повідомлення про можливі збої під час передачі даних та інше.
- InfoMessage – для передачі на сервер поточного стану клієнта.

Структура пакету

Байти	0 - 4	5 - 8	9 - 12
0…8	VERSION	…	
9…16	COMMUNICATION_SERVER_ID	…	
17…32	SERVER_SERIAL	…	
33…40	SERVER_RESERVATION_1	…	
41…48	SERVER_RESERVATION_2	…	
49…56	CLIENT_SERIAL	…	
57…64	CLIENT_RESERVATION_1	…	
65…72	CLIENT_RESERVATION_2	…	
73…80	MESSAGE_ID	…	…
81…96	TIME	…	…
97…	Тіло пакета	…	…

Схема сесій


Сервер авторизації
Обробка пакету
Клієнт 1
Packet
Сессія 1
Відправка відповіді
Packet
Login
Ping
Logout
DialogMessage
InfoMessage

Висновки

- Досліджено багато методів захисту програмного забезпечення від шкідливого впливу хакерства. Опрацьована література дала можливість дослідити позитивні та негативні якості використання цих методів. Їх недоліки були враховані, а як результат було обрано сервер авторизації.
- Головною метою було розробити комплексний захист, при якому буде декілька змішаних типів захисту, через які зловмисникам було б дуже складно досягти своєї мети, або ж, як мінімум, це було невиправданим зайняттям, як по часу, так і по вартості. Була вирішена проблема доступу до ресурсів системи користувачами, які не мають на це права. Реалізований реальний засіб для захисту від несанкціонованого використання програмних засобів, який разом з іншими засобами захисту, зробить систему надійно захищеною від хакерів.

ДЯКУЮ
ЗА УВАГУ!