

# СТВОРЕННЯ ЗАХИЩЕНИХ ФАЙЛООБМІННИХ ВЕБ-СЕРЕДОВИЩ ДЛЯ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS SERVER

Вінницький національний технічний університет

## *Анотація*

*Протягом кількох десятиліть поспіль спостерігається сумна зростаюча статистика витоків даних з корпоративних файлообмінних сховищ. Втрата корпоративних даних може серйозно нашкодити діловій репутації підприємства, а також понизити рівень довіри. Сучасні рішення для корпоративного сектору в шифрування файлів зазвичай є складними у налаштуванні або вимагають покупки кошовної ліцензії. Саме тому варто здійснювати пошук шляхів для створення продукту, який в достатній мірі буде позбавлений подібних недоліків. Розроблено вимоги для створення захищених середовищ без використання пропрієтарних рішень для шифрування на базі ОС Windows.*

**Ключові слова:** веб-сервіси, засоби шифрування, захист даних, файлообмінні сервіси, Windows Server

## *Abstract*

*For several decades along there has been a sad growing statistic of data leakage from corporate file-sharing repositories. Loss of corporate data can seriously damage a company's business reputation and cause trust reduction. Modern solutions for the corporate sector for file encryption are usually difficult to set up or require the purchase of an expensive license. That is why it is worth looking for ways to create a product that will be sufficiently devoid of such shortcomings. Requirements have been developed for creating secure environments without the use of proprietary solutions for encryption based on Windows.*

**Keywords:** web services, encryption tools, data protection, file sharing services, Windows Server

## **Вступ**

Сучасні корпоративні файлообмінні сервіси досить часто піддаються вірусним атакам, через які може відбуватись витік даних. Необхідність розробки вимог для створення захищених файлообмінних веб-середовищ під ОС Windows обумовлена тим, що більшість сучасних програм-шифрувальників розраховані саме на платформу Windows [1, 4]. З використанням інфікування методом хробаків у подібного програмного забезпечення існують досить великі шанси [2] інфікування застарілої серверної інфраструктури на базі Windows Server, особливо при використанні недостатньо захищеної технології доменів Active Directory.

Підґрунтям для створення захищеного файлообмінного веб-середовища має стати розробка вимог при проектуванні подібного ПЗ. Саме на цьому етапі варто визначити основні вимоги до архітектури, резервного копіювання та шифрування.

## **Розробка вимог**

Розробка вимог для створення захищених файлообмінних веб-середовищ під ОС Windows передбачає водночас як врахування особливостей архітектури, резервного копіювання та шифрування, так і конкурентні переваги, які дозволять створити по справжньому конкурентноздатний продукт як для

підприємств-інтеграторів, так і для кінцевих користувачів. При розробці вимог варто ознайомитись з найбільш сучасними розробками у сфері захисту файлів [3, 4, 5].

Для реалізації програмного продукту передбачено використання мови програмування C++. Для створення передбачається використання технології багатопотоковості, де кожна з дій потоку виконується послідовно одна за одною без змоги перервати процес створення. При проектуванні додатку було застосовано послідовний засіб кодування. Послідовний засіб кодування – формування коду класифікаційного групування чи об'єкту класифікації з використанням кодів послідовно розміщених підпорядкованих групувань, що одержують при ієрархічному засобі класифікації, та його присвоєння.

Під час розробки мають бути досягнені наступні цілі:

- створити модуль HTTP-серверу з можливістю налаштування аліасів директорій (рис. 1);
- створити простий та зрозумілий графічний інтерфейс для управління та конфігурування HTTP-серверу;
- створити модуль резервного копіювання за допомогою технології rsync;
- виконати тестування програмного додатку з перехопленням мережевого трафіку [6];
- виконати написання інструкції користувача програмного додатку HTTP-серверу.

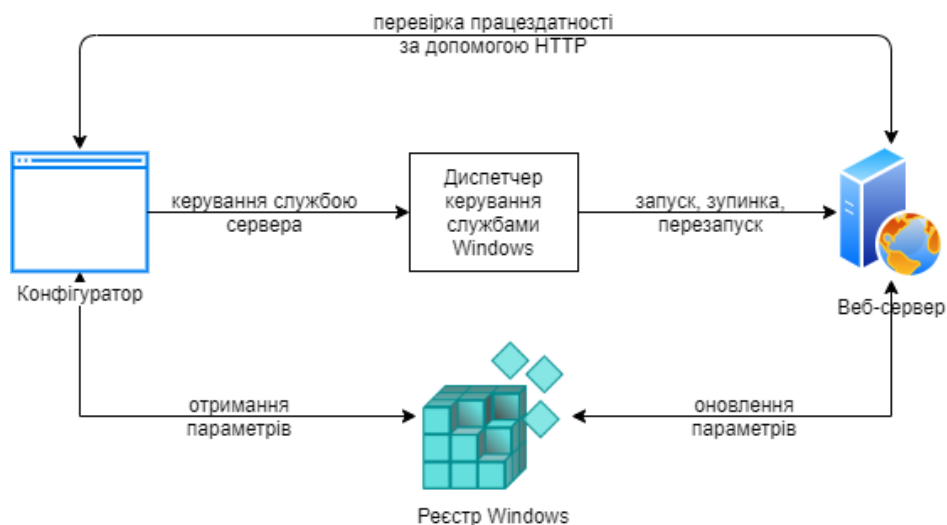


Рис. 1. Функціональна схема програмного додатку

Перелік програмного забезпечення і СУБД, які планується використовувати для створення інформаційної системи:

- ОС: Windows 7-10 та Windows Server 2012-2019;
- СУБД: реляційні бази даних типу MySQL, SQLite або реєстр Windows (на вибір користувача).
- програмна платформа: Boost (сервер) та .NET Framework 4.0 та 4.5 (конфігуратор);

Вимоги до системи шифрування:

- підтримка HTTPS;
- можливість вибору типу шифрування: симетричного AES та асиметричного RSA та розміру ключів шифрування;
- можливість шифрування та розшифрування файлів на стороні клієнта за допомогою бібліотек JavaScript.

Програмний додаток повинен мати ліцензію GNU GPL або подібну та бути простим у користуванні, щоб добре себе зарекомендувати на ринку. Програмний продукт лише дозволяє надавати віддалений доступ до директорій для перегляду чи завантаження, але не змінює файли на комп'ютері, тому не може мати критичних наслідків після використання. Врахувавши ці фактори, можна з упевненістю сказати, що програмний додаток буде надійним.

## Висновки

Розглянуто проблеми створення захищених файлообмінних веб-середовищ на базі ОС Windows Server. Приділено увагу вірусним загрозам, які можуть спричинити інфікування застарілої або неправильно сконфігурованої інфраструктури на базі Windows Server. Визначено найбільш дієві вимоги, що можуть позитивно вплинути на розробку архітектури, резервного копіювання та шифрування.

В результаті виконання вимог можна отримати конкурентноздатне серверне веб-середовище, на базі якого можна розгорнути досить надійну систему обміну файлами.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Арсенюк І. Зменшення кількості інформативних ознак для задачі детектування комп'ютерних атак [Електронний ресурс] / І. Арсенюк // Матеріали XLVII науково-технічної конференції підрозділів ВНТУ, Вінниця, 14-23 березня 2018 р. – Електрон. текст. дані. – 2018. – Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2018/paper/view/5097>.
2. Crazy Malware and Virus Statistics, Trends & Facts. [Електронний ресурс] – Режим доступу: <https://www.safetymalware.com/blog/malware-statistics/>
3. Куперштейн Л. М. Захист файлів в операційній системі Android [Текст] / Л. М. Куперштейн, С. О. Прокопчук, А. Г. Буда // Тези доповідей П'ятої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації», м. Вінниця, 19-21 квітня 2016 року. – Вінниця : ВНТУ, 2016. – С. 77-78.
4. Булда О. О. Програмний засіб для захисту файлів на Windows 10 mobile [Електронний ресурс] / О. О. Булда // Матеріали XLV Науково-технічної конференції ВНТУ, Вінниця, 23-24 березня 2016 р. - Електрон. текст. дані. - 2016. - Режим доступу : <http://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2016/paper/view/953>.
5. Кветний, Р. Використання гібридної криптографії в «хмарних» технологіях комп'ютерних обчислень [Текст] / Роман Кветний, Євгеній Титарчук // Proceedings of the ninth international scientific-practical conference "Internet-Education-Science" (IES-2014), Vinnytsia, 14 - 17 October, 2014. - Vinnytsia : VNTU, 2014. - С. 181-182.
6. Малініч І. П. Ін'єктивний метод отримання даних користувацького досвіду в ігрових симуляторах комп'ютерних мереж [Текст] / І. П. Малініч, В. І. Месюра // Вісник Вінницького політехнічного інституту. – 2019. – No 5. – С. 49-54.

**Томчук Микола Антонович**, кандидат технічних наук, доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, Вінниця, [tomchuk@vntu.edu.ua](mailto:tomchuk@vntu.edu.ua)

**Малініч Павло Павлович**, студент групи ІПІ-18б, факультет ІТКІ, Вінницький національний технічний університет, м. Вінниця

**Малініч Ілля Павлович**, асистент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця

**Tomchuk Mykola**, Candidate of Engineering Sciences, Assistant Professor of the Department of Life and Security Pedagogy, Vinnytsia National Technical University, Vinnytsia, [tomchuk@vntu.edu.ua](mailto:tomchuk@vntu.edu.ua)

**Malinich Pavlo**, group IPI-18b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia

**Malinich Illia**, assistant lecturer of Computer Sciences Department, Vinnytsia National Technical University, Vinnytsia