КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ
Факультет автоматизації і інформаційних технологій
Кафедра кібербезпеки та комп'ютерної інженерії

Кваліфікаційна робота на тему:

«Програмний модуль захисту інформації в корпоративному веб-додатку»

Студент групи БІКСм-24

Пермінов А.Д.

Керівник:

д.т.н., проф. Терентьєв О.О.

АКТУАЛЬНІСТЬ

- Інтернет за останні роки розвивається з неймвоpіною швидкістю. З'являються соціальні мережі , вся коммунікація переходить в режим оналйн. Бізнеси переходять в мережу та продають будь-який спектр товарів та сервісів саме там, тому що користувачам зручно користуватися інтернетом.

- С точки зору розробки веб-додатка, наймати программістів в цій сфері значно легше. Процесс розробки дуже зручний , багато спеціалістів , масштабування та швидкість реалізації роблять веб-додатки такими популярними серед ідей та бізнесу. Величезна кількість готових рішень, наборів інтрументів та громади розробників ще більше спрощує ситуацію на ринку веб-додатків.

- Популярність веб-додатків також зумовлюється тим, що вони мають багато вразливостей. Оскільки розробників велика кількість, але не всі кваліфіковані достатнью , щоб правильно захистити веб-додаток. Таким чином протягом 20 років було зроблено величезна кількість атак на веб-ресурси.

- **Корпоративні веб-додатки** повинні оновлюватись та відповідати новим технологіям , тому їх розробка з використанням останніх підходів, як Singe Page Application та API, наразі актуальна. З 2017 інші типи сайтів почали поступово переходити на цю технологію. Але саме для корпоративних веб-додатків немає чітких принципів, практик та методів застусування цих технологій. Особливо для **архітектури захисту інформації**, яка є невід'ємною та важливою частиною будь-якого корпоративного веб-додатку.

МЕТА ДОСЛІДЖЕННЯ

Створення програмного модулю захисту інформації в сучасному корпоративному веб-додатку де використовуються останні технології розробки та мікросервісна або сервісна архітектура

Досягнення мети роботи потребує розв’язання наступних **задач**:

- Аналіз вже існуючих загроз для веб-додатків
- Аналіз існуючих архітектур та рішень для корпоративного веб-додатку
- Аналіз загроз, які з'явились з початком використанням API за останні роки
- Підбір технологій для розробки та методів захисту від загроз
- Розробка модулю захисту для корпоративного веб-додатку

НОВИЗНА

Вперше запропоновано повну методику, принципи розробки та реалізацію модулю захисту корпоративного веб-додатку з використанням сервісної архітектури, API та SPA, що дало готовий підхід до розробки корпоративних веб-додатків з подібною архітектурою

ПРАКТИЧНА ЦІННІСТЬ

Практична цінність полягає у тому, що практики винайдені протягом програмної реалізації модуля та сама реалізація може бути використана у реальних веб-додатках с подібною архітектурою.

Об’єкт дослідження

Захист веб-додатків від існуючих загроз в мережі Інтернет

Предмет дослідження

Методи та засоби захисту інформації в сучасному корпоративному веб-додатку

Причини вразливостей веб-додатків

1. **Проблема бюджету бізнесу чи замовника.** Неможливість найняти висококваліфікованих розробників та закупити потрібну техніку
2. **Непрофесійність і халатність технічних та програмних спеціалістів.** Незнання методів захисту при написанні програмного кода
3. **Нехтування правилами захисту бази даних та СУБД.** Не використання ролей доступу до таблиць та паролів
4. **Недостатня увага до авторизації, автентифікації, та розмежуванню ролей.**
5. **Людський фактор.** Найчастіше сам користувач заходить на сайт зловмисника та вводить персональні дані

КЛАСИФІКАЦІЯ ЗАГРОЗ ДО ЯКИХ ВРАЗЛИВІ ВЕБ-ДОДАТКИ

Атаки на сервер	Атаки на користувача	Атаки на мережу
DDos - атака — Полягає у тому , щоб перенавантажити сервер, та зупинити його функціонування на деякий час	**XSS - атака** — Полягає у тому , щоб заманити користувача на сторінку сайту, де буде відпрацьовувати шкідливий скрипт	**Перехват трафіку** — Полягає у тому , щоб перехопити трафік який йде до серверу з персональними даними користувача
Brute force паролю — Полягає у переборі всіх варіантів паролю користувача. Не-безпечно якщо пароль занадто короткий	**CRSF - атака** — Полягає у тому , щоб від імені користувача виконати дії на сайті, які вигідні зловмиснику	
SQL – ін’єкція — Суть такої атаки полягає у впровадженні довільного SQL кода хакера у веб-додаток	**Фішингові сторінки** — Полягає у тому , щоб заманити користувача на схожу до оригіналу сторінку , де він введе свої персональні дані	

МЕТОДИ ЗАХИСТУ ВІД ПОПУЛЯРНИХ ЗАГРОЗ

Назва атаки	Методи захисту
DDos	Потужне обладнання, тайм-аут запиту, спеціальна система яка блокує підозрілі запити
Brute Force	Валідація та умови складності паролів, CAPTCHA, тайм-аут авторизації
SQL – ін’єкція	Функціонал плейсхолдерів та екранування вхідних даних, білі списки структури запиту, хешування паролів
XSS – атаки	Декодування та екранування вхідних даних, білі списки, встановлення прапору HttpOnly для Cookie, використання загоовку Content Security Policy (CSP)
CRSF – атаки	CRSF токен, використання заголовку Content-Type зі значенням “application/json” або SameSite
Фішингові сторінки	Двухфакторна автентифікація
Перехват трафіку	Використання HTTPS протоколу

ВИДИ КОРПОРАТИВНХ ВЕБ-ДОДАКІВ ТА ЇХ ФУНКЦІЇ

Корпоративний сайт – це звичайний багатосторінковий або лендінг сайт з елементами бренду компанії, який орієнтованій для залучення клієнтів та опублікований публічно в інтернеті.

Корпоративний портал (або корпортал)– це внутрішній інформаційно-комунікативний веб-ресурс для управління організацією, забезпечення працівникам доступу до корпоративної інформації, а також для збирання та використання даних про бізнес-процеси та управління комплекснеми бізнес-процесами.

Функції та особливості корпорталу:

- Інтеграції у внутрішню корпоративну мережу
- Управління та візуалізації бізнес-процесів
- Кластеризації веб-ресурсу, тобто, його географічного розподілу на кількох серверах з метою покращення доступності порталу та його масштабування при великих навантаженнях
- Об'єднує інформаційні ресурси компанії, забезпечуючи всім учасни-кам доступ до даних
- Забезпечує безпеку комерційної інформації, тому що зайти на веб-ресурс можуть лише співробітники або ті, кому відкрито доступ. Причому, кожному користувачеві можна встановити свій рівень до-ступу

ГОТОВІ РІШЕННЯ ТА ІСНУЮЧА АРХІТЕКТУРА

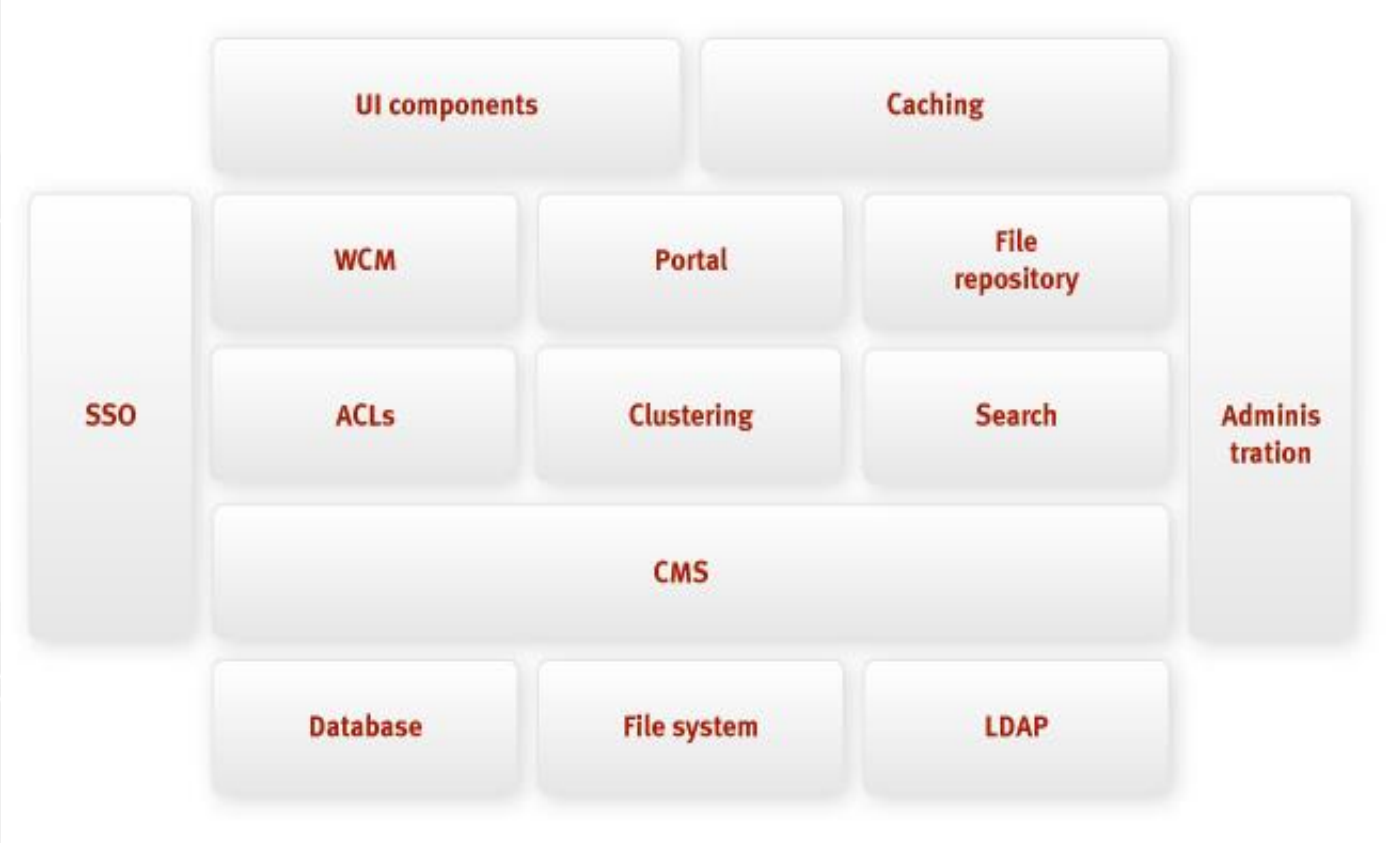
1С·БИТРИКС

UMI.CMS

netcat

HostCMS

AmiroCMS



Недоліки:

- Монолітна архітектура
- Неможливість паралельної розробки в різних командах
- Дири в безпеці
- Неможливість масштабування
- Проблеми з високою нагрузкою
- Неможливість кастомних бізнес процессів з асинхронною обробкою данних
- Неможливість гнучкості системи

ТЕХНІЧНЕ ЗАВДАННЯ

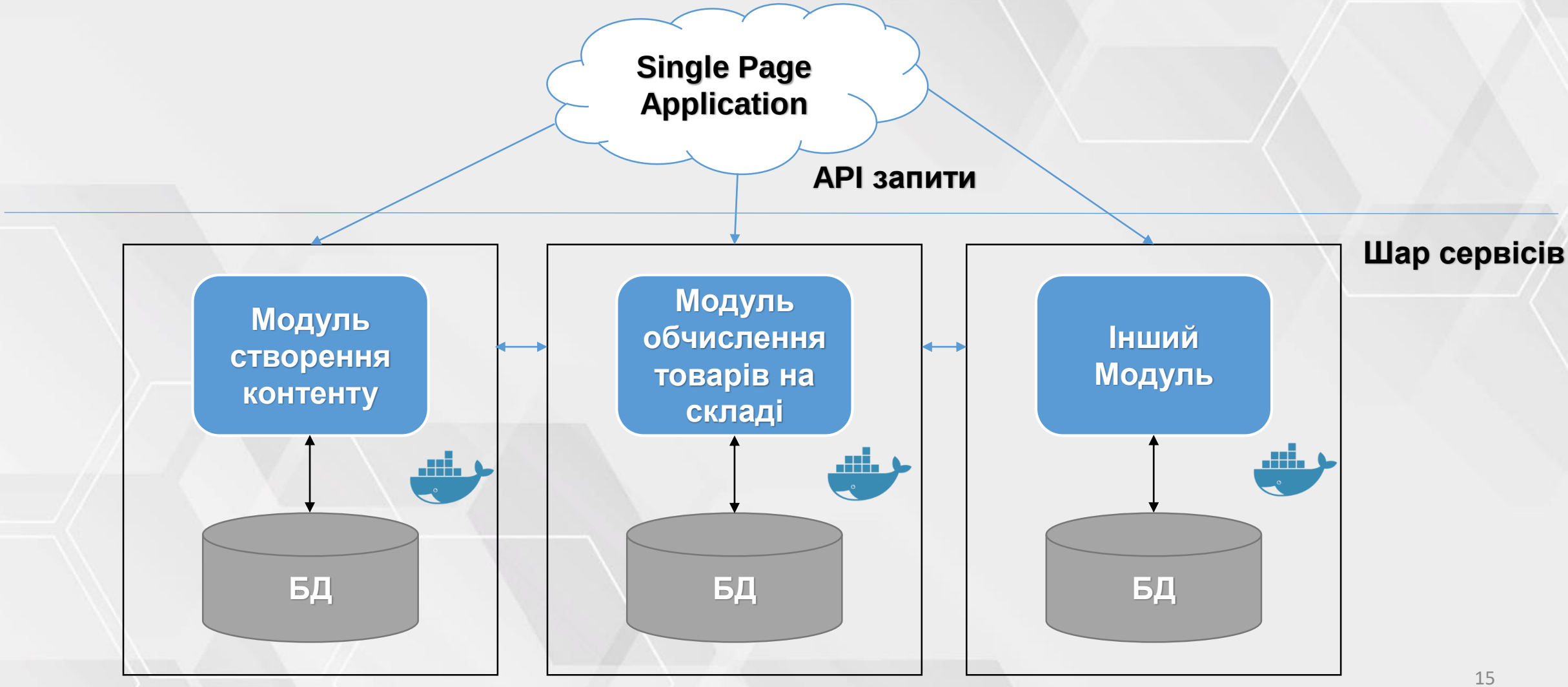
ВИБІР ТЕХНОЛОГІЙ

- Для бекенд частини був вибраний PHP Framework Symfony, який має гарну структуру, готові рішення та інструменти. Також він включає себе ORM Doctrine 2, що робить автоматично неможливим атаку типу SQL-ін’єкція.
- Для фронтенд частини був вибраний AngularJs, що дозволяє швидко писати інтерфейси користувача, також має багато інструментів та дозволяє реалізовувати SPA . З фреймворками такого типу неможлива атака типу XSS та CRSF.
- Для контейнерізації та розгортування кожного сервісу був вибраний Docker

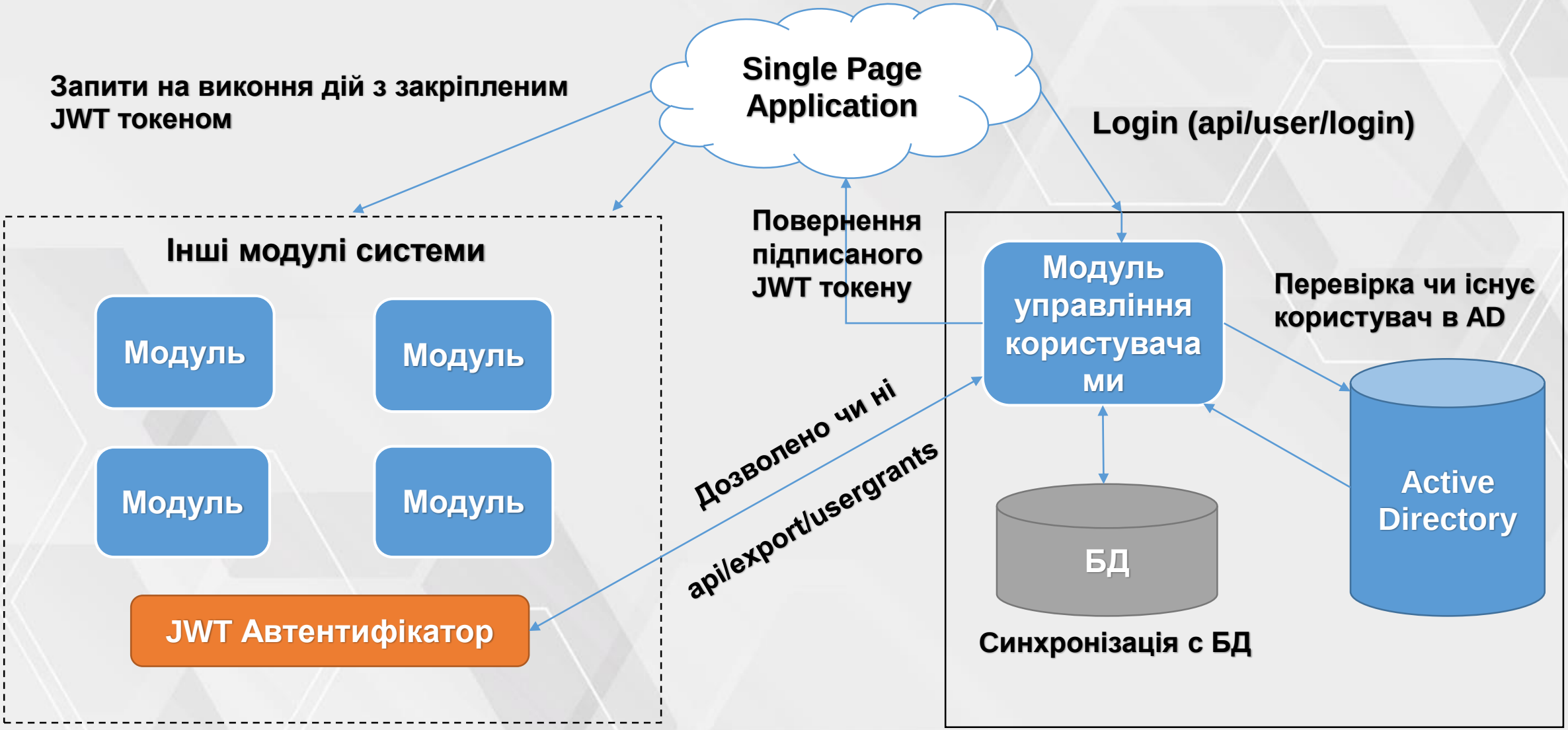
МЕТОДИ ЗАХИСТУ ВІД ЗАГРОЗ В НОВІТНІХ ПРОЕКТАХ

Назва загрози	Методи захисту
API2:2019 Broken User Authentication (Недоліки аутентифікації користувачів).	Використання заголовку Authorization разом з підписанним сервером аунтентифікації JWT токеном
API 1: 2019 Broken Object Level Authorization (Недоліки контролю доступу до об'єктів)	Чітке розмежування доступу. Таблиця User містить зв’язки за таблицею ROLE, яка в свою чергу містить зв’язок з таблицею ACTION. Перевірка доступу користувача завдяки токену при кожному запиті.
API 3: 2019 Excessive Data Exposure (Розголошення конфіденційних даних)	Використання спеціального сервісу ModelBuilder , який буде створювати модель для кожного запиту та віддавати тільки необхідні для клієнту дані.
API 6: 2019 Mass Assignment (Небезпечна десеріалізація)	Кожен вхідний запит в форматі json буде перетворюватись у модель звідки будуть зберігатися в базу тільки необхідні дані.
API 7: 2019 Security Misconfiguration (Некоректне налаштування параметрів безпеки)	Надійне зберігання конфігурації в Docker Secret сховищі, які будуть підставлятись тільки після ініціалізації додатку
API 10: 2019 Insufficient Logging & Monitoring (Недоліки журналирования і моніторингу)	Логування всіх невдалих спроб увійти в систему, та сповіщення в спеціальний канал
Insecure Passwords and Insecure Transport	Паролі не зберігаються в базі додатку, а знаходяться виключно в Active Directory. HTTPS не використовується оскільки підключення до приватної мережі можливо тільки через VPN

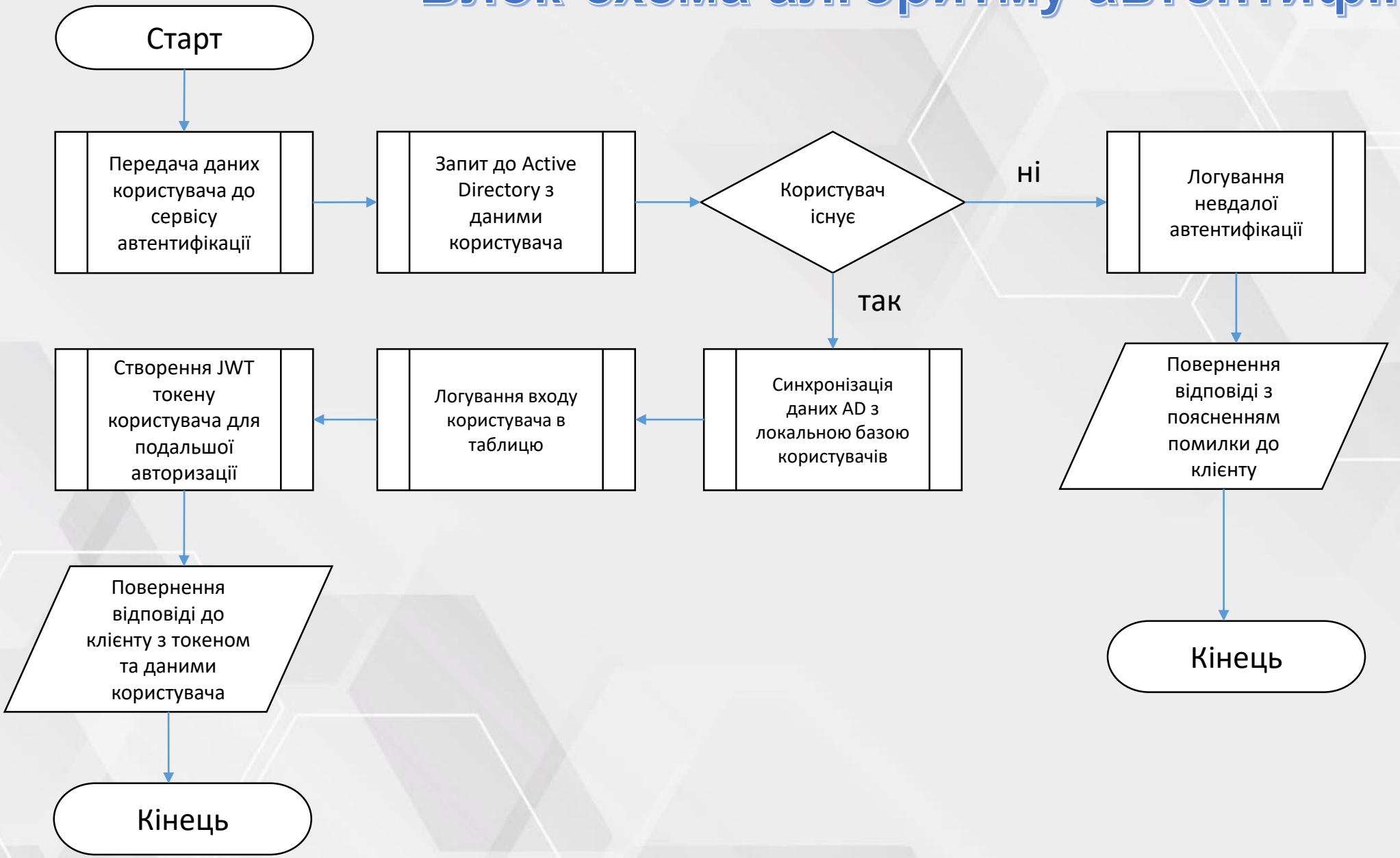
Структура веб-додатку з сервісно-орієнованою архітектурою



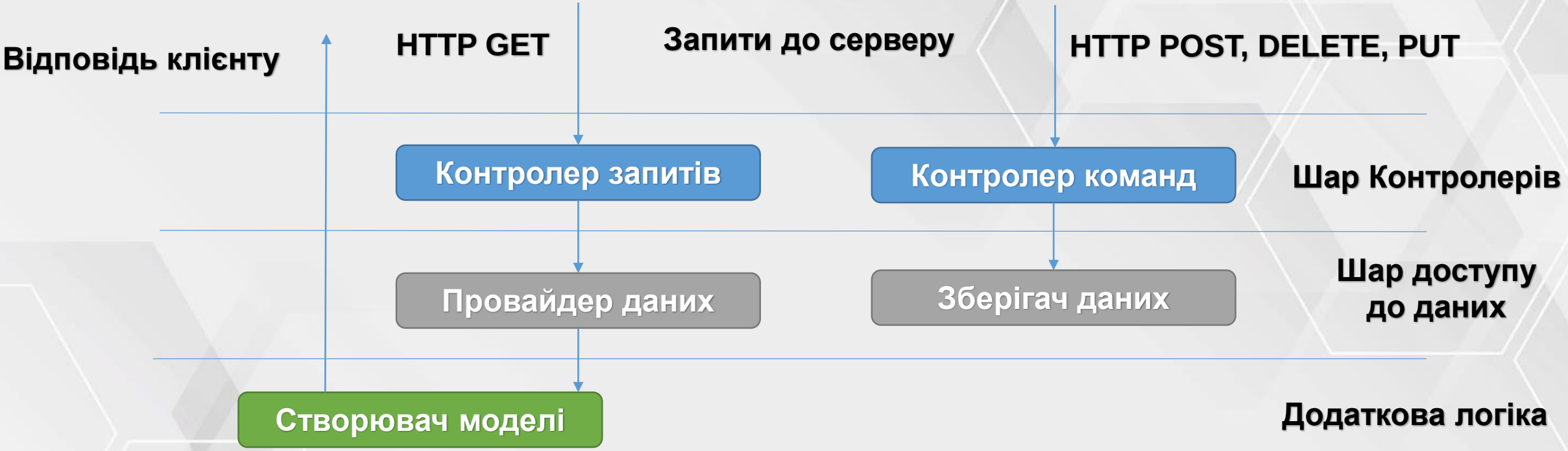
Структура веб-додатку з модулем захисту



Блок-схема алгоритму автентифікації



Основна структура бекенд частини



Інтерфейс для керування розмежуванням доступу

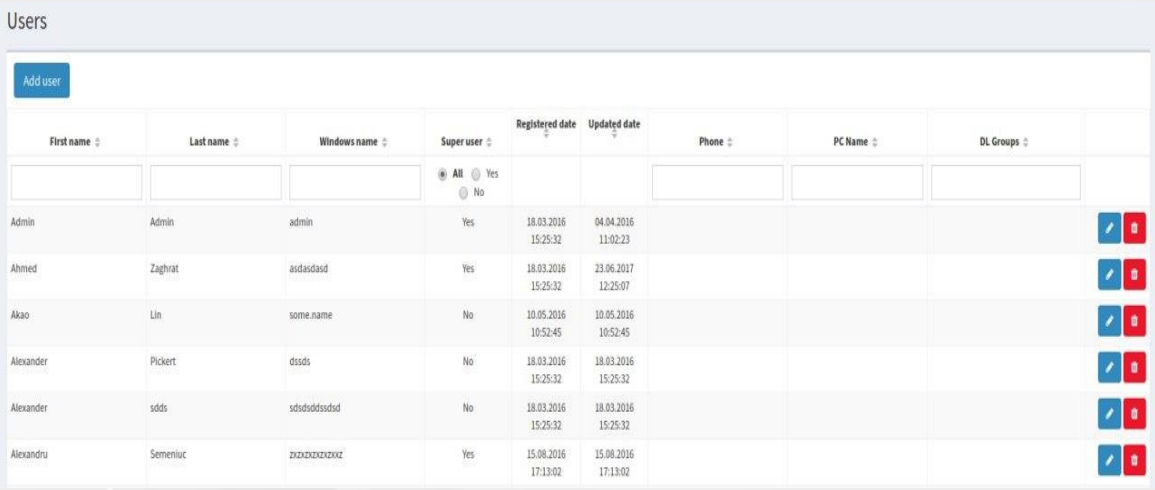


Рис. 3. Інтерфейс Users Overview

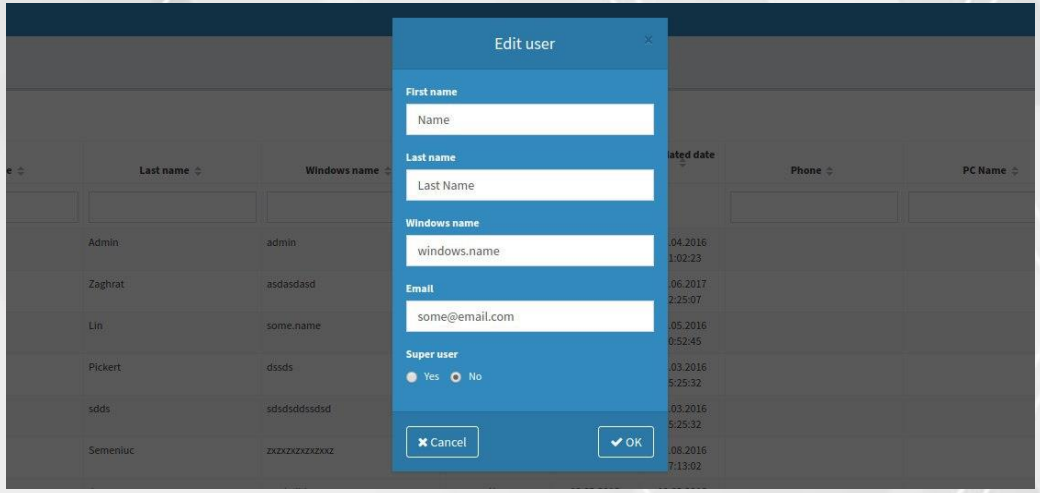


Рис. 4. Приклад компонента модального вікна для редагування користувача

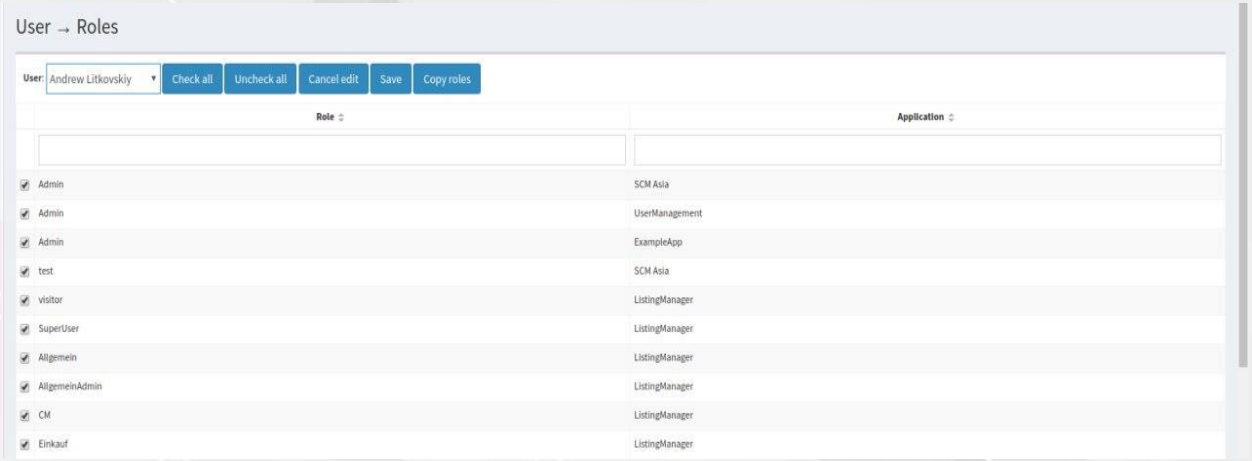


Рис. 5. Інтерфейс надання ролі користувачу

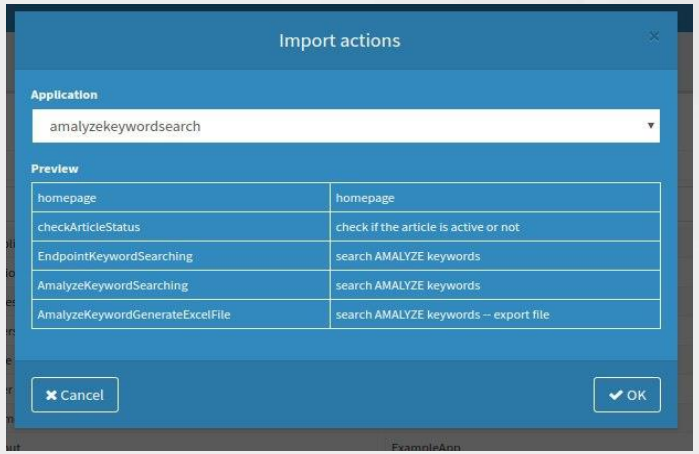
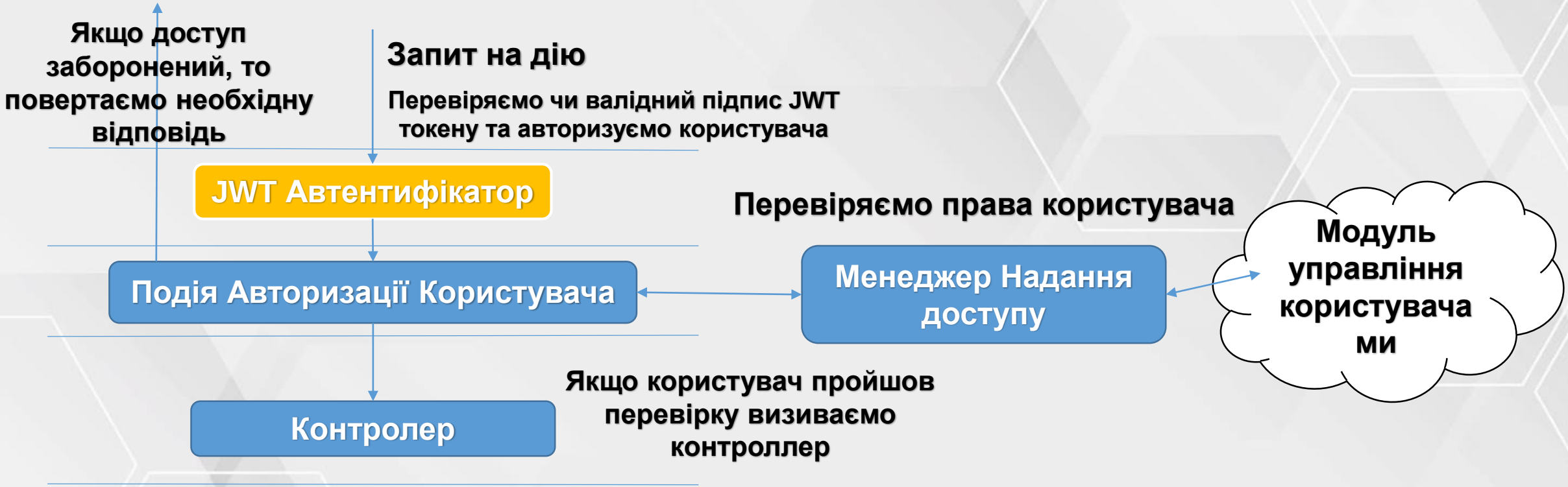


Рис. 6. Інтерфейс імпорту дій

Процес надання доступу користувачу



Висновки

Було виявлено ряд проблем щодо розробки модуля захисту інформаціїї в корпоративному веб-додатку з використанням SPA та сервісно-орієнтованної архітектури. Наприклад, повна відсутність принципів, рекомендацій та практик щодо реалізації подібного функціоналу.

В ході роботи були вирішені наступні задачі:

- Були проаналізовані старі проблеми, якими оперують зловмисники, що дало розуміння чи вразливі сучасні підходи в розробці до вже відомих атак
- Також проаналізований рейтинг нових проблем OWASP (Broken User Au-thentication, Broken Object Level Authorization, Mass Assigment, Data Expo-sure, Security Misconfiguration), що дало чітке визначеня про те, як проектувати захист
- Підбір технологій для створення модулів корпоративного веб-додатку, що дало чітке розуміння, що багато вже відомих атак можуть бути знешкодженні просто при виборі цих технологій
- Розробка повного модулю захисту інформації з автентифікацію та авторизацією з використанням підписаного JWT токену та інтеграції веб-додатку з Active Directory, що притаманна корпортаивним мережам. Практики винайдені протягом програмної реалізації модуля та сама реалізація може бути використана у реальних веб-додатках с подібною архітектурою.

ДЯКУЮ ЗА УВАГУ