**Запити зацікавлених осіб**

Вступ …………………………………………………………………2

1. Мета ……………………………………………………….……….2

2. Основні положення……………………………………………….2

3.Короткий огляд продукту…………………………………….….. 6

4. Контекст…………………………………………………. ..………6

5. Ділові правила …………………………………………….……….7

6. Сценарії…………………………………………..............................8

7.Діаграми …………………………………………………………...21

8. Діаграма бізнес-процесів…………………………………………27

8. Функціональність …………………………………………..…….28

10. Практичність ………………………………………………….....29

11. Надійність……………………………………………………..…29

**Вступ**

У цьому документі описуються запити зацікавлених осіб по відношенню до розроблювальної системи «Система управління персональними даними у ВНЗ» в якості яких виступають: адміністратор, бухгалтерія, деканат та клієнти ( авторизовані викладачі і студенти).

**1.Мета**

Метою документу є визначення основних вимог до функціональності, продуктивності, експлуатаційної придатності, забезпечення інформацією усіх зацікавлених осіб, а саме: замовника, розробників, користувачів системи та інших.

**2. Основні положення.**

Система управління персональними даними – головна складова процедури оперативного управління студентами, викладачами, кадрами. Результативність даного управління впливає на процес вступу студентів, прийняття на роботу викладачів тощо. Відсутність засобів автоматизації ускладнює роботу бухгалтерії, відділу кадрів, вступної комісії, що негативно впливає на швидкість прийняття рішення та додавання нових юзерів . Для вирішення заданої проблеми, нам потрібно врахувати всі аспекти нашого проекту: від організаційної частини, до практичного втілення.

**2.1. Постановка завдання системи управління персональними даними**

Проблема системи управління персональними даними полягає у тому, що існує декілька прав доступу користувачів до даних: читання, запис, зміна. Також з’являється проблема розмежування користувачів: звичайні студенти, викладачі, бухгалтерія, деканат тощо, що може призвести до значної втрати конфіденційної інформації, що неприпустимо і потрібно передбачити. Також потрібно зробити зрозумілу та зручну у користуванні реєстрацію, аутентифікацію та авторизацію. Слід враховувати наступні обмеження: кожна група користувачів має свої обмежені права доступу, у кожної групи є адміністратор, який може ставити кожному користувачу свої права доступу.

2.2. **Аналіз стану використання системи управління персональними даними**

Ідея нашої системи полягає у усуненні паперової документації та бюрократії, адже електронна система більш гнучка та універсальна. Управління будуть здійснювати адміністратори, що будуть контролювати права доступу кожного користувача та перевіряти правильність реєстрації.

2.3. **Автоматизація розподілу аудиторного фонду**

Ядром нашого проекту буде система програмного забезпечення, яка буде реалізувати розподіл ресурсу через базу даних в яку будуть внесені персональні дані, токени та облікові записи користувачів (викладачів, студентів, бухгалтерів тощо). Контроль над ресурсом буде здійснюватися через підключену до системи мережу аутентифікації, тобто СКУД (систему контроля управління доступом).

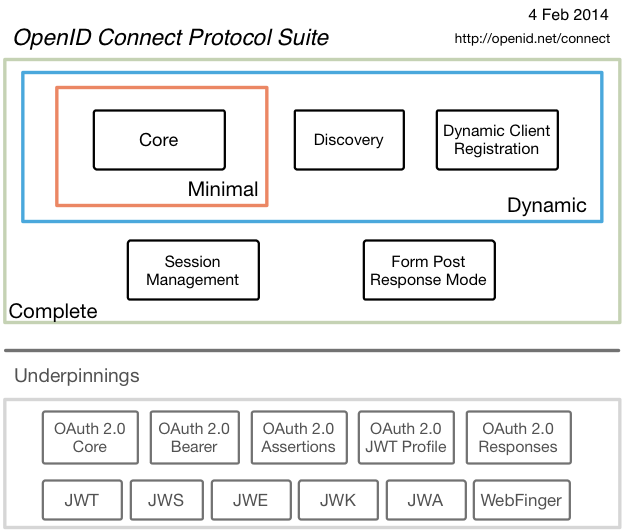
**2.4. СКУД**

Системи контролю доступу є невід'ємною частиною комплексної системи безпеки входу. Основне завдання системи контролю та управління доступом – обмеження і розмежування можливості доступу до різних частин контрольованих даних. Системи контролю й керування доступом дозволяють організувати контрольовані читання, запис, додавання, видалення. Основними вимогами до системи контролю доступу є їх простота і зручність в їх використанні, а також надійність контролю доступу. Системи контролю й керування доступом зазвичай складаються з декількох елементів – ідентифікаторів користувачів, авторизації, систем автентифікації, контролюючих доступ до даних.

Наша система являтиме собою такий набір складових:

**Ідентифікатор користувача.** Це деякий пристрій або ознака, по якому визначається користувач. Ідентифікаторами можуть бути логін і пароль, токени доступу, зображення райдужної оболонки ока, відбиток пальця, відбиток долоні і багато інших фізичних ознак. В системі контролю доступу кожному коду ставиться у відповідність інформація про права і привілеї власника ідентифікатора.

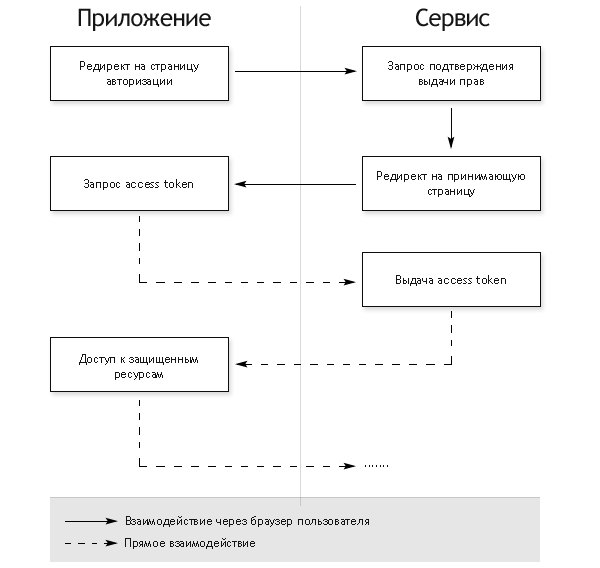
Наш вибір пав на токени, що після реєстрації переходять у логін і пароль. На нашу думку, це найзручніший спосіб для забезпечення доступу до даних.

**Автентифікація.** Процедура встановлення належності користувачеві інформації в системі пред'явленого ним [ідентифікатора](https://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%BE%D1%80).

З позицій [інформаційної безпеки](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0) Автентифікація є частиною [процедури](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B0" \o "Процедура) надання доступу для роботи в [інформаційній системі](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0" \o "Інформаційна система), наступною після [ідентифікації](https://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0)" \o "Ідентифікація (інформаційна безпека)) і передує [авторизації](https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F" \o "Авторизація).

Одним з найвідоміших протоколів автентифікації є OpenId, що є і самим зручнішим.

**Авторизація. Авторизація** - керування рівнями та засобами [доступу](https://uk.wikipedia.org/w/index.php?title=%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF&action=edit&redlink=1) до певного захищеного ресурсу, як у фізичному розумінні (доступ до кімнати готелю за карткою), так і в галузі цифрових технологій (наприклад, автоматизована система контролю доступу) та ресурсів системи залежно від [ідентифікатора](https://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%BE%D1%80" \o "Ідентифікатор) і [пароля](https://uk.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C) користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних.

З позицій [інформаційної безпеки](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0" \o "Інформаційна безпека) Авторизація є частиною [процедури](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B0" \o "Процедура) надання доступу для роботи в [інформаційній системі](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0" \o "Інформаційна система), після [ідентифікації](https://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0)" \o "Ідентифікація (інформаційна безпека)) і [автентифікації](https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F" \o "Автентифікація).

### Одним із протоколів авторизації є OAuth 2.0, що є дуже простим у використанні, тому і був вибраний для цього проекту.

**Принцип функціонування системи контролю та управління доступом.** Принцип функціонування системи контролю та управління доступом наступний:

Кожен викладач, студент, бухгалтер тощо отримує ідентифікатор (токен) – код, за яким він повинен зареєструватися у системі управління персональними даними, увівши логін і пароль, що згодом будуть прив’язані до токена (токен анулюється та за ним не можна більше реєструватися). Зареєструвавшись, він отримує права доступу в залежності від приналежності до групи користувачів (студенти, викладачі тощо) з якими може працювати надалі. Також існують головні адміністратори, котрі слідкують за справністю системи та правильністю надання прав доступу тим чи іншим користувачам

**3.Короткий огляд продукту**

Система «Система управління персональними даними для ЗВО» надає інтерфейс взаємодії між власно персональними даними, клієнтами різного рівня доступу та адміністраторами. Перший рівень користувача (студенти, працівники на робочих посадах) має тільки права на читання своїх власних даних, що не є приватними документами закладу . Другий рівень доступу (викладачі) має право на читання власних даних, часткового читання та запису даних студентів. Третій рівень (деканат, завхоз) має права на часткове читання та запис усіх користувачів. Четвертий рівень, найвищий, (скажімо бухгалтер), має повний доступ читання-запису перших усіх персональних данних. А роль адіміністратора - надання конкретним людям цих рівнів. Адміністратор також може доповнювати рівні ролями зі зміною вихідних конфігурацій системи.

**4.Контекст**

Перелік вимог, зазначених у даному документі є основою технічного завдання для розробки системи «Система управління персональними даними для закладу вищої освіти».

# **5. Ділові правила і приписи**

**5.1. Призначення системи.**

Система управління персональними даними учбового закладу призначена для зберігання, обробки і захисту інформації, використовуваної закладом.

Вона являє собою контрольовану адміністратором гнучку систему ролей, в якій набір ролей встановлюється адміністратором і кожна з яких має свій набір прав доступу до інформації і свої можливості.

**5.2. Політика взаємовідносин з клієнтом.**

Клієнтами системи можуть бути тільки авторизовані особи, які попередньо були зареєстровані в системі за токеном, наданим адміністратором, а також підтвердили свою реєстрацію за цим токеном.

Ректор – найвищий орган в ієрархії системи але не впливає на неї прямо. Фактичним таким органом є адміністратор – особа яка має найвищий рівень доступу в системі, а також несе відповідальність за збереження і захист даних.

Політика взаємовідносин клієнта системи полягає в наданні доступу до інформації після авторизації за допомогою системи авторизації. В свою чергу авторизація можлива при попередній трьох-кроковій реєстрації, яка складається з генерації особистого токена користувача, реєстрації в системі за допомогою токена, при чому токен анулюється, та підтвердження реєстрації адміністратором.

**5.3 Характеристика ділового процесу.**

Права по керуванню системою належать ректору, адміністратор, як виконавчий орган вносить здійснює інструкції по внесенню, редагуванню даних, реєстрації, спостереженню та екстреному доступу. Також в цьому процесі беруть участь усі користувачі системи, яким було надано відповідні права. В інших аспектах система діє самодостатньо, та накопичує дані своєї експлуатації, тобто зберігає інформацію про будь-які маніпуляції з даними.

**6. Сценарії**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.1 |
| Назва | Реєстрація нового клієнта (викладача) |
| Учасники | Викладач, адміністратор |
| Передумови | Коректно заповнені форми на реєстрацію |
| Результат | Профіль клієнта (викладача) |
| Виключні ситуації | Некоректно заповненні форми |
| Основний сценарій | 1. Отримання токену від головного адміністратора 2. Реєстрація (введення логіну та паролю, токен анулюється) 3. Отримання прав доступу в залежності від приналежності до групи користувачів 4. Перевірка правильності надання адміністратором 5. Створення профілю |

**Сценарій “Реєстрація нового користувача (викладача)”**

**Сценарій “Реєстрація нового користувача (студента)”**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.2 |
| Назва | Реєстрація нового клієнта (студента) |
| Учасники | Студент, адміністратор |
| Передумови | Коректно заповнені форми на реєстрацію |
| Результат | Профіль клієнта (студента) |
| Виключні ситуації | Некоректно заповненні форми |
| Основний сценарій | 1. Отримання токену від головного адміністратора 2. Реєстрація (введення логіну та паролю, токен анулюється) 3. Отримання прав доступу в залежності від приналежності до групи користувачів 4. Перевірка правильності надання адміністратором 5. Створення профілю |

**Сценарій “Реєстрація нового користувача (бухгалтера)”**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.3 |
| Назва | Реєстрація нового клієнта (бухгалтера) |
| Учасники | Бухгалтер, адміністратор |
| Передумови | Коректно заповнені форми на реєстрацію |
| Результат | Профіль клієнта (бухгалтера) |
| Виключні ситуації | Некоретно заповнені форми |
| Основний сценарій | 1. Отримання токену від головного адміністратора 2. Реєстрація (введення логіну та паролю, токен анулюється) 3. Отримання прав доступу в залежності від приналежності до групи користувачів 4. Перевірка правильності надання адміністратором 5. Створення профілю |

**Сценарій “Формування бази даних”**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.4 |
| Назва | Формування бази даних |
| Учасники | Адміністратор, система |
| Передумови | Наявність профілів клієнтів |
| Результат | База даних |
| Виключні ситуації | Відсутність профілів клієнтів |
| Основний сценарій | 1. Адміністратор формує базу даних за розширеним розкладом та множиною профілів клієнтів. |

**Сценарій «Авторизація клієнта»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.5 |
| Назва | Авторизація клієнта |
| Учасники | Клієнт, система |
| Передумови | База даних, наявність профілю клієнта |
| Результат | Вхід клієнта у профіль |
| Виключні ситуації | Клієнт не зареєструвався, введений неправильний логін чи пароль |
| Основний сценарій | 1. Клієнт вводить логін та пароль. 2. Опрацьований запит порівнюється із даними в базі 3. Вхід клієнта в профіль |

**Сценарій «Зміна даних клієнта (студента)»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.6 |
| Назва | Зміна даних клієнта (студента) |
| Учасники | Адміністратор |
| Передумови | База даних, наявність профілю студента |
| Результат | Дані про студента змінені |
| Виключні ситуації | Студент відсутній в базі даних |
| Основний сценарій | 1. Адміністратор повідомляється про необхідність зміни даних студента 2. Адміністратор виконує зміну |

**Сценарій «Зміна даних клієнта (викладача)»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.7 |
| Назва | Зміна даних клієнта (викладача) |
| Учасники | Адміністратор |
| Передумови | База даних, наявність профілю викладача |
| Результат | Дані про викладача змінені |
| Виключні ситуації | Викладач відсутній в базі даних |
| Основний сценарій | 1. Адміністратор повідомляється про необхідність зміни даних студента 2. Адміністратор виконує зміну |

**Сценарій «Зміна даних клієнта (студента)»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.8 |
| Назва | Зміна даних клієнта (бухгалтера) |
| Учасники | Адміністратор |
| Передумови | База даних, наявність профілю бухгалтера |
| Результат | Дані про бухгалтера змінені |
| Виключні ситуації | Бухгалтер відсутній в базі даних |
| Основний сценарій | 1. Адміністратор повідомляється про необхідність зміни даних бухгалтера 2. Адміністратор виконує зміну |

**Сценарій «Видалення клієнта (студента) із бази даних та видалення профілю клієнта (студента)»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.9 |
| Назва | Видалення клієнта (студента) із бази даних та видалення профілю клієнта (студента) |
| Учасники | Адміністратор |
| Передумови | База даних, наявність профілю студента |
| Результат | Клієнт та його профіль видалені з бази даних |
| Виключні ситуації | Студент відсутній в базі даних |
| Основний сценарій | 1. Адміністратор повідомляється про необхідність видалення викладача із бази даних та видалення профілю викладача 2. Адміністратор виконує видалення |

**Сценарій «Видалення клієнта (викладача) із бази даних та видалення профілю клієнта (викладача)»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.10 |
| Назва | Видалення клієнта (викладача) із бази даних та видалення профілю клієнта (викладача) |
| Учасники | Адміністратор |
| Передумови | База даних, наявність профілю студента |
| Результат | Клієнт та його профіль видалені з бази даних |
| Виключні ситуації | Викладач відсутній в базі даних |
| Основний сценарій | 1. Адміністратор повідомляється про необхідність видалення викладача із бази даних та видалення профілю викладача 2. Адміністратор виконує видалення |

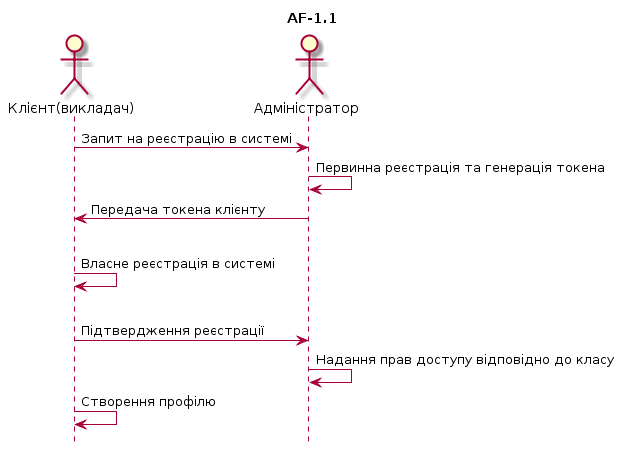
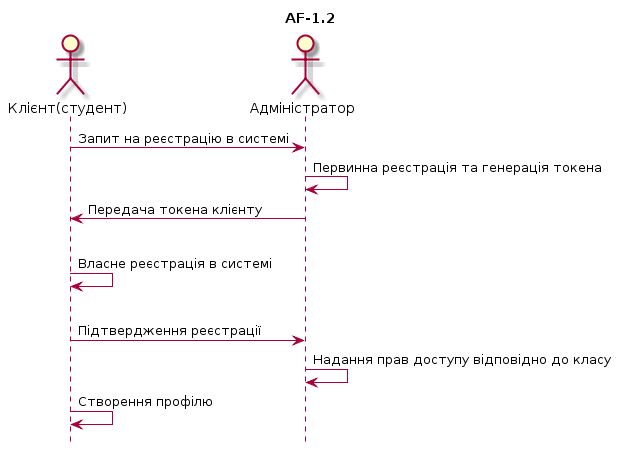
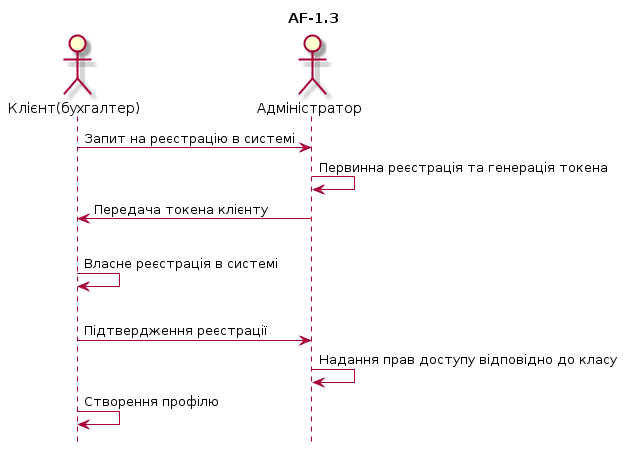
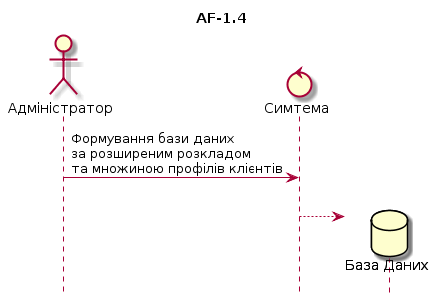
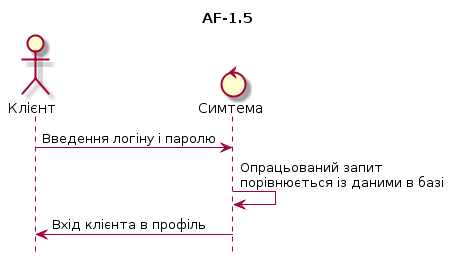
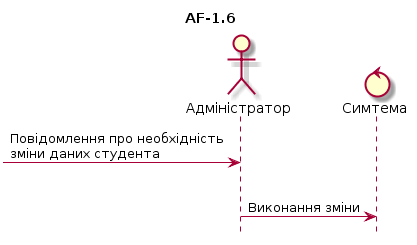
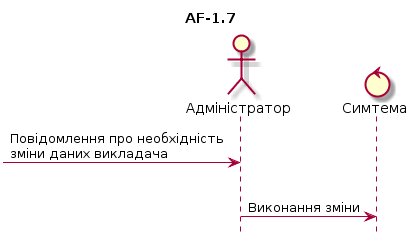
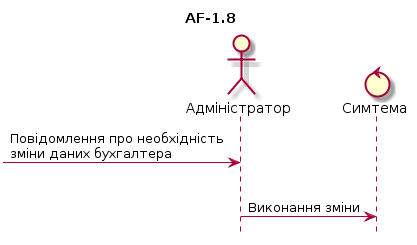
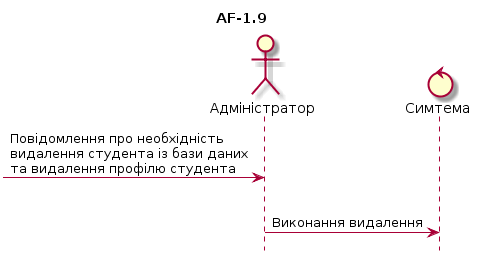
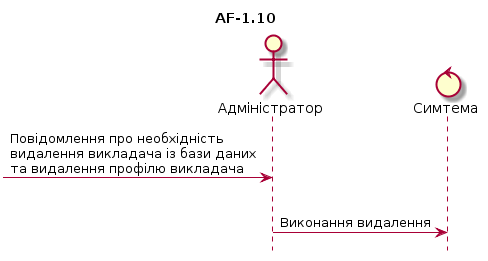
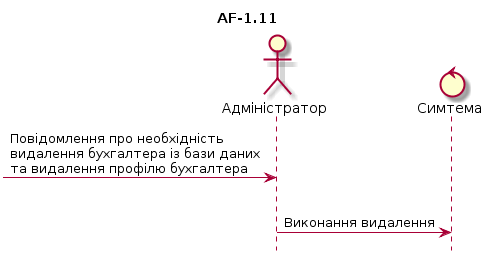
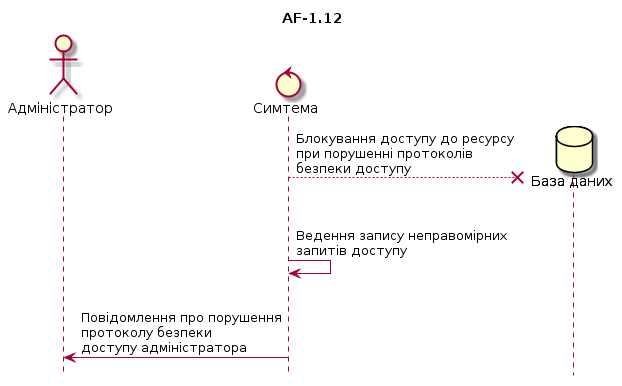
**Сценарій «Видалення клієнта (бухгалтера) із бази даних та видалення профілю клієнта (бухгалтера)»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.11 |
| Назва | Видалення клієнта (бухгалтера) із бази даних та видалення профілю клієнта (бухгалтера) |
| Учасники | Адміністратор |
| Передумови | База даних, наявність профілю бухгалтера |
| Результат | Клієнт та його профіль видалені з бази даних |
| Виключні ситуації | Бухгалтер відсутній в базі даних |
| Основний сценарій | 1. Адміністратор повідомляється про необхідність видалення бухгалтера із бази даних та видалення профілю бухгалтера 2. Адміністратор виконує видалення |

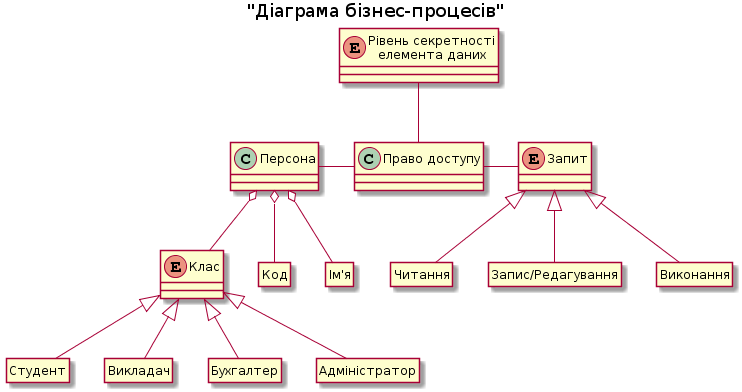
**Сценарій «Порушення протоколів безпеки доступу»**

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.12 |
| Назва | Порушення протоколів безпеки доступу |
| Учасники | Адміністратор, система |
| Передумови | Порушення протоколів безпеки |
| Результат | Блокування ресурсу, повідомлення адміністратору |
| Виключні ситуації | Тотальний збій системи при атаці на програмне забезпечення, недієздатність адміністратора. |
| Основний сценарій | 1.Система блокує доступ до ресурсу при порушенні протоколів безпеки доступу. 2.Система веде запис неправомірних запитів доступу. 3. Система повідомляє про порушення протоколу безпеки доступу адміністратора. |

**7. Діаграми**



**8. Діаграма бізнес-процесів**



**10. Функціональність.**

Основні вимоги до функціональності, пред’явлені зацікавленими особами, відносяться до трьох категорій:

1. Деканат

2. Адміністратор

3. Клієнт (студент, викладач)

4. Бухгалтерія

**10.1. Структура системи.**

1. Система доступу до бази даних.

2. База даних.

3. Адміністратор як виконавчий орган деканату та бухгалтерії.

4. Клієнтська база.

**10.2. Можливості зацікавлених осіб.**

10.2.1. Можливості Адміністратора.

1. Спостереження за системою, її оцінка.

2. Оповіщення про роботу системи.

3. Внесення змін в систему даними, що підкріпленні задокументованими запитами деканату та бухгалтерії.

4. Підтримка системи в робочому стані.

10.2.2. Можливості клієнтів.

1. Санкціонований доступ до ресурсу після реєстрації.

2. Можливість взаємодії з системою залежно від визначених рівнів та прав доступу.

**11. Практичність**

**11.1. Стандартизація**

Система ефективно надає доступ до ресурсу кожному її авторизованому клієнту, при відповідності запиту ідентифікатора базі даних системи.

**11.2. Інтерфейс користувача**

Інтерфейс сервісу системи відповідає наступним вимогам:

1. Зрозумілий, створений з урахуванням ергономічних вимог.

2. Простий у використанні та зручний.

3. Надійний та зменшує часові затрати на доступ до ресурсу.

**12. Надійність**

Аналіз системи показав її високу надійність у захисті ресурсу від незаконного втручання в систему.

Надійність не падає навіть при значному прискоренні процедури доступу. Для забезпечення цілісності, незмінності та достовірності даних, буде використовуватися комплекс технологічних і адміністративних процедур, що перешкоджають випадковій або навмисній зміні збережених архівів із бази. Для забезпечення збереження даних клієнтів, має бути використаний метод резервного копіювання. Токени для реєстрації забезпечують її безпеку. Головний адміністратор контролює видачу прав, що унеможливлює виникнення несподіваних ситуацій.