**Запити зацікавлених осіб**

[Вступ 2](#_Toc4649128)

[1.Мета 2](#_Toc4649129)

[2. Основні положення. 2](#_Toc4649130)

[3.Короткий огляд продукту 13](#_Toc4649131)

[4.Контекст 13](#_Toc4649132)

[5. Ділові правила і приписи 13](#_Toc4649133)

[6. Сценарії 15](#_Toc4649134)

[7. Діаграми 27](#_Toc4649135)

[8. Діаграма бізнес-процесів 34](#_Toc4649136)

[9. Функціональність. 35](#_Toc4649137)

[10. Практичність 37](#_Toc4649138)

[11. Надійність 37](#_Toc4649139)

### 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 ринку систем з керування персональними даними та ознайомлення із законами щодо персональних даних**

Персональні дані — це сукупність відомостей про фізичну особу, яка може бути конкретно ідентифікована. До персональних даних не належить інформація про юридичних осіб. Обробка персональних даних — будь-яка дія або сукупність дій, здій­снених повністю або частково в інформаційній системі, або в картотеках персональних даних, які пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, поновленням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знеособленням, знищенням відомостей про фізичну особу. Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них. Системи управління персональними даними – це системи, які являють собою сукупність персональних даних, що містяться в базі даних, а також інформаційних технологій і технічних засобів, що дозволяють здійснювати обробку таких персональних даних з використанням засобів автоматизації або без використання таких засобів. У даному випадку вони повинні бути узагальненими та упорядкованими в електронній формі. Відповідно до листа Державної служби з питань захисту персональних даних від 20.08.2012 №10/3905-12, персональні дані декількох фізичних осіб називаються базою, якщо вони згруповані у сукупність та обробляються. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Спочатку варто з'ясувати, з якою метою обробляються персональні дані. У нашому випадку такою є відносин у сфері освіти, а також інших підприємств. З точки зору Закону № 2297 підприємство є володільцем бази. Закон визначає що володілець бази — це фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних та яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом. Мета обробки персональних даних повинні обов’язково відповідати цілям діяльності володільця бази персональних даних, що зафіксовані в його установчих документах або передбачені законодавством України, що регулює діяльність володільця бази. Згідно з статтею 2 Закону № 2297 розпорядник бази персональних даних — це фізична чи юридична особа, якій володільцем бази персональних даних або законом надано право обробляти ці дані. Володілець бази персональних даних може доручити обробку їх розпоряднику бази персональних даних відповідно до договору в письмовій формі. Прикладом розпорядника може слугувати та ситуація, коли на підприємстві немає відділу кадрів і кадрове діловодство ведеться сторонньою фірмою, тоді ця фірма може вважатися розпорядником бази даних. Пунктами 2 та 3 статті 6 Закону № 2297 встановлено, що персональні дані їх склад та зміст мають бути точними, достовірними, відповідними та оновлюватися в міру потреби, визначеної метою їх обробки.

Згідно з статтею 1 Закону «Про захист персональних даних», він не розповсюджується на фізичних осіб, які використовують бази персональних даних виключно для непрофесійних особистих чи побутових потреб. Відповідно до статті 9 Закону №2297 будь яка база персональних даних підлягає державній реєстрації. Проте зовсім не вся інформація має проходити дану процедуру, а лише такі дані: реквізити власника бази персональних даних, найменування та місцезнаходження даної бази, мета обробки персональних даних, правові підстави обробки персональних даних (відповідно до статті 11 Закону України “Про захист персональних даних”) та реквізити розпорядників бази персональних даних.

Порядок подання заяви на реєстрацію бази персональних даних затверджений Наказом Міністерства юстиції 08.07.2011 №1824/5 «Про затвердження форм заяв про реєстрацію бази персональних даних та про внесення змін до відомостей Державного реєстру баз персональних даних і порядку їх подання». Заява може бути подана в паперовій або в електронній формі на вибір володільця бази. У разі подання заяви в електронній формі, вона повинна відповідати вимогам Законів України «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг», тобто підписана електронним цифровим підписом. В електронній формі можна подати заяву надіславши її на електронну адресу register@zpd.gov.ua або заповнивши заяву на сайті https://rbpd.informjust.ua . Варто пам’ятати, що не можна залишити заяву на реєстрацію декількох баз. Згідно статті 9 Закону №2297 реєстрація баз здійснюється за заявочним принципом шляхом повідомлення. База персональних даних вважається зареєстрованою з моменту внесення відповідного запису Державною службою України з питань захисту персональних даних до Державного реєстру баз персональних даних, а не отримання володільцем бази персональних даних свідоцтва про державну реєстрацію, що є наслідком зазначеного факту. Відповідно до Наказу Мінюсту №1824/5 Державна служба захисту персональних даних повідомляє заявника про реєстрацію. Якщо заява подавалася у паперовій формі, то лист надсилається звичайною поштою. У разі подання заяви в електронній формі заявнику приходить електронне повідомлення.

При зміні відомостей, які необхідні для реєстрації бази персональних даних, її володілець зобов’язаний повідомити Державну службу України з питань захисту персональних даних про кожну зміну не пізніше, ніж протягом 10 робочих днів від введення таких змін. Реєстрації підлягають лише ті зміни, які стосуються даних, що були вказані у заяві на реєстрації бази персональних даних. Тобто, якщо змінюються відомості дані про фізичну особу, то такі зміни реєструвати не варто. Згідно з роз’ясненням Мінюсту від 21.12.2011 для видалення бази персональних даних з Державного реєстру баз персональних даних, володілець такої бази направляє в Державну службу захисту персональних даних заяву про внесення змін до відомостей Державного реєстру баз персональних даних та позначає вилучити всі поля відомостей, які були внесені.

Обробка персональних даних здійснюється за згодою суб’єкта персональних даних (фізичної особи) або у випадках, передбачених законами України, у порядку, встановленому законодавством. Відповідно до абзацу 5 статті 2 Закону №2297 згодою суб’єкта персональних даних є будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки. Державна служба України з питань захисту персональних даних рекомендує вважати формами надання згоди суб’єкта персональних даних наступні документи: документ на паперовому носії з реквізитами, який дає змогу ідентифікувати даний документ та фізичну особу; електронний документ, який має містити обов’язкові реквізити, що дають змогу ідентифікувати цей документ та фізичну особу, також добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних доцільно засвідчувати електронним підписом суб’єкта персональних даних; відмітку на електронній сторінці документа чи в електронному файлі, що обробляється в інформаційній системі на основі документованих програмно-технічних рішень. Згідно з частиною 2 статті 12 Закону №2297 фізичну особу варто повідомити про її права виключно у письмовій формі протягом десяти робочих днів з дня включення її персональних даних до бази персональних даних. Права суб’єкта персональних даних визначені у статті 8 Закону №2297.

Порядок ведення баз персональних даних регулюється «Типовим порядком обробки персональних даних у базах персональних даних». Насамперед варто визначити наявність володіння підприємством персональними даними, цілей обробки та кількості баз персональних даних. Затвердження порядку обробки та захисту персональних даних. Далі отримується дозвіл від фізичних осіб на обробку їх персональних даних та відбувається ознайомлення таких осіб з їхніми правами відповідно до Закону №2297. Потім визначаються посадові особи та структурні підрозділи, котрі є відповідальними за обробку персональних даних. Після цього відбувається подання заяви на реєстрацію бази до Державної служби з питань захисту персональних даних. В кінці кінців за умови дотримання всіх належних форм та відповідності закону, отримання повідомлення від служби та відбувається отримання свідоцтва про реєстрації бази персональних даних. Пункт 5 статті 24 Закону 2297 вимагає визначити структурний підрозділ або відповідальну особу, яка організовує роботу, пов’язану із захистом персональних даних при їх обробці. Призначення відповідальних здійснюється наказом керівника підприємства. Зазвичай ці функції покладаються на кадрову службу, а в деяких випадках на IT-службу. При розробці, слід орієнтуватися на «Типовий порядок обробки персональних даних у базах персональних даних» затверджений Наказом Мінюсту від 30.12.2011 №3659/5. Зі змістом положення треба ознайомити працівників, чия робота безпосередньо пов’язана з обробкою персональних даних на підприємстві.

У зв'язку з появою нових законодавчих вимог варто привести посадові інструкції працівників кадрової служби у відповідність до законодавства про захист персональних даних. Згідно із Законом № 2297 володілець бази персональних даних повинен забезпечити захист цих даних. Бажано розробити локальний нормативний акт, яким регламентуватиметься процес обробки персональних даних на підприємстві, наприклад, Положення про захист персональних даних. Одна із основних функцій цього документа — запровадження процедур доступу до персональних даних, що обробляються на підприємстві.

Наразі Державною службою України з питань захисту персональних даних розроблено проект Типового порядку обробки персональних даних, в якому передбачено, що з метою створення дієвої системи управління персональними даними володільцем має бути визначено структурний підрозділ або відповідальну особу, яка організовуватиме роботу, пов'язану із захистом персональних даних при їх обробці відповідно до законодавства України, яке регулює його діяльність, та установчих документів володільця бази персональних даних. Після прийняття даного порядку цей нормативно-правовий акт можна буде використовувати як основу при розробленні локального нормативного акта, що регламентуватиме обробку персональних даних.

Якщо процес обробки персональних даних на підприємств припиняється, то бази персональних даних підлягають знищенню або передачі в архів. При цьому до державної служби з питань захисту персональних даних треба надіслати заяву про внесення змін до відомостей Державного реєстру баз персональних даних згідно Наказу Мінюсту №1824/5. Про знищення персональних даних також треба повідомити фізичних осіб, щодо яких ці персональні дані оброблялися.

Контроль за додержанням законодавства про захист персональних даних здійснює Державна служба України з питань захисту персональних даних. Контроль здійснюється шляхом проведення виїзних та безвиїзних перевірок володільців та розпорядників баз персональних даних. Якщо в ході проведення перевірки контролери виявлять порушення у законодавства про захист персональних даних, вони складають протоколи про адміністративні правопорушення. Рішення про застосування відповідальності приймається судовими органами за результатами розгляду протоколу.

Відповідальність за порушення в сфері захисту персональних даних передбачена статтями 188-39 та 188-40 Кодексу України про адміністративні правопорушення та статтею 182 Кримінального кодексу України. Громадяни, посадові особи, громадяни-суб’єкти підприємницької діяльності притягуються до адміністративної відповідальності за вчинення таких правопорушень: неповідомлення або несвоєчасне повідомлення суб’єкта персональних даних про його права у зв’язку із включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються; неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних; ухилення від державної реєстрації бази персональних даних; недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них; невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних щодо усунення порушень законодавства про захист персональних даних. За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності. При заподіянні істотної шкоди охоронюваним законом правам, свободам та інтересам особи або повторенні протизаконних дій запобіжні заходи можуть сягнути до 5 років позбавлення волі.

На даний момент часу існує досить великий вибір серед програм з автоматизації обліку та персональних даних. Найбільш популярними в Україні є програми компанії 1С, якими за різними джерелами користуються від 80% до 98% підприємців. Дані програми мають свої переваги та недоліки. Щодо негативних сторін, то на кожному підприємстві використовується унікальне рішення 1С, яке реалізоване не завдяки налаштуванню конфігурації, а запрограмоване власною мовою 1С. Тобто підприємець буде вимушений власноруч допрацьовувати та налаштовувати дану платформу під себе, що призводить до більшого використання ресурсів. І якщо великі компанії можуть дозволити собі це, то для малих даний процес виявиться затратним щодо часу та бюджету. Все налаштування та запуск здійснюється 1С-програмістом. Часто у клієнта виникають ситуації, коли треба отримати швидкі вирішення помилок та питань, тоді йому не обійтись без спеціальних компаній, котрі надають дані послуги або окремим програмістом, який буде здатним написати новий функціональний модуль, знайти та скорегувати помилки в коді, що був написаний до нього.

Компанія 1С досить часто випускає оновлення у зв’язку з помилками та змінами в чинному законодавстві України. Аби отримувати такі оновлення продуктів, треба придбати недешеву підписку. При цьому як в платформі, так і в будь-якій конфігурації присутня досить велика кількість багів від розробника, а сама система настільки складна і об'ємна, що виправити ці їх силами програміста 1С досить важко і найголовніше невигідно для кінцевого користувача. Більш того, як у платформі, так і в конфігураціях відсутня модульність. В результаті для виправлення багів доводиться встановлювати оновлення. При цьому оновлюється кожного разу повністю платформа й конфігурація, в той час як налаштування, додаткові плагіни й інша робота, проведена програмістом, повинна бути виконана знову. Сама компанія 1С зацікавлена в тому, щоб користувачі оновлювалися якомога частіше. Таким чином клієнти часто отримують нагадування про нові оновлення, попередження про необхідність оновити платформу або конфігурацію. Але при цьому на сайті немає достатньо докладної інформації про те, що саме отримає користувач в разі оновлення, які проблеми виправлені, які можливості з'явилися що. Тобто об'єктивно оцінити необхідність встановлення, того або іншого поновлення неможливо. В результаті багато користувачів оновлюються просто про всяк випадок. Оскільки відсутня модульність, то для того, щоб внести навіть найдрібніші зміни, доводиться вивчати всю платформу. Крім того, при оновленні платформи досить часто користувачі стикаються з тим, що ліцензійні ключі перестають працювати.

Одним із найважливіших недоліків також є низький рівень безпеки та захисту інформації. Завдяки набутій популярності програм 1С існує безліч способів незаконного доступу та викрадення даних. Їхня кількість має тенденцію до зростання. Більш того, програма не має багатокористувацького режиму роботи, тобто займатися обліком за допомогою базової версії 1С може тільки один користувач і тільки на одному локальному ПК. Одночасна робота з системою безлічі користувачів, наприклад, в досить великій організації допускається тільки версією ПРОФ. Ведення обліку декількох організацій одночасно, що є необхідним для великих організацій, також неможливе. Крім того, відсутня підтримка роботи з розподіленими базами даних, що є знову досить актуальним переважно для великих організацій.

Щодо переваг, то такою є безперечно вбудована об’єктно-орієнтована мова, спеціально розроблена компанією 1С, зручність інтерфейсу. Усі конфігурації мають відкритий код, тому будь-який 1С-прогаміст може її змінити чи дописати. Не зважаючи на те, що програми компанії 1С заборонені на території України та мають значну частину недоліків, вони є занадто популярними серед більшості підприємців.

На ринку України існують проекти і з невеликою вартістю ліцензії, де основні витрати припадають на підтримку продукту, однак такі рішення не володіють достатньо розвиненим функціоналом. У даних випадках клієнт приймає на себе всі ризики, пов'язані з такими можливими обставинами, як нестача фахівців для надання підтримки, повільне внесення змін для відповідності вимогам контролюючих держорганів. Серед систем, які користуються популярністю в Україні, в першу чергу варто згадати «Галактика» і «Парус». Варто пам’ятати, що ці продукти також російського виробництва, і підпадають під ті ж санкції, що й 1С. В Україні стають популярними аналогічні продукти з Німеччини, США тощо: Microsoft Dynamix Ax, Dynamix Nav, IFS, Epicor, Infor, Oracle та SAP. Для функціонування вищезазначених продуктів необхідна розвинена сучасна ІТ-інфраструктура, висококласні, а, отже, і дорогі, ІТ-фахівці підтримки. Безумовно вартість таких програм в рази, а іноді й у десятки разів, перевищує 1С чи інших українських аналогів.

Отже, у розробці власної системи управління персональними даними наша компанія буде звертати увагу в першу чергу на відповідність чинному законодавству України, зручність платформи, інформаційну захищеність та можливість використання даної системи у різних сферах. Досить важливо, щоб кожен працівник міг безперешкодно підлаштовувати її під свої потреби та легко міг розібратися в управлінні. Планується об’єднати якомога більше позитивних сторін із мінімально можливими недоліками. Аналіз ринку показав, що існує компанія-монополіст, продукти котрої мають велику кількість проблем, а західні аналоги часто є занадто дорогими, тому є доцільною розробка власної системи.

2.3. **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.

2.4. **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).

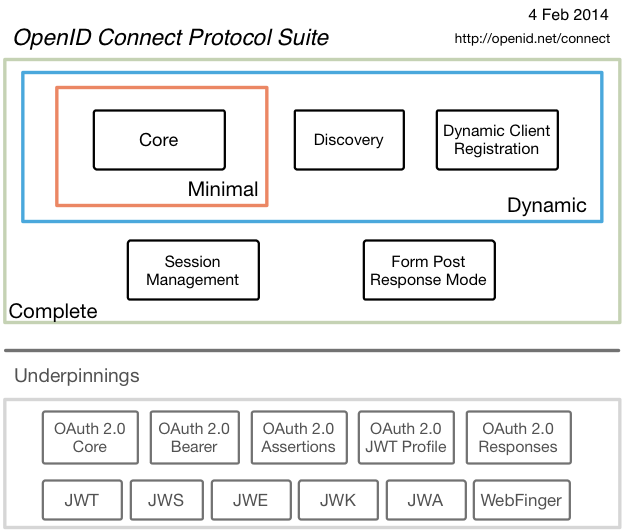
**2.5. СКУД**

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),

Рис. 1. Схема протоколу OpenId для аутентифікації користувача

[<https://openid.net/connect/>]

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.

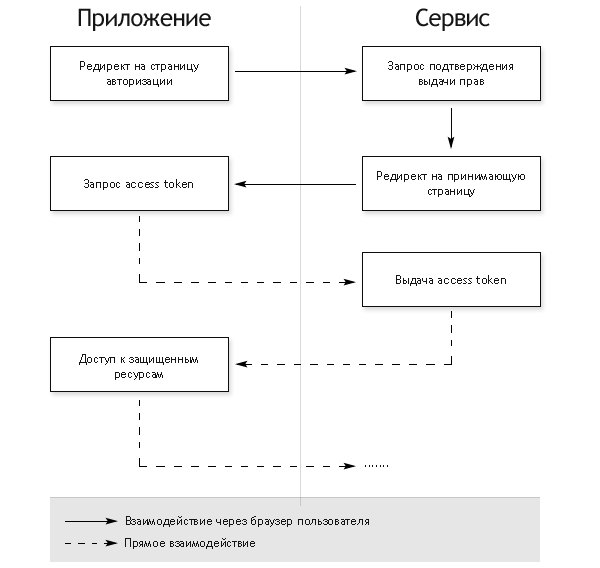
З позицій [інформаційної безпеки](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0" \o "Інформаційна безпека) Авторизація є частиною [процедури](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D0%B4%D1%83%D1%80%D0%B0" \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).

Рис. 2. Схема роботи системи під управлінням OAuth 2.0

[<https://sohabr.net/habr/post/115163/>]

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. Позиція адміністратора може являти собою додаткові обов’язки іншого працівника установи, наприклад працівника деканату.

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.

Окремим користувачам можуть бути надані права на часткове адміністрування системи.

**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.

**Використані джерела:**

1. Про захист персональних даних // <https://zakon.rada.gov.ua/laws/show/2297-17>
2. 1C: Підприємство // <http://1c.ua/>

### 6. Сценарії

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.1 |
| Назва | Реєстрація нового клієнта (викладача) |
| Учасники | Викладач, адміністратор, система |
| Передумови | Коректно заповнені форми на реєстрацію |
| Результат | Профіль клієнта (викладача) |
| Виключні ситуації | Некоректно заповненні форми |
| Основний сценарій | 1. Викладач отримує токен від головного адміністратора. 2. Викладач ініціює процес реєстрації. 3. Система надає викладачу форму для реєстрації. 4. Викладач проводить реєстрацію (вводить логіну та паролю, токен анулюється системою) 5. Викладач отримує права доступу в залежності від приналежності до групи користувачів. 6. Адміністратор перевіряє правильність надання прав. 7. Система створює профіль. |

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

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

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.2 |
| Назва | Реєстрація нового клієнта (студента) |
| Учасники | Студент, адміністратор, система |
| Передумови | Коректно заповнені форми на реєстрацію |
| Результат | Профіль клієнта (студента) |
| Виключні ситуації | Некоректно заповненні форми |
| Основний сценарій | 1. Студент отримує токен від головного адміністратора 2. Студент ініціює процес реєстрації. 3. Система надає студенту форму для реєстрації. 4. Студент проводить реєстрацію (вводить логін та пароль, система анулює токен). 5. Студент отримує права доступу в залежності від приналежності до групи користувачів. 6. Адміністратор перевіряє правильність надання прав. 7. Система створює профіль. |

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

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.3 |
| Назва | Реєстрація нового клієнта (бухгалтера) |
| Учасники | Бухгалтер, адміністратор, система |
| Передумови | Коректно заповнені форми на реєстрацію |
| Результат | Профіль клієнта (бухгалтера) |
| Виключні ситуації | Некоретно заповнені форми |
| Основний сценарій | 1. Бухгалтер отримує токен від головного адміністратора 2. Бухгалтер ініціює процес реєстрації. 3. Система надає бухгалтеру форму для реєстрації. 4. Бухгалтер реєструється (вводить логін та пароль, система анулює токен). 5. Бухгалтер отримує права доступу в залежності від приналежності до групи користувачів. 6. Адміністратор перевіряє правильність надання прав. 7. Система створює профіль. |

**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 в системі 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 ініціює процес входу в систему. 2. Система надає клієнту форму для входу. 3. Клієнт вводить логін та пароль. 4. Система опрацьовує запит та порівнює його із даними в базі. 5. Клієнт входить у профіль. |

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

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.6 |
| Назва | Зміна даних клієнта (студента) |
| Учасники | Адміністратор, деканат, система |
| Передумови | База даних, наявність профілю студента |
| Результат | Дані про студента змінені |
| Виключні ситуації | Студент відсутній в базі даних |
| Основний сценарій | 1. Деканат повідомляє адміністратора про необхідність зміни даних студента. 2. Адміністратор ініціює процес зміни даних студента. 3. Система надає форму для зміни даних студента. 4. Адміністратор виконує зміну в системі. |

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

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.7 |
| Назва | Зміна даних клієнта (викладача) |
| Учасники | Адміністратор, деканат, система |
| Передумови | База даних, наявність профілю викладача |
| Результат | Дані про викладача змінені |
| Виключні ситуації | Викладач відсутній в базі даних |
| Основний сценарій | 1. Деканат повідомляє адміністратора про необхідність зміни даних викладача. 2. Адміністратор ініціює процес зміни даних викладача. 3. Система надає форму для зміни даних викладача. 4. Адміністратор виконує зміну в системі. |

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

|  |  |
| --- | --- |
| Ідентифікатор | AF-1.8 |
| Назва | Зміна даних клієнта (бухгалтера) |
| Учасники | Адміністратор, деканат, система |
| Передумови | База даних, наявність профілю бухгалтера |
| Результат | Дані про бухгалтера змінені |
| Виключні ситуації | Бухгалтер відсутній в базі даних |
| Основний сценарій | 1. Деканат повідомляє адміністратора про необхідність зміни даних бухгалтера. 2. Адміністратор ініціює процес зміни даних бухгалтера. 3. Система надає форму для зміни даних бухгалтера. 4. Адміністратор виконує зміну в системі. |

**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, деканат, система |
| Передумови | База даних, наявність профілю студента |
| Результат | Профіль студента видалений із бази даних |
| Виключні ситуації | Профіль студента відсутній в базі даних |
| Основний сценарій | 1. Деканат повідомляє адміністратора про необхідність видалення профілю студента із бази даних. 2. Адміністратор ініціює процес видалення профілю студента. 3. Система надає форму для видалення профілю студента. 4. Адміністратор виконує видалення в системі |

**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 | Профіль викладача видалений із бази даних |
| Виключні ситуації | Профіль викладача відсутній в базі даних |
| Основний сценарій | 1. Деканат повідомляє адміністратора про необхідність видалення профілю викладача із бази даних. 2. Адміністратор ініціює процес видалення профілю викладача. 3. Система надає форму для видалення профілю викладача. 4. Адміністратор виконує видалення в системі. |

**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 | Профіль бухгалтера видалений із бази даних |
| Виключні ситуації | Профіль бухгалтера відсутній в базі даних |
| Основний сценарій | 1. Деканат повідомляє адміністратора про необхідність видалення профілю бухгалтера із бази даних. 2. Адміністратор ініціює процес видалення профілю бухгалтера. 3. Система надає форму для видалення профілю бухгалтера. 4. Адміністратор виконує видалення в системі. |

**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

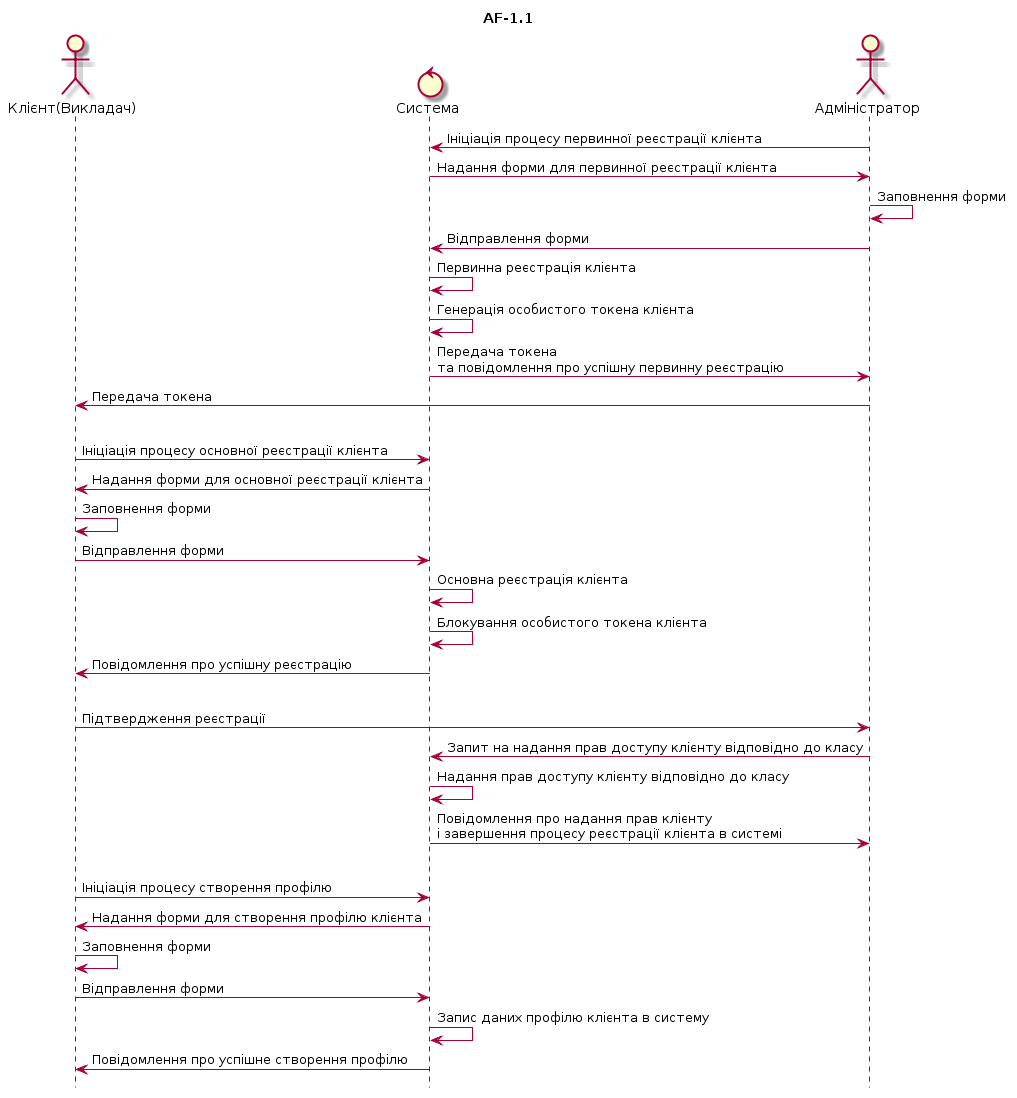


Рис. 3

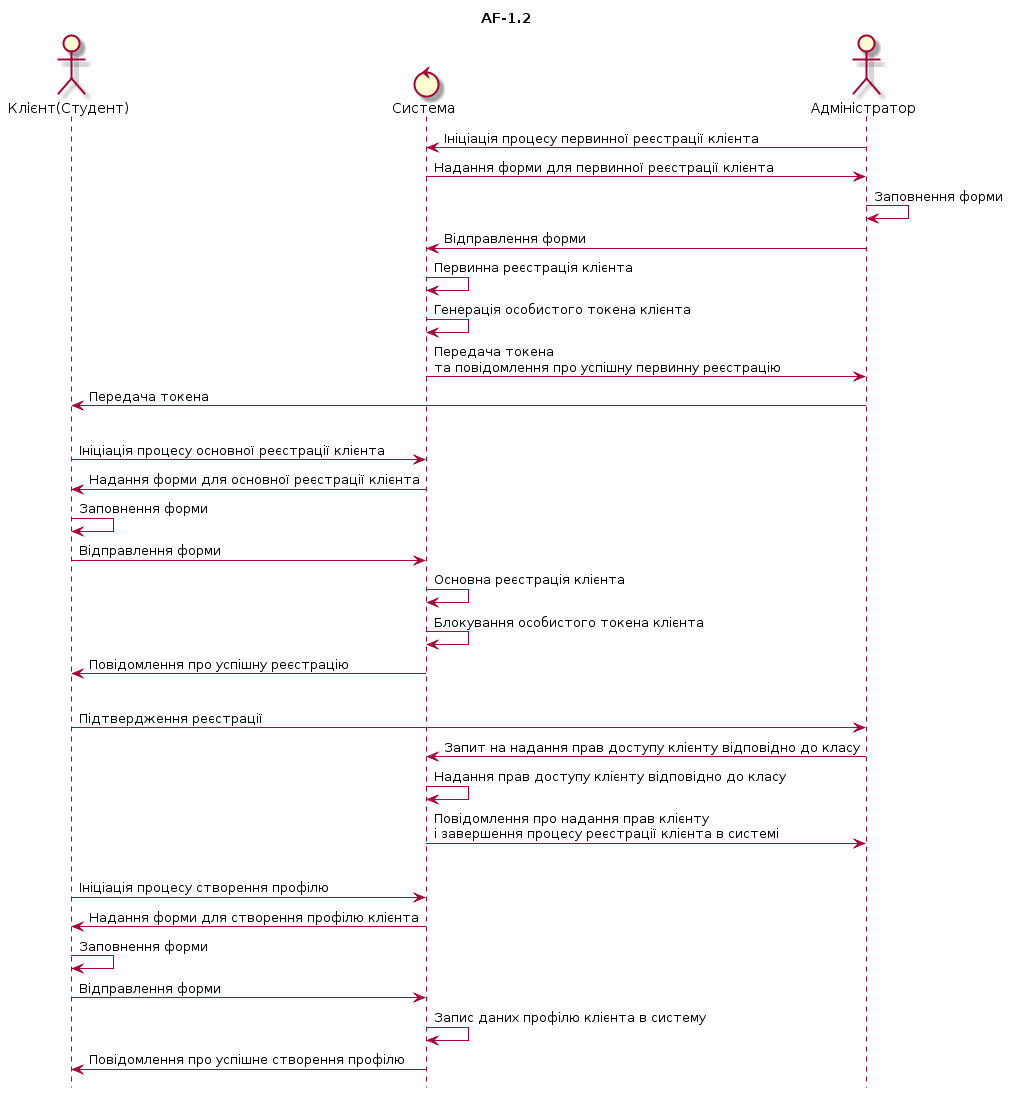


Рис. 4

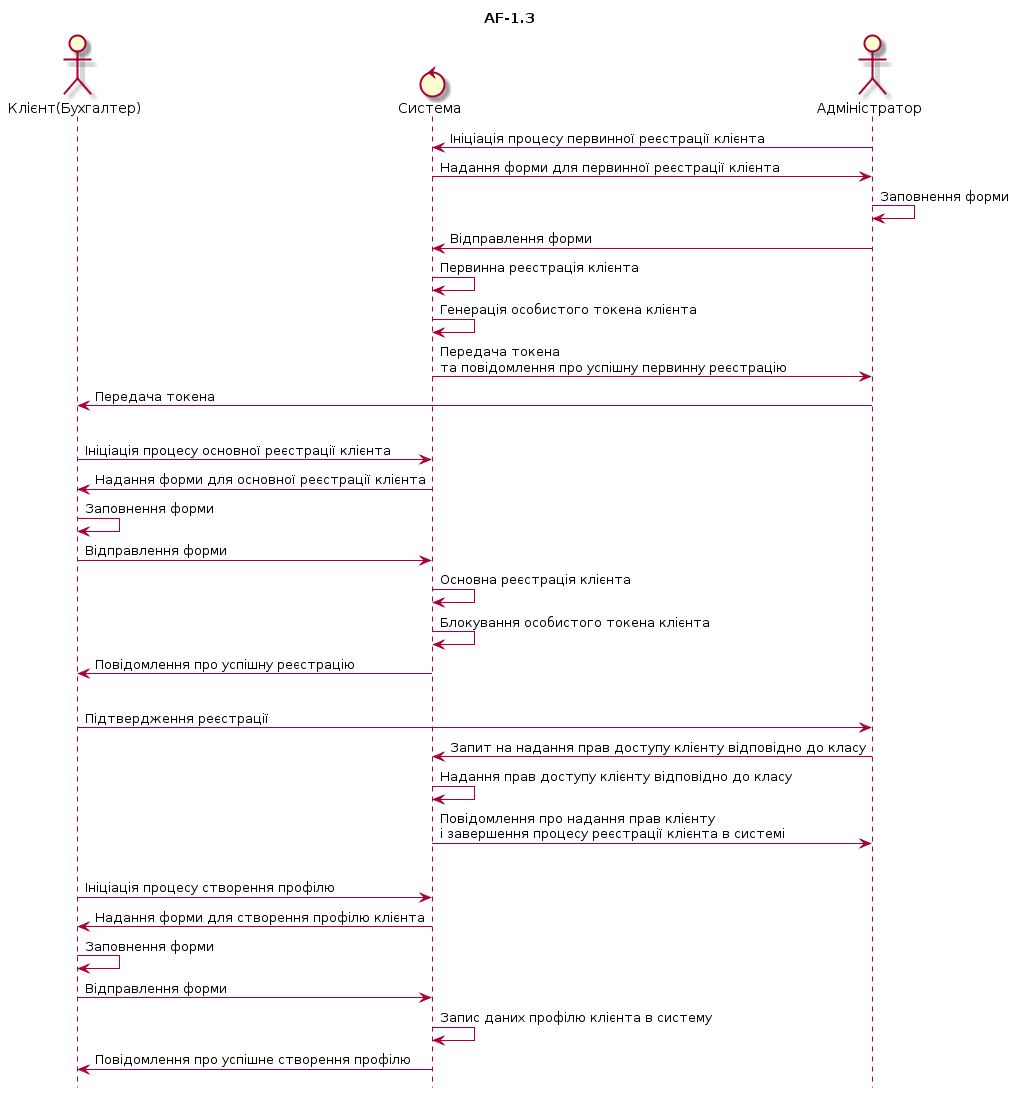


Рис. 5

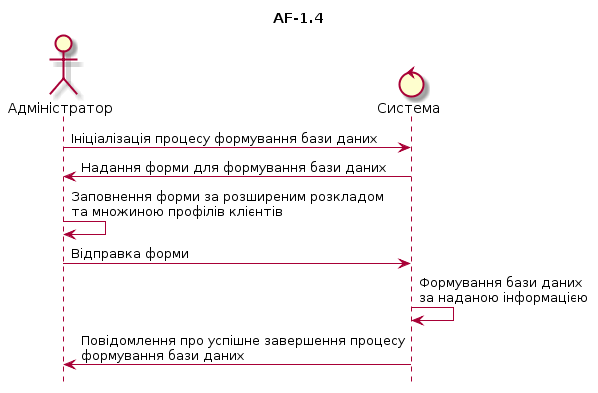


Рис. 6

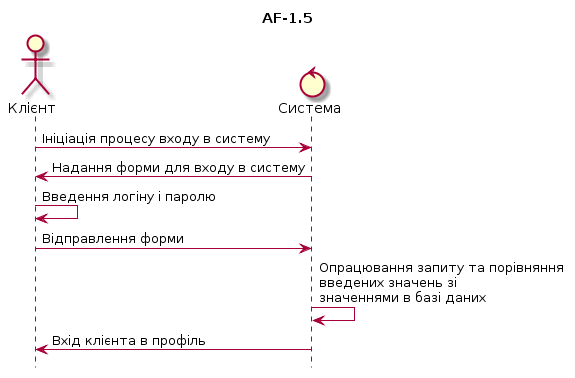


Рис. 7

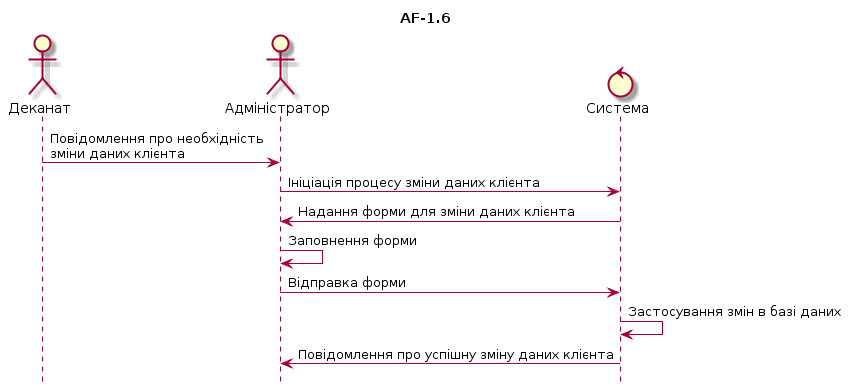


Рис. 8

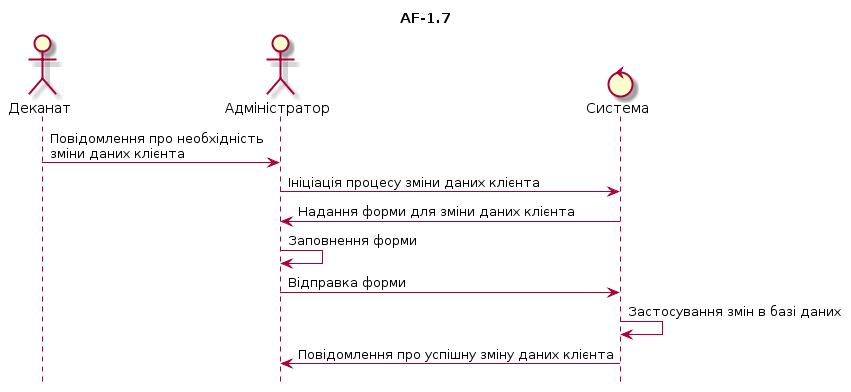


Рис. 9

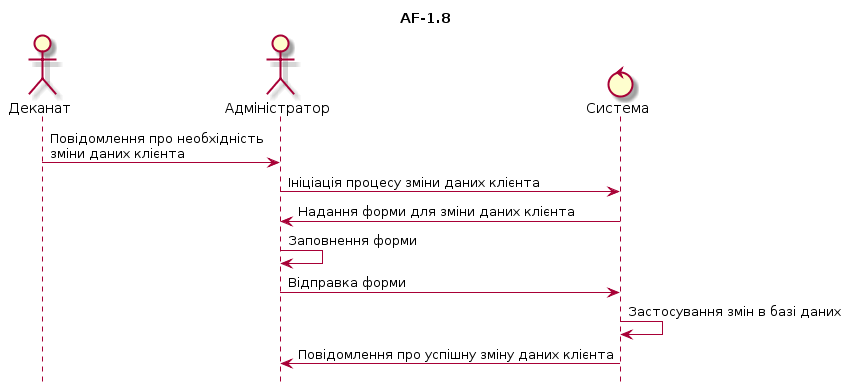


Рис. 10

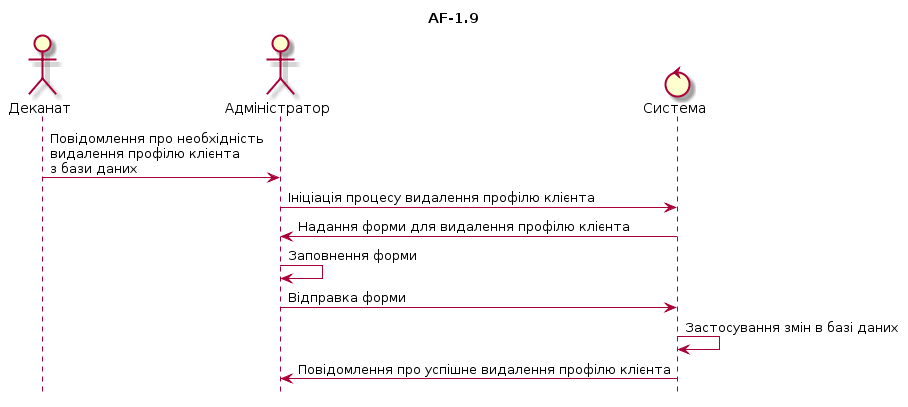


Рис. 11

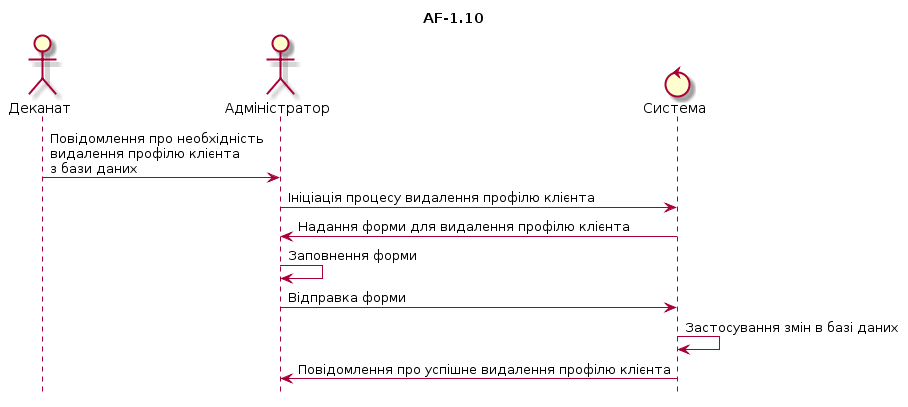


Рис. 12

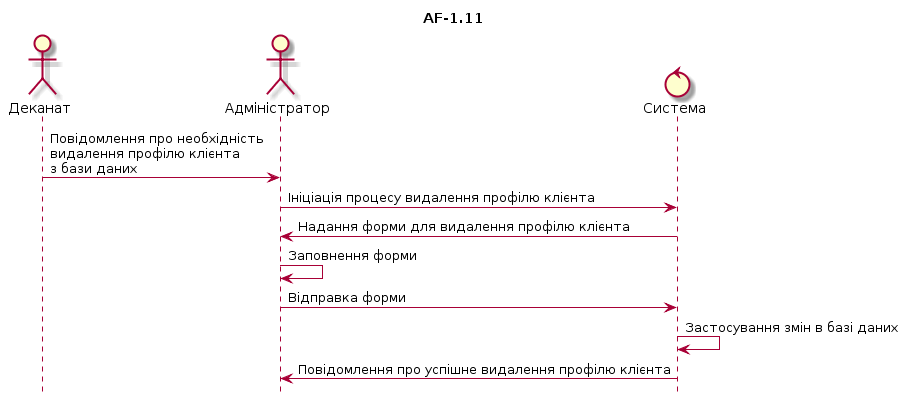


Рис. 13

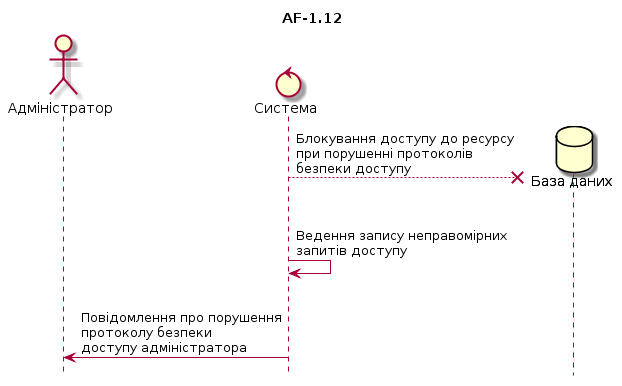


Рис. 14

### 8. Діаграма бізнес-процесів

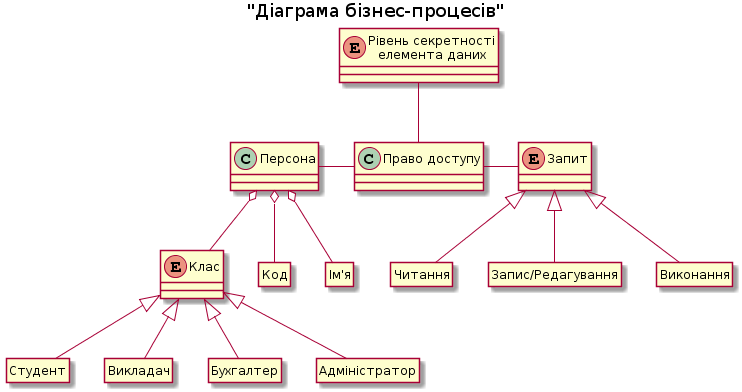


Рис. 15

### 9. Функціональність.

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

1. Деканат

2. Адміністратор

3. Клієнт (студент, викладач)

4. Бухгалтер

**9.1. Можливості зацікавлених осіб.**

10.1.1. 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.

5. Надання прав клієнтам.

6. Можливості комунікації з клієнтами і системою.

**9.2.2. Можливості клієнтів.**

1. Санкціонований доступ до ресурсу після реєстрації.

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

### 10. Практичність

**10.1. Стандартизація**

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

**10.2. 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.

### 11. 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.