НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

«На правах рукопису»
УДК 004.422.83

«До захисту допущено»

Завідувач кафедри
_____ І.Р. Пархомей
(підпис)

“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 121 «Інженерія програмного забезпечення»

на тему: Контроль доступу до файлів в системі електронного документообігу

Виконав: студент другого курсу, групи ІТ-74мп
(шифр групи)

Лобанов Іван Олександррович _____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник професор, д.т.н. Жураковський Б.Ю. ___ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

Рівень вищої освіти – другий (магістерський)

Спеціальність 121 «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ І.Р. Пархомей
(підпис)

«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Лобанову Івану Олександровичу
(прізвище, ім'я, по батькові)

1. Тема дисертації «Контроль доступу до файлів в системі електронного документообігу», _____
науковий керівник дисертації професор, д.т.н., Жураковський Б.Ю., _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «07»листопада 2018 р. №4112-с

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження – доступ до файлів в системі електронного документообігу

4. Предмет дослідження – забезпечення захисту доступу до файлів в системі електронного документообігу, комфортна робота з системою.

5. Перелік завдань, які потрібно розробити – аналіз проблеми та існуючих рішень; аналіз і реалізація алгоритму захисту; розробка моделі; дослідження ефективності розробленого методу.

6. Орієнтовний перелік ілюстративного матеріалу – шість плакатів

7. Орієнтовний перелік публікацій – дві публікації

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз предметної області	13.09.2018 р.	
2	Постановка задачі	15.09.2018 р.	
3	Аналіз інформаційного забезпечення	20.09.2018 р.	
5	Аналіз алгоритмічного забезпечення	25.09.2018 р.	
6	Розробка алгоритмічного забезпечення	15.10.2018 р.	
7	Розробка програмного забезпечення	01.11.2018 р.	
8	Маркетинговий аналіз стартап-проекту	10.11.2018 р.	
9	Висновки	15.11.2018 р.	

Студент _____ Лобанов І.О.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Жураковський Б.Ю.
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

У роботі розглянуто проблему не достатнього рівня захищеності файлів систем електронного документообігу, показано основні особливості існуючих систем, їх переваги та недоліки.

Розроблено безпечну систему електронного документообігу, що надає користувачам високий рівень захищеності персональних даних та обміну файлами. Дана система може бути використана на підприємствах, в компаніях та для особистого використання. Дозволяє збільшити рівень безпеки й захищеності документообігу у будь-якій сфері.

Ключові слова: електронний документообіг, алгоритми шифрування, Java, система, робота з файлами, RSA.

Розмір пояснювальної записки – 94 аркушів, містить 18 ілюстрацій, 28 таблиць, 6 додатків.

ABSTRACT

The paper considers the problem of insufficient level of security of files of electronic document management systems, shows the main features of existing systems, their advantages and disadvantages.

A secure electronic document management system has been developed, providing users with a high level of protection of personal data and file sharing. This system can be used at enterprises, companies and for personal use. Allows you to increase the level of security and security of documents in any area.

Keywords: electronic document flow, encryption algorithms, Java, system, file manipulation, RSA.

The size of the explanatory note is 94 sheets, contains 18 illustrations, 28 tables, 6 annexes.

Пояснювальна записка
до магістерської дисертації

на тему: *Контроль доступу до файлів в системі електронного документообігу*

Київ – 2018 року

ЗМІСТ

ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ

БД – база даних

ЕЦП – електронний цифровий підпис

ІО – індивідуальні особливості

ОС – операційна система

ПО – предметна область

ПК – персональний комп’ютер

ПЗ – програмне забезпечення

СЕД – система електронного документообігу

СУБД – истема управління базою данних

JSP – серверні сторінки джава

ВСТУП

Система автоматизації Документообігу – це потік документів в організації з моменту їх створення або отримання з інших джерел до моменту отримання для зберігання.

Документообіг - організаційно-технічна система, що забезпечує процес створення, контролювання доступу й поширення документів в електронному вигляді в комп'ютерних мережах й забезпечує управління потоками документів в установі або підприємстві.

Аби забезпечити електронний документообіг на сервері підприємства створюється база данних для зберігання всіх документів. Доступ до бази даних здійснюється різними шляхами. Доступ можливо організувати як через локальну мережу (внутрішню), так і через інтернет (зовнішню).

До документів можна добратися через певні виділені каталоги установи. Каталоги розподілені ієрархічно, структуровано підрозділам організації.

Редагувати усі документи має можливість та право лише особа, наділена певними правами та можливостями.

Основні принципи електронного документообігу.

Разова реєстрація документа, що дозволяє точно ідентифікувати документ в будь-якій установці даної системи.

Можливість одночасного виконання операцій над документами, що дозволяє прискорити роботу.

Безперервність руху документа, що дозволяє визначити відповідального за виконання завдання в кожен момент часу його життя.

Єдина база інформації про документи, що унеможливлює їх дублювання.

Система пошуку документа, яка дозволяє знаходити документ, володіючи мінімальною інформацією.

Система звітності яка інформує про різні статуси і атрибути документів, що контролює рух документів по процесам документообігу і приймає управлінські рішення за даними звітів.

Встановлення системи електронного документообігу, забезпечує велику гнучкість в роботі та зберіганні інформації і стимулює бюрократичну систему організації працювати швидко й більш продуктивна. Також, дана система породжує багато ризиків, тому не варто зневажати захистом, бо це велика загроза конфіденційності інформації.

Останні роки попит на системи електронного документообігу збільшуеться й, з легкістю можна прогнозувати, що ця тенденція продовжиться. Впроваджуючи СЕД не можна забувати про безпеку системи – є велика кількість шахраїв які хотіли б отримати доступ до чужих документів. Вже роками створюється велика кількість підручників про промислове шпигунство, комп'ютерні злочини, а ті в яких багато практичної частини дуже часто використовуються.

Базовим елементом будь-якої системи електронного документообігу є документ, в системи це може бути файл або запис в базі даних. Згадуючи про захищений документообіг, часто враховують саме захист документів, та їх захищену передачу, захист того що в них зберігається. Тут все зводиться до простого завдання - захисту даних від отримання до них доступу сторонніми особами.

Тут є велика проблема, адже зазвичай мова йде про захист системи, а не тільки про захист даних в ній. Можна зробити висновок, що потрібно захистити також і файли з якими працюють користувачі, рішенням може стати шифрування данних яким клієнти оперують при роботі з системою. Система – це живий організм, необхідно захистити його вміст й зв'язок між його внутрішніми елементами та забезпечити їх працездатність. Тому до захисту системи електронного документообігу необхідно підійти комплексно,

захиститит на всіх рівнях. Від захисту фізичних носіїв інформації та даних які зберігаються на них, до розгляду всіх організаційних питаннь.

Тож, в першу чергу необхідно захищати апаратні елементи системи. Це комп'ютери, сервери, елементи мережі та обладнання, тобто маршрутизатори, switch'i і т.д.. Необхідно звернути увагу на такі загрози, як поломки обладнання, доступ шахраїв до обладнання, втрата живлення й інші, на перший погляд, дрібниці.

Дуже важливим є захист файлів системи. Це програмні файли та файли бази даних, рівень між апаратними пристроями, логічними елементами та фізичними частинами. Якщо цього не врахувати, з'являється можливість впливу шахраїв або зовнішніх чинників на файли системи, не втручаючись в систему. Прикладом може слугувати пошкодження або втрата файлів бази данних в результаті помилки в роботі операційної системи або обладнання. Ніколи не можна нехтувати захистом документів та інформації, якими система оперує.

Виконуючи все вище-перераховане, можна побудувати систему, захищену по всім напрямкам, й встановити захист від загроз на кожному рівні. Це може виглядати параноїдально, але ціна такї безпеки не менше ніж саа система електронного документообігу, тому необхідно шукати баланс між захистом і вартістю.

Тож система безпечного електронного документообігу є дуже важливою для користувачів, компаній та підприемств для забезпечення безпечного та швидкого обміну важливими документами, максимально мінімізуючи будь-які хлопоти які виникають при роботі з паперовими документами.

РОЗДІЛ 1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

Аби сформувати вимоги до системи яку ми розробляємо, необхідно проаналізувати подібні системи які були створені раніше. Сформувати перелік необхідного функціоналу може допомогти ретельний аналіз, та визначити основні переваги та недоліки схожих систем електронного документообігу.

Електронний документообіг це сукупність процесів роботи з електронними документами та інформацією, це їх обробка, створення, редагування, видалення. Ці процеси виконуються за допомогую перевірки цілісності та за допомогою підтвердження факту одержання таких документів, якщо це необхідно. Електронний документообіг – важливий високотехнологічний крок на зустріч прогресу, який сприяє суттєвому підвищенню швидкості та продуктивності роботи підприємств, організацій, установ, органів, які встановлюють собі таку систему.

Верховна Рада України вже давно прийняла такі закони як: "Про захист інформації", "Про електронні документи та електронний документообіг", "Про електронний цифровий підпис", "Про Національну програму інформатизації", "Про телекомунікації", "Про Національну систему конфіденційного зв'язку в інформаційно-телекомунікаційних системах" та багато інших. В них описані основні засади електронного документообігу й прицнипи використання електронних файлів та данних. Тобто, можна сказати, що використання електронного документообігу законодавчо підкріплене та досить розповсюджено в багатьох організаціях та сферах України.

Загалом можна сказати, що системи електронного документообігу - це організаційно-технічні системи котрі відповідають за створення, керування доступом і розпоширення цифрової інформації у компьютерних мережах,та контролюють обіг документів в установі які її встановили.

Великою перевагою данної системи є те що вона може якісного й точного виконанувати дуже велику кількість задач документообігу та працює

з великим обсягом документів. Типи файлів,з якми зазвичай працюють СЕД, це текстові документи, зображення, електронні таблиці, аудіо- та відеодані і веб-документи. Система електронного документообігу призначена для організації та збереження документів в електронному вигляді,та роботи з ними, а саме, їх пошуку як за атрибутами і змістом. У СЕД зазвичай автоматично відслідковуються зміни в документах, сроки їх виконання, переміщення по каталогам, а також контролюються версії. Комплексна система обігу документів має охоплювати весь процес роботи з документами підприємства чи організації – починаючи створенням модератором або директором завдання по створенню конкретного документа до останнього моменту його життя, відправлення в архів. Також вона має забезпечувати збереження файлів та інформації у будь-яких форматах, це можуть бути навіть складні композиційні документи. У СЕД має бути чітке розмежування доступу користувачів до певних документів залежно від їх компетенції, прав доступу, посади. Також, система електронного документообігу має бути підігнана під конкретну організаційно-штатну структуру і систему роботи організації, має мати можливість інтегруватися з існуючими системами.

Зазвичай СЕД користуються великі організації, підприємства, банки та інші структури, які при роботі працюють з великою кількістю документів, створюють велику массу інформаційну массу яку було б дуже комфортно та просто тримати в електронному вигляді.

Основні принципи за якими функціонує електронний документообіг є разова реєстрація файлу, можливість одночасного виконання різних операцій аби скоротити час обробки й продовження роботи, підвищення оперативності й продуктивності виконання операцій над файлами. Руху документа не призупиняється. Є основна та едина база інформації про файли для зберігання документів в одному місці й уникнення випадків дублювання файлів, швидка та налагоджена система для пошуку файлів, система звітності документів, яка

інформує про статус документа в певний проміжок часу, за допомогою якого можна поетапно контролювати рух документів.

Провівши аналіз, можна сказати, що більшість вітчизняних підприємств коритуються пакетом програмного забезпечення від корпорації Microsoft, аби забезпечити електронний документообіг,це можна пояснити тим що він дуже зручний в експлуатації та має великий спектр можливостей для подальшого розвитку.Тож, на мою думку, більш актуальним буде огляд характеристик систем електронного документообігу, які працюють на платформі Microsoft, визначення їх можливостей, технічних характеристик, вартості, та складності. Найцікавішими та поширеними СЕД на вітчизняному ринку є такі:

Система "Справа". Компанія "Електронні офісні системи" являється її виробником. Данна система створена для автоматизації управлінської діяльності в вітчизняних міністерствах і відомствах, місцевих органах влади, та в інших організаціях які організовують свою діяльність в різних сферах.

DocsVision або "Архів-Діловодство". Данну систему створила фірма DocsVision. Ця система позиціонує себе як закінчений додаток, створений для роботи з архівівами документів, автоматизації всіх процедур по роботі з документами в організації та бізнес-процесів по обробці файлів та обігу інформації на підприємстві.

"Кодекс: Документообіг". Її розробила компанія ДП "Центр комп'ютерних розробок". Ця система електронного документообігу являє собою комплексвсіх пов’язаних між собою систем по роботі з файлами, створена для великих баз з документами і корпоративних сервісів по роботі з файлам, які автоматизують розв' язок задач по роботі з документами і документообігу. Зазвичай це органи державної влади й організації схожі з ними за осягом.

"ГРАН-ДОК" для Microsoft Windows. створена компанією Граніт-Центр. Ця система керування обігом документів відноситься до серії Documentum 4, вона вирішує великий спектр задач по автоматизації документообігу в

організації які пов'язані з діяльністю різних частин підприємства, й автоматизує бізнес-процеси які є типовими для цих установ.

LanDocs створений компанією Ланіт, призначена для загальної автоматизації процесу роботи з файлами організацій та ведення електронного архіву файлів з якими вони працюють.

Lotus Notes від компанії Lotus, забезпечує можливість розроблення і розміщення програм групового забезпечення. Ця система електронного документообігу дозволяє клієнтам отримувати, моніторити процес обробки, спільно обробляти й створювати файли та інформацію по обробці документів, предоставляючи таким чином високий контроль.

0PTiMA WorkFlow від компанії 0PTiMA, керує процесами створення, обробки, збереження, моніторингу та видання файлів, та автоматизує усі основні єтапи які необхідні для ведення сучасного діловодства та реалізації документообігу в установах які працюють з великим обсягом данних.

Documentum 4i яку створила корпорація Documentum, це система автоматизації роботи з документами і документообігу для державних і муніципальних установ. Вона має великий рівень безпеки, який потребують організації такого типу[2,3].

Тому можна сказати що усі вище перераховані системи дуже добре підходять для автоматизації документообігу на підприємстві, але лише одиниці з них надають належний рівень безпеки, а деякі взягалі не позиціонують себе як безпечні. Це є наявним прикладом того що системи не надійно захищені але їми користуються такі важливі державні організації, втрата документів в яких, може призвести до великих збитків. Наприклад у судовій системі України використовується система "Діловодство", в яких захист файлів не стоїть на першому місці, але незважаючи на різноманіття систем автоматизації документообігу і діловодства, існують загальні вимоги, яким повинні відповідати ці системи, та в них нема такого пункту як захист.

До цих вимог відносять: зручність і простота в адмініструванні та користуванні, масштабовуваність – підтримка дуже великої кількості користувачів, можливістьзбільшення потужності тобто додання більшої кількості апаратних ресурсів для кращої роботи системи, розподіленість – аби з системою могли працювати будь- які користувачі з будь-яких регіонів, які працюють в конкретній установі, модульність – це можливість користувача обрати які модулі йому необхідні для роботи залежно від потреб та правильність їх функціонування між собою, відкритість – для того аби систему можливо було інтегрувати або додати якийсь сторонній функціонал, аби розширити або зпростити роботу, тим самим додаючи системі гнучкості, універсальність – щоб система могла коректно функціювати в будь-якому апаратному та програмному середовищі.

1.2 Огляд системи електронного документообігу “Діло”

Розглянемо систему «ДІЛО» від компанії «Електронні Офісні Системи» (ЕОС). Вона являє собою комплексне рішення по автоматизації процесу обробки та роботи з документами, та повноцінного електронного документообігу в організації. Даною СЄДО користуються в невеликих комерційних компаніях та в менших,розподілених холдингових, можливо навіть в державних структурах.

В 1996 році була випущенаперша версія «ДІЛО». На теперішній час її використовують більше 1500 компаній, підприємств, організацій України та країн СНД, а кількість конкретних осіб які її використовують більше 150 000. Цю систему, не даремно, було нагороджено «Сертифікатом Найвищого Якості».

Система являє собою тиражований продукт. Може безез будь-яких додатків вирішити завдання автоматизації електронного документообігу в більшості організацій, які хочуть перевести паперовий обіг в

електронний. Гнучко зпроектована система з легкістю встановлюється та налаштовується під будь-які забаганки замовника.

Система дуже легко і швидко налаштовується, дуже гнучко зпроектована,легка в адаптації до будь-яких потреб в документообізі в роботі з будь-якою кількістю робочих місць для користувачів.

Здатна забезпечити необхідний користувачам рівень захищеності файлів та відповідає усім нормам вимог українського документообігу й міжнародним стандартам.

Забезпечує конфіденційність електронного документообігу за допомогою використання ЕЦП й складних криптографічних алгоритмів та засобів. Компанія засновник цієї системи має всі необхідні сертифікати від служб безпеки для використання криптографічних засобів в своїй системі.

Надає можливості маштабного переходу з паперових документів на електронний документообіг тим самим розміщуючи файли в базу даних системи використовуючи застосунок «Потокове сканування».

Працює з проектами документів, файлами та інформацією, підтримує маршрутизацію і версійність.

З документами може пряцювати як у локальній мережі, так і дистанційно, здійснюючи обіг через інтернет, за допомогою застосунку «Діло-WEB».

Архітектура системи повністю відкрита що надає можливість поєднувати її з іншими сторонніми програми як від самої компані розробника системи електронного документообігу, так й від інших виробників програмного забезпечення.

До переваг цієї системи можна віднести швидкість пошуку та в можливість ведення документа від моменту його створення до направлення в архів, контроль виконання робіт по обробці файла, швидкість підготовки документу, комфортна робота з проектами, можливість створення звітів та ведення журналювання, можливість адміністрування доступу.

Для користувачів системи, а саме офісних працівників, можна виділити такі переваги: можливість реєстраці документів через систему довідників, візуалізація та доступ до інформації про обробку документа, швидкий та детальний пошук, наявність журналів передачі та реєстрів відправки обох типів, можливість створення звітів.

Візуалізує та забезпечує повним набором інформації про документ з яким проводяться роботи з моменту його формування до відалення.

Робота з вхідними та вихідними файлами реалізована в вигляді такого функціоналу: приймання та моніторинг вхідних та вихідних файлів, автоматизоване додавання прийнятих електронною поштою файлів, налаштування номеру файла відповідно номенклатурі, ознайомлення з звітами та їх створення за резолюціями, відправка файлів на обробку в середині організації користувачам які будуть з ними працювати, реалізація усіх складних пошукових запитів та збереження іх історії, відправлення оброблених файлів до архіву.

Цілковито реалізована підтримка всіх спектрів робіт з проектами документів, створення задач по обробці, внесення змін до файлу або проекту. При внесенні змін йде резервне копіювання та логування всіх внесених змін, тобто реалізована система контролю версій. Реалізовано процес електронного узгодження документа, можливість його реєстрації та формування доручень які мають бути виконані з цим файлом. Робота з документом реалізована таким чином, що коженклієнт може виконувати певну частину по обробці. Його обов’язково хтось контролює, й все це відображено в інтерфейсі. Тоб-то створюються цілі ієрархічні дерева резолюцій. Далі документи передаються співробітникам на ознайомлення. Контролер може повністю бачити весь процес обробкитак як система делегування функцій контролю детально сформована. Реалізована підсистема контролю доступу до документів та інформації. Є можливість створення шаблонів.

Інформаційна безпека системи має можливості контролювання прав доступу користувачів до певних документів.Є конкретно сформовані для будь-якої організації рівні доступу які вони можуть налаштувати. Всі дії користувачів логуються та адміністративні особи мають можливість їх переглянути. В системі використовуються криптографічні застосунки, такі як цифровий підпис та шифрування документів.

Можливості зовнішньої роботи з данної системи, тобто через інтернет,дуже широкі. Будь яка особа яка має права доступу та являється співробітником організації яка встановила данну систему, де б вона не знаходилась, може підключитися до системи та отримати повний функціонал який вона предоставляє. Вона може реєструвати документи та користуватись функціями автоматичного заповнення, засвідчувати свій електронно цифровий підпис та перевіряти підпис файлів з якими працює. Може виносити резолюції та контролювати виконання роботи над документом, узгоджувати та підписувати проекти документів, проводити пошук файлів і резолюцій, переглядати та формувати звіти по внутрішньому та зовнішньом документообігу.

В наші часи усі підприємства та організації переходять або вже працюють з документами та файлами в електронному вигляді.Велика кількість з них працюють з використанням систем електронного документообігу.

Весь потік документів, створення, виделення, редагування та копіювання проходять в електронному вигляді. Всі вхідні та вихідні потоки інформації та файлів в організації переводяться в цифровий вигляд.

Впровадження систем електронного документообігу значно спрощують роботу офісних робітників та директорів підприємств, він прискорює процеси обробки інформації та спрощує процедури пошуку та обробки. Дозволяє з легкістю обмінюватися документами як в середини системи так і з зовні, між будь-якими особами які працюють з системою. Зменшується обсяг використовуваного паперу та допоміжних матеріалів, які необхідні для роботи

з фізичними документами, зменшуються витрати на копіювання, розмноження, створення та розповсюдження документів та на певних співробітників.

При електронній подаці документів виникають ризики з розкриття конфіденційності або безпеки. Аби ідентифікувати права доступу данного користувача в системах електронного документообігу використовують електронний цифровий підпис, який являє собою аналог звичайного підпису особи яка його завірила. Що значно спрощує життя користувачам.

Електронно цифровий підпис не тільки може затвердити особу яка підписала ним документ, а й гарантувати те що після цього в нього не було внесено ніяких змін.

При реєстрації вхідних документів, які отримує установа, особа яка контролює цей потік може поставити на ньому свій підпис на файл, підтверджуючи його справжність.

Вихідні документи та проекти теж потребують наявність електронного підпису для узгодження достовірності файлу, підтвердження завершення його обробки контролюючою особистістю, та подальшого направлення за циклом його обробки.

Аби використовувати цифровий підпис в системі розроблено спеціальний застосунок, він дозволяє підписувати документи цифровим способом й забезпечує безпеку ведення електронного обліку документів. Якщо існує така необхідність файл можуть підписади декілька осіб, залежно від єтапів його обропки та задач поставлених на нього, це дозволяє комфортно візуалізувати та налагодити процес обробки.

Аби залишити або перевірити цифровий підпис, достатньо одного натиску кнопки миші.Будь-яка людина яка потім працює с документом може побачити його та повністю бути впевненою в тому що документ справжній й не був відредагований сторонніми особами після підписання

Можливості модулю шифрування та електронних цифрових підпис дуже широкі, їх можна використовувати як при роботі з внутрішніми документами так і з зовнішніми, відправляючи підписані файли зовнішнім користувачам, які знаходяться в іншій філії цієї організації, клієнтам або партнерам, отдночасно шифруючи канал зв’язку, аби захистити канал й тим самим завадити перехопленню, пошкодженню або підмініінформації.

Якщо данна система встановлена у всіх учасників обміну документами, то вони разом з файлом отримують всю необхідну інформацію про нього. Тобто усі учасники корпоративног обміну отримують інформацію про цифровий підпис та мають можливість підписувати та поширювати отриманий документ. Це дозволяє підтримувати коректну роботу підприємства на дистанційному рівні. Перевірка підпису в цьому випадку проходить так само легко як й у співробітника який знаходиться безпосередньо поруч з установою, тобто підпис директора установи, який затверджує його узгодження з данним файлом, можна перевірити одним натиском кнопки миші.

Кожен робітник який має право підписувати документи, на початку роботи отримує ключ, який являє собою пару згенерованих ключів, приватного й відкритого.

Секретний ключ користувач системи може занести на будь- який фізичний носій, або на електронний ключ, аби він постійно був разом з ним. Аби завадити втраті фізичного ключа, є можливість додаткового захисту його паролем.

Секретним ключем, робітник, який має права доступу, може підписати файли для їх підтвердження або для дешифрування інформації яка була для нього зашифрована та надіслана електронною поштою. Аби підписати отриманий документ, користувачу необхідно лише підєднати носій на якому розміщено ключ до машини на якій він хоче зчитати файл або залишити підпис, й натиснути кнопку підпису.

На основі відкритого ключа формується сертифікат, який надалі використовують для перевірки цифрового підпису й достовірності що підпис був залишений саме тою особою яка це мала зробити.

Секретні ж ключі співробітників та їх сертифікати створює адміністративна особа яка відповідає за централізоване управління системою ключів, яка являється набором програмного забезпечення та застосунків для запису та зчитування носіїв-ключів.

Централізована система управління ключами являється центром організації безпеки в організації, підприємстві або філії. Він видає сертефікати які потім можуть бути підписані особами які стоять вище засвідчуючого центру. Дана система розміщується на окремій фізичні машині або сервері, який функціонує самостійно, видаючи підписи, й не підключеному до жодної мережевої лінії з засад забезпечення безпеки роботи організації й унеможливлення отримання підпису шахраями.

Адміністування централізованої системи управління ключами не вимагає особливих знаннь та навиків, все що необхідно корпорація предоставляє у вигляді простих гайдів по роботі, документація постачається разом із системою.

Отримати та встановити можливості використанн цифрового підпису та шифрування можна в трьох варіантах.

З отриманням повного функціоналу. Користувач може підписувати файли та інформацію, шифрувати данні які пересилаються, перевіряти підписи. Ті хто встановлює собі повнофункціональну систему також надають пристрій для перевірки й зчитування ключа з фізичного носія.

З непофним функціоналом перевірки підпису. Тобто якщо користувачу не потрібно підписувати документи а лише потрібно бачити інформацію про те чи підписали їх певні особи до того як він потрапив йому в руки то цей тип саме для нього. Також йому не потрібні ніякі пристрої та застосунки для зчитування ключів.

Функціонал дистанційної перевірки підпису. Такий функціонал предоставляється для тих хто пряцює з веб версією системи документообігу. Тобто у користувача є можливість перевірки підписів але немає можливості їх створювати. До цього пакету входить придбання та встановлення серверу який буде перевіряти всі підписи будь-яких осію які працюють з системою дистанційно.

Тобто можна комбінувати варіанти встановлення системи, залежно від того які ресурси та можливості необхідні організації. Наприклад, можна придбати повний функціонал для всіх керуючих співробітників, аби вони залишали свої підписи, а для інших співробітників лише перевірку, аби вони були впевнені в достовірності й легітимності документів з якими працюють. Або взагалі всім придбати повний функціонал, тим самим тримати весь обіг документів під ретельним контролем, за кожним життєвим кроком документа.

Підсистема електронного цифрового підпису й шифрування використовується за допомогою криптографічного шифрування ”Кріпто Про” й сертифікування ФАПСИ. Інтегрування в систему данних застосунків виконано компанією ЕОС, та підкріплене ліцензіями ФАПСИ.

Система проводить документ протягом усього циклу його життя від створення, узгодження та обробки до відправки в архів або видалення.Процес обробки можна побачити на (рис. 1.1).

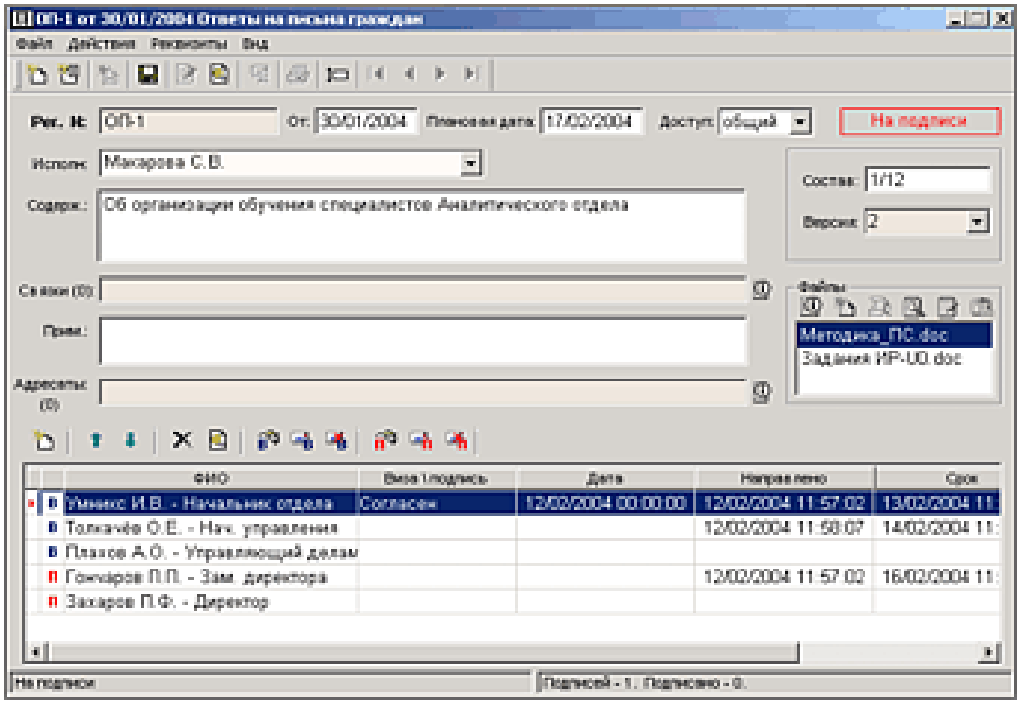

Рисунок 1.1 - Процеси обробки документів

Весь процес створення та обробки документа автоматизований та реалізований в системі, робота з проєктами документів проходить з виконанням таких процесів як створення РК проєкту, внесення змін до проєкту з системою контролю версій, затвердження проекту файлу, реєстрація файлу на основі проекту.

Під час роботи з проектом проводиться повний контроль над його виконанням, розглядаються терміни його підготовки, виконується його послідовна та паралельна маршрутизація (рис 1.2).

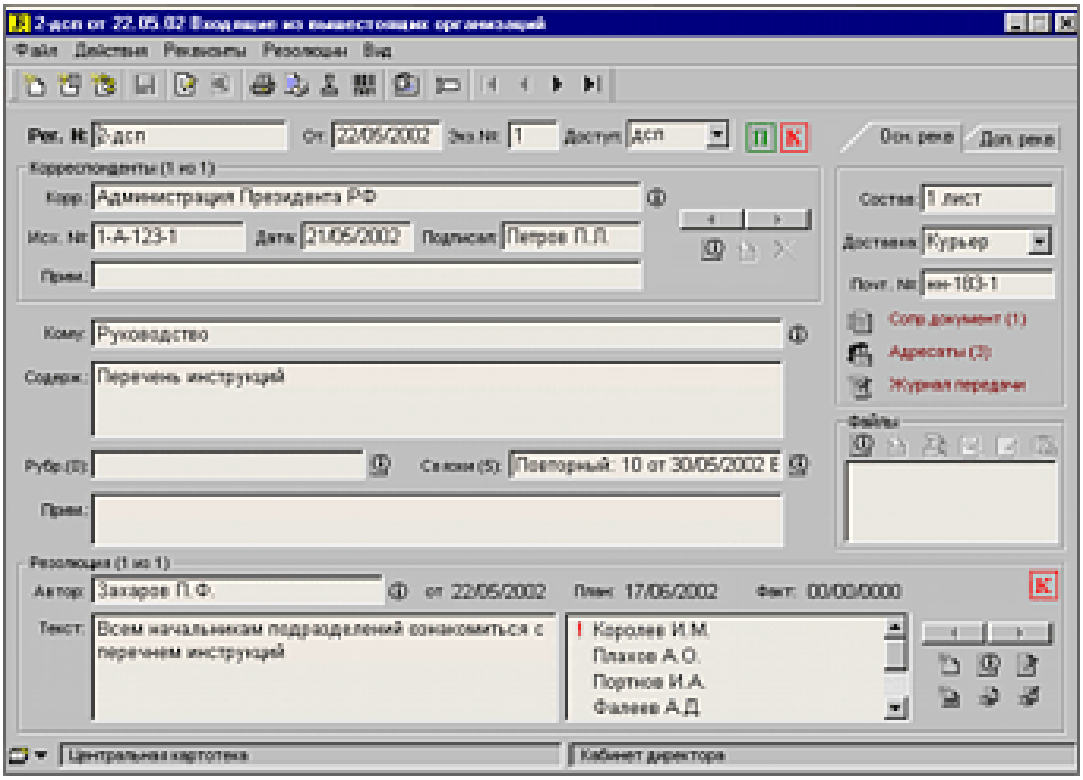

Рисунок 1.2 – Процес контролю та поля з даними

Реєстрація документів проходить послідовно, на першому етапі створюється його реєстраційна карта в якій знаходиться інформація файл. Реєстрацію проходять усі типи документів, як зовнішні, прийняті електронною поштою від різних філій організанції так і внутрішні, створенв безпосередньо в основній філії, в якій встановлена система. До таких документів відносять: договори, накази, листи, розпорядження, бухгалтерыські звіти та ін. В реєстраційній карті зазначаються: кореспонденти, зміст файлу, права доступу, наявність додатків, склад фалу, номенклатура та ін. Деякі поля можуть мати необмеженну кількість значень. Запити по резолюціям відображені на (рис. 1.3).

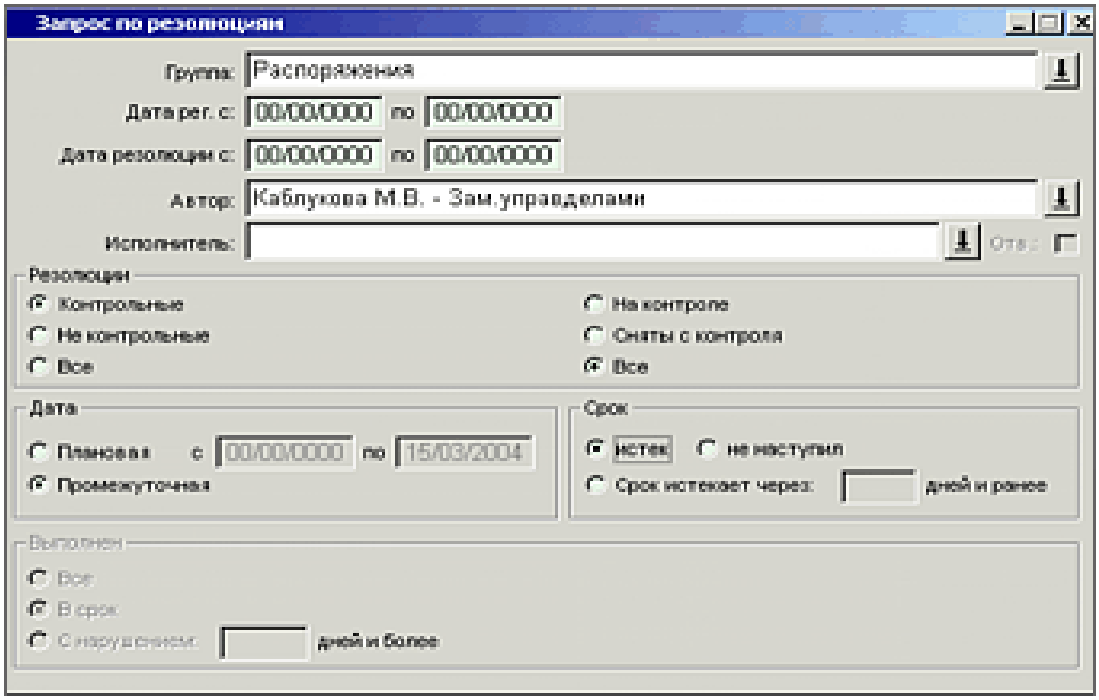

Рисунок 1.3 - Запит по резолюції

Контроль виконання робіт по обробці реалізований такиим чином що базується на виконанні резолюцій та виконання всіх завданнь по обробці самого файлу. Терміни виконання теж зазнають жорсткого контролю, тобто система виділяє документи з простроченим терміном або терміном який скоро зацінчиться, тим самим нагадуючи користувачам про терміновість його обробки, прискорюючи роботу обігу документів на підприємстві та збільшуючи продуктивність робіт. Є функціонал нагадування у вигляді повідомлень на електронну пошту робітникам яким було видане завдання по обробці. Таким чином користувач ніколи не пропустить завдання поставлене йому по обробці й завжди буде достатньо проінформований про єтапи виконання робіт.

1.3 Огляд системи електронного документообігу “LanDocs”

LanDocs являє собою програмный застосунок для формування системи електронного документообігу на підприємстві та автоматизованої системи контролю й управління контентом.

Позиціонує себе як застосунок для вирішення всіх завдань системи електронного документообігу та системи управління контентом, дозволяючи побудувати повний спектр реалізації СЕД будь-якої складності. Являється відкритою системою, що надає йому гнучкості в налаштуванні й впровадженні, для підприємства будь-якого типу. Система має можливість дистанційної роботи, тобто її мережа може включати в себе як головний офіс так і філії, чим розширює свій функціонал та об’єм робіт. Система електронного документообігу має характерну особливість так як вона реалізована в широкому спектрі робіт – автоматизує найважливіші бізнес-процеси організації й проста їх налаштуванні, не вимагає важких конфігурацій й орієнтована на звичайного користувача. Скоріш за все вам не доведеться викликати сторонню особу заради її налаштування, так як всі процеси конфігурацій дуже прості й описані в документації яка постачається разом з програмним продуктом. Ця система надає усі необхідні інструменти для тонкого налаштування роботи системи електронного докоументообігу відповідно необхідним потребам користувачів. Підходить для устаов будь-яких типів.

В ній реалізовані такі безнес-рішення як: узгодження документыв в цифровому вигляді, контроль виконнаня поставлених завдань по обробці файлів, органцізація обробки зовнішніх потоків інформації, формування детальної звітності, узгодження документообігу між філіями, захист електронних документів від шахраїв.

Lan Docs розробила компанія «ЛАНІТ». Після її встановлення, замовник отримує не просто систему а й усі послуги. Спектр послуг варіюється від моніторингу стану документаційного управління на підприємстві, до технічної підтримки коректної роботи системи, що є великою перевагою стосовно інших програмних застосунків цього типу. Функціонал який предоставляє система Lan Docs достатньо широкий аби охопити увесь спектр

послуг та потреностей якы необхыдны для пыдприэмст будь-якої сфери дыяльності та маштабів.

Lan Docs як програмний застосунк, створюючий технологічну платформу, дозволяє охопити весь необхідний для систем електронного документообігу функціонал й зформувати системи будь-якої складності, від простих до наймаштабніших.

Lan Docs простий для користувачів з низьким рівнем знань роботи з електронними документами та максимально близько приведений до тих умов робіт з якими працювали робітники при роботі з паперовими документами. Інтерфейс ситеми дуже доброзичливо налаштований на рядового фісного працівника. Особливістю Lan Docs є гнучкість та функціональність, що дозволяє налаштувати документообіг таким чином як того хочуть користувачі системи, максимально наблизивши умови їх роботи до комфортної зони. Гнучкість та відкритість дозволять налаштувати ситему для всіх типів організацій які хочуть перевести свій документообвг в цифровий вигляд.

Клієнт-серверне програмне забезпечення за допомогою якого реалізується захист, електронні цифрові підписи та шифрування, забезпечує інфрастурктуру відкритих ключів за Internet X.509 Public Key Infrastructure, та функції централізованого зберігання сертифікатів. Файли зашифровуються відкрито для користувачів, відповідно до їх власних ключів. Ведеться логування даних в спеціальному файлі, журналі захисту.

Є можливість використання кількох криптографічних засобів одночасно, це можуть бути основані на базовому криптопровайдері Microsoft CSP, або застосунки електронного цифрового підпису сторонніх компаній.

В Lan Docs є єдина база данних користувачів в якій зберігається інформація про права та доступ користувачів філій.

В Lan Docs інтегровані застосунки криптографічного захисту які підтримують інфраструктуру публічних ключів.

В сфері інформаційної безпеки Lan Docs реалізовує та предоставляє можливості аутентифікації користувачів при вході в систему, це може бути як ім’я і пароль так і засоби аутентифікації операційної системи, можливо з використанням криптографічних засобів, електронного ключа. Можливості розмежування прав доступу користувачів до файлів, підсистем та функцій системи певною особою яка має адміністративні права.

Використання електронного цифрового підпису для затвердження легітимності, приватності та безпеки роботи з файлом. Можливості шифрування конкретних документів які потребують більшої захищеності. Ведення стеження за роботою з файлами, тобто ведення тонкого та легкого в налаштуванні логування. Система веде детальний моніторинг доступу до підсистем, файлів та роботи користувачів в цілому.

Підтримка (на вибір замовника) одного з декількох криптопровайдерів (постачальників засобів криптографічного захисту): КріптоПро CSP (сертифіковане ФАПСИ), Кріптобанк (ЛанКріпто), Microsoft Base Cryptographic Provider (поставляється в складі ОС Windows), а також Тумар CSP (Республіка Казахстан), Енігма (Республіка Білорусь), Авест (Республіка Білорусь). Забезпечено можливість інтеграції з ПО інших криптопровайдерів.

Власний центр сертифікації, можливість інтеграції з зовнішніми засвідчують центрами.

Власне централізоване сховище сертифікатів, можливість інтеграції з сховищами сертифікатів зовнішніх центрів, що засвідчують.

Серверне програмне забезпечення для централізованого управління зберіганням змісту документів (файлів документів) в електронному архіві, здійснює підтримку операцій читання, записи, видалення, передачі файлів документів на довгострокове зберігання, протоколювання всіх цих операцій на спеціалізованому сервері під керуванням ОС Windows 2003/2008 / 2008R2 / 2012 / 2012R2. Приклад роботи можна побачити на (рис. 1.4).

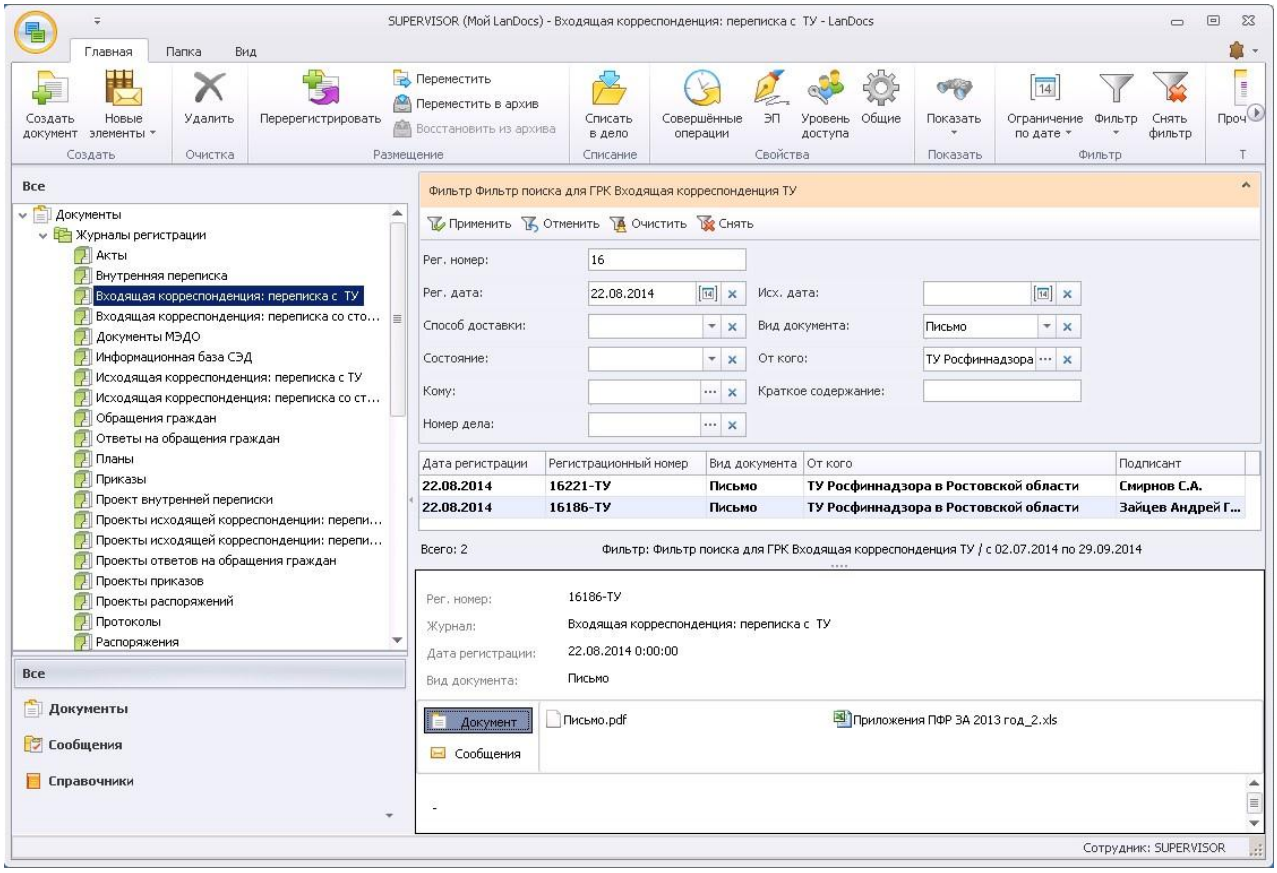

Рисунок 1.4 – Робота з вхідною кореспонденцією

ЛАНІТ готовий надати своїм замовникам наступні послуги зі зберігання документів в архіві:

- Позаофісне зберігання документів в знеособлених коробах з оперативним доступом до них (традиційний спосіб організації архівного зберігання документів);
- Відокремлений архів (організація корпоративного архіву замовника на території
- Спеціалізованого сховища);
- Архівний сейф (надання в оренду захищеної архівної осередки для найважливіших документів).

Зовнішнє зберігання документів в спеціалізованому сховищі дозволить:

- Оптимізувати витрати на зберігання, обслуговування і захист документів від різних ризиків;

- Знизити непрофільну навантаження на фахівців і вивільнити офісні площі;
- Налагодити систематизацію та облік документів.

Електронний архів організації - це система структурованого зберігання документів, що функціонує як незалежно, так і в складі будь-якої інформаційної системи корпоративного рівня.

Електронний архів забезпечує:

- Архівне зберігання будь-яких типів документів;
- Неможливість втрати інформації;
- Організацію та контроль доступу до документів;
- Оперативний пошук і розрахований на багато користувачів доступ.

ЛАНІТ має компетенцію і досвід створення електронних архівів будь-якого рівня - від архівної підсистеми СЕД підрозділу або невеликої організації до єдиної інформаційної системи корпоративного рівня або відомства федерального масштабу.

Архівна обробка - це рішення, що забезпечує зручну і прозору роботу з документами в повній відповідності до законодавства та вимог Росархіву. Приклад зображено на (рис. 1.5).

Архівна обробка документів дозволить:

- Дотримуватися вимоги законодавства при передачі документів на зберігання до державного архіву;
- Здійснювати швидкий пошук потрібної інформації;
- Систематизувати архів;
- Своєчасно знищувати документи;
- Оптимізувати передачу справ між посадовими особами;
- Відновлювати втрачену інформацію на основі архівуються документів;
- Підготувати справи до палітурки.

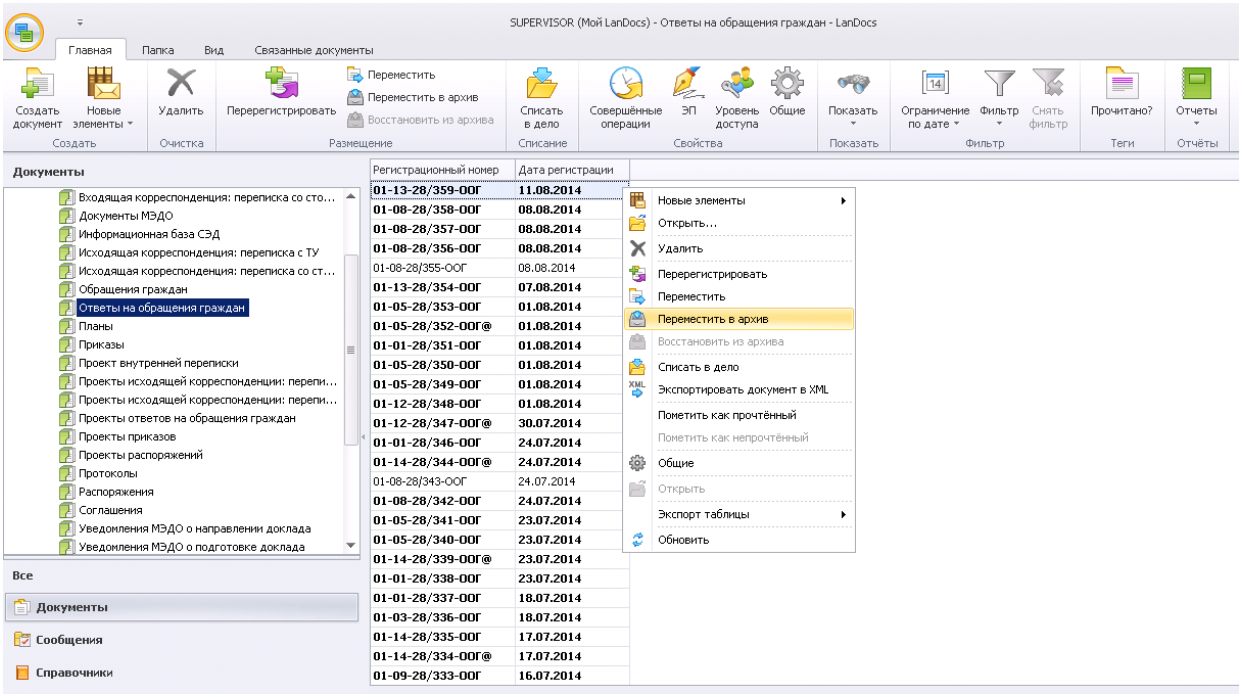

Рисунок 1.5 – Можливості обробки та демонстрація циклу

Висновки до розділу

Існує велика кількість систем електронного документообігу, усі вони надають користувачам величезний спектр програмного функціоналу для спрощеня роботи, прискорення та переведення в цифровий вигляд усього документообігу. Організації які хочуть встановити подібну систему й автоматизувати документообіг зазвичай витрачають велику кількість грошей на апаратну частину та встановлюють системи які простіше для них, але далеко не всі з них здані надати високий рівень безпеки при роботі з документами. Яку складну систему захисту не було б реалізовано в системі, завжди будуть ризики зі сторони навколишнього середовища або необережності користувачів. В проєктуванні власної системи документообігу, варто брати до уваги захист, орієнтуватися на користувача, враховувати усі потреби по обробці документів, тоб-то шаблони і норми. При проєктувані важливо реалізувати гнучкість системи, за рахунок розбиття на підсистеми, аби її можна було налаштувати під організації з будь-яким типом зайнятості.

РОЗДІЛ 2 РОЗРОБКА ТА ТЕСТУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1 Призначення та область застосування

Система призначена для забезпечення безпечного обміну документами та файлами між кліентами та сервером Дає можливість розміщення файлів на сервері та роботу з ними. Дозволляе контролювати доступ до файлів певним користувачам. Зашифровуе та розшифровуе данні якими оперують користувачі не навантажуючи їх зайвою інформацією. Призначена для підприємств різних типів, від маленьких до великих корпорацій, для обміну документами в середини підприемства.

Така система полегшує роботу з документами на підприємстві, надаючи можливість повного переведення документообігу в електронний вигляд. Системи електронного документообігу надають користувачам гнучкий підбір функцій, який потрібен конкретним організаціям, незалежно від маштабу, форми власності та сфери діяльності, для представників малого бізнесу та найбільших підприємств на ринку.

Такі систему мають велику кількість додаткових функцій які можуть спростити роботу, наприклад, планувальник завданнь, управління користувачами, автообробник документів. Вони максимально оптимізують звітність та велику кількість інших процесів. Захищають інформацію користувачів, економлять особистий час тих хто з ними працює й скорочують витрати підприємства. Спрощують обробку бланків відповідно до державних норм. Надійні в роботі й постійно підтримуються.

Всі вищеперераховані переваги роблять системи електронного документообігу дуже комфортним рішенням проблем паперового документообігу.

2.2 Характеристики та вимоги до СЕД

Технічні характеристики:

– операційна система: Linux, Windows 7, 8,10;

– оперативна пам’ять: 16 ГБ.

Вимоги до функціоналу:

– забезпечити можливість реєстрації. Система повинна забезпечувати можливість створення нового облікового запису.

– забезпечити можливість вибору конкретного файлу для передачі.

– зашифровувати, розшифровувати та перешифровувати конкретний файл з яким ведутся роботи.

– забезпечити можливість адміністрування над усіма користувачами системи, для більш широгого контролю доступу.

– можливість роздавання особистих завданнь кліентам.

– забезпечити передачу відкритих ключів між кліентами.

– можливість авторизованого входу. Спроектувати зручну форму для реєстрації / авторизації користувача. Реєстрація не повинна бути складною та довготривалою, форма має містити мінімум полів з метою спрощення процесу.

– забезпечити зберігання інформації в базі даних та занесення всіх змін і маніпуляцій в базу. Найпоширеніший, простий і надійний спосіб зберігати дані і обробляти їх.

– забезпечити можливість обміну повідомленнями між користувачами.

– система має бути інтуїтивно-зрозумілою, графічний інтерфейс повинен бути близьким будь-якому користувачу.

Системи електронного документообігу спідкають загрози які можна класифіковані таким чином. Загроза цілісності – втрата та пошкодження файлів та інформації, зміна структури файлу – випадково або в результаті певних збоїв, можливо й навмисна. Конфіденційність файлів – будь-яке втручання та отримання доступу до конфіденційної інформації, їх крадіжка,

перехоплення файлів. Загроза правильному функціонуванню системи – велика кількість загроз, при яких порушується або зупиняється робота системи; Це умисні атаки й помилки користувачів системи, помилки при роботі з обладнанням та в програмній частині.

Будь-яка система електронного документообігу має захищати від данних загроз. Встановлюючи СЕД, працюючи з інформацію, утворюється велика кількість загроз, але коли впорядкується документообіг можна спроектувати більш захищену від шахраїв та збоїв систему.

Існує дуже велика кількість загроз які необхідно врахувати: це, як неосвідченість адміністраторів систем, так і техніка, яка часто дає збої, незвичайні ситуації які дуже важко прорахувати. Як не пожежа в серверній, так в приміщенні, пожежники обов'язково зальють їх водою. Є певно встановлені користувачі системи: легальні, адміністративний IT-персонал, зовнішні зловмисники.

Помилки які можуть зашкодити нормальній роботі можуть виникнути від зареєстрованих користувачів, їх дуже багато – це скріпки в апаратних частинах, викрадення інформації та файлів з корисними цілями. Користувач системи – це потенційний зловмисник, він може спецыально або навіть не взявши це до уваги порушити конфіденційність інформації.

Дуже важлива группа – це адміністратори які слідкують за системою або особи які слідкують за її безпекою. Вони мають велику кількість прав доступу та повноваженнь, маючи певний доступ до файлів які зберігаються, обов'язково необхідно розглянути цю группу як потенційно небезпечну. Маючи не тільки доступ а й будучи найбільш кваліфікованими в питаннях безпеки, вони становляться в рази небезпечнішими. Не має різниці причина або мотив злодіяння яке вони вчиняють, будь це корисливі причини або помилка, інформація буде пошкоджена, або втрачена, або розкрита її конфіденційність. Дослідивши статистику, можна зазначити, 70 - 80% збитків від злодіяннь завдають чинники з внутрішньої частини організацій. До

зовнішніх можна віднести не велику кількість чинників. Це партнери або конкуренти, це може бути дивним, але й клієнти становляться причиною втрати безпеки роботи системи.

Система має завадити втраті, пошкодженню файліві, завжди має буди можливість відновлення скривджених документів. Проаналізувавши статистику, можна зазначити - 45% ситуацій втрати та пошкодження даних припадають на проблеми з фізичною частиною, 35% необережність та помилки користувачів й приблизно 20% – шахраї та вірусне програмне забезпечення. Аналітичні компанії приводять такі статистичні данні – більше 50% компаній натикаються на проблему втрати данних кожен рік. 33% з них спричинили дуже серйозні фінансові збитки. Їх представники стверджують, що причинами становляться: халатне ставлення до ынформаційного захисту компанії, та необережності користувачів, й лише 20% стверджують, що конфіденційність їх данних захищена належним чином. Оглядаючи системи електронного документообігу, можна сказати, що твердо впевненими в захисті своїх данних є лише 24%.

Загалом, в основі систем електронного документообігу зазвичай використовують бази даних Microsoft SQL Server або Oracle, зауважуючи на тому, що краще користуватися ресурсами резервного копіювання від розробника бази, тобто Microsoft або Oracle. Деякі системи мають свої власні підсистеми резервного копіювання,створені самим виробником системи документообігу. Тут не лише можливість відновлення пошкоджених файлів або данних а й відновлення системи якщо вона зазнала пошкоджень.

Зазвичай це враховують як безпеку системи електронного документообігу, що обмежує розуміння захисту системи. Доступ до даних в системі має забезпечуватися аутентифікацією та розмежуванням прав для забезпечення безпечного доступу.

Аби спростити, визначення особи користувача й процеси підтвердження його легітимності на різні типи дій та інформацію, будемо називати –

аутентифікацією, враховуючи весь комплекс дій, що мають бути виконані як при вході користувача в систему,так і впродовж його роботи з нею, постійно його контролюючи.

Звернемо увагу на способи аутентифікації. Зазвичай використовують парольний метод доступу, його основны проблеми, що знижують безпеку його роботи – це людський фактор. Змусивши користувача користуватися грамотно зформованим та згенерованим паролем, зазвичайвони залишають його запис на папері поруч з своїм робочим місцем, деякі, надзвичайно обдаровані можуть залишити його на самому видному місці, наприклад на моніторі.

Самий старий спосіб аутентифікації – фізичний. Колись, підтвердженням власності скрині була наявність у користувача фізичним ключем, зараз на першому рівні розвиток технологічного прогресу, і право власності й повноваження підтверджуються конкретним носієм інформації. Є велика кількість варіантів майнової аутентифікації: це USB-ключі, смарт-карти, магнітні картки, використовуються навіть такі застарілі засоби як дискети, і CD. Але й тут варто враховувати людський фактор, але шахраю все одно необхідно отримати доступ до самого фізичного ключа й отримати PIN-код.

Самим надійним методом ідентифікації та наступної аутентифікації являється – біометричний спосіб, де користувач ідентифікується за допомогою власних біометричних даних, тобтоце це може бути відбиток пальця, сканування сітківки ока, голос, та багато інших, данна сфера зараз на високому підйомі. Однак ці засоби можуть мати велику вартість рішення, а сучасні біометричні технології не на найвищому рівні й є багато практичних прикладів обходу описаних систем, аби завадити помилкові спрацьовування або відмови.

Також важливою є аутентифікація за кількістю врахованих факторів. Аутентифікація може бути однофакторною, двохфакторною і т.д. Можливо комбінувати данні засоби: парольний, майновий, біометричний.

Аутентифікація може проходити за допомогою пароля й фізичного ключа (двухфакторна аутентифікація).

Кожна система має розглядати розмежування прав користувача, обов'язково – чим гнучкіше і детальніше, тим краще, та білш захищено. Це може зайняти велику кількість часу на налаштування, а в результаті ми маємо систему яка має високий рівень захищеності. Цього ми досягнемо розмежувавши права в системі та технічно їх налаштувавшистворивши свою підсистему, або підсистему безпеки бази данних, яка встановлена в нашій системі електронного документообігу. Також можна комбінувати, використовуючи свої розробки й створюючи підсистеми бази данних. Це навіть краще, таким чином ми закриваємо недоліки підсистем захисту СУБД, в яких, само собою, є недоліки, так звані "діри".

Вагомим плюсом для конфіденційності файлів э криптографічні методи захисту документыв та інформації. Використовуючи їх ми не торкаємося конфіденційності файлу навіть якщо доступ до нього отримає шахрай. Обов'язково враховуємо, будь-який алгоритм криптографії має певну характеристику яку називають - криптостійкістю, це його захист і межа.Не існує таких шифрів та алгоритмів, які не можливо взламати та прорахувати – це питання часу і матеріального забезпечення того хто хоче його розшифрувати. Застарілі на данний момент алгоритми, які раніше вважалися дуже надійними, зараз душе швидко обхотять та взламують, розшифровуючи даніі які були захищені з їх допомогою. Аби зберегти конфіденційність необхідно прорахувати час, який займе взлом та розшифрування зашифрованої інформації, щоб до того часу вона застаріла, або ресурси, які підуть на її злом, будуть більші ніж цінність самої інформації, щоб злом не підкований економічно.

Організаційні заходи безпеки потребують дуже великої уваги. На скільки б криптографія не була надійною, шахраю не завадить нічого піддивитися документ іншими засобами, як варыант, напряму прочитавши

документ стоячи за спиною користувача, який маэ доступ до цього документа або файлу. Так само розшифрувати перехоплений файл, скориставшись ключем він якимось чином викрав у співробітника. Тому необхідно реалізувати роботу системи так щоб файли йшли на сервер в зашифрованому вигляді, обравши алгоритм RSA, таким чином оброблені документи будуть відправлятися на сервер в зашифрованому вигляді й прочитати їх можна буде лише за допомогою єдиного ключа, який збережений в системі й постійно змінюється, а відправити зашифрований файл зможе кожен клієнт, використовуючи відкритий ключ.

2.3 Розробка архітектури СЕД

У комп'ютерних технологіях трирівнева архітектура, яка передбачає наявність наступних компонентів програми: клієнтський застосунок («тонкий клієнт» або термінал), підключений до сервера застосунків, який в свою чергу підключений до серверу бази даних.

Клієнт - це інтерфейсний, зазвичай графічний, компонент, який представляє перший рівень, власне застосунок для кінцевого користувача. Перший рівень не повинен мати прямих зв'язків з базою даних (за вимогами безпеки), не повинен бути навантаженим основною бізнес-логікою (за вимогами масштабованості) і зберігати стан програми (за вимогами надійності). На перший рівень може бути винесена і зазвичай виноситься найпростіша бізнес-логіка: інтерфейс авторизації, алгоритми шифрування, перевірка значень, що вводяться, на допустимість і відповідність формату, нескладні операції (сортування, групування, підрахунок значень) з даними, вже завантаженими на термінал.

Сервер застосунків розташовується на другому рівні. На другому рівні зосереджена більша частина бізнес-логіки. Поза ним залишаються фрагменти, що експортуються на термінали, а також розміщені в третьому рівні збережені процедури і тригери.

Сервер бази даних забезпечує зберігання даних і виноситься на третій рівень. Зазвичай це стандартна реляційна або об'єктно-орієнтована СУБД. Якщо третій рівень являє собою базу даних разом з збереженими процедурами, тригерами і схемою, яка описує застосунок в термінах реляційної моделі, то другий рівень будується як програмний інтерфейс, що зв'язує клієнтські компоненти з прикладною логікою бази даних.

У правильній з точки зору безпеки, надійності і масштабування конфігурації, сервер бази даних міститься на відділеному комп'ютері (або кластері), до якого по мережі підключені один або кілька серверів застосунків, до яких, в свою чергу, по мережі підключаються термінали. Схему трирівневої архітектури зображено на (рис. 2.1).

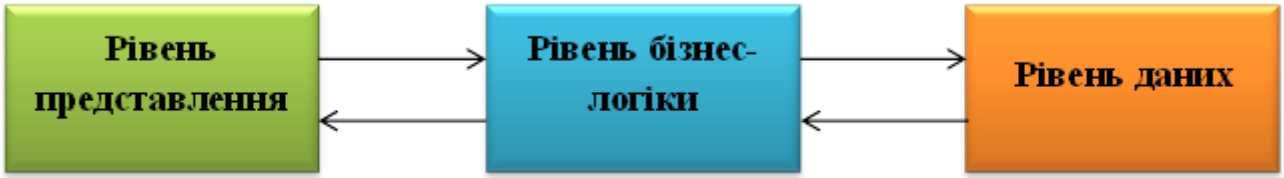

Рисунок 2.1 — Схема трирівневої архітектури

2.3.1 Розробка рівеня представлення

Рівень представлення в данній роботі виглядає як веб інтерфейс користувача в браузері, реалізований за допомогою JSP.

В представленному в данній роботі прототипі реалізовані такі JSP як: download.jsp, footer.jsp, header.jsp, message.jsp, profile.jsp, register.jsp, signin.jsp, upload.jsp.

Приклади роботи з рівнем представлення користувача описані в (табл. 2.1, 2.2, 2.3, 2.4, 2.5).

Користувачі системи діляться на 2 типи: Користувач системи (User), адміністратор (Admin).

User — перегляд файлів та інформації про них, запит на окремі документи, обробка файлів, завантаження оброблених документів, огляд завданнь.

Admin — управління користувачами, створення задач для користувачів, модерація файлів, надання доступу користувачам до певних файлів, повний контроль документів, форумання задач користувачам, створення документів, контроль роботи користувачів, робота з базою даних,надання прав доступу певним користувачам до конкретних документів, технічна підтримка та забезпечення коректної роботи системи, своєчасне виявлення та виправлення неполадок.

При першому вході користувач бачить інтерфейс з повідомленням, який пропонує йому зареєструватися або залогінитись в системі, (рис. 2.2).

Рисунок 2.2 – Стартова сторінка

Таблиця 2.1 - Реєстрація нового користувача

Діючі особи	Новий користувач

Мета	Створення облікового запису в системі, реєстрація нового користувача.
Предумова	Користувач перший раз зайшов до системи та не має облікового запису.

Продовження таблиці 2.1

Успішний сценарій: Створюється новий обліковий запис в системі. Система зберігає логін та пароль користувача, генерується пара ключів для обміну данними з користувачем. Публічний ключ зберігається на сервері а приватний відправляється користувачу та видаляється з сервера.	
Результат	Створюється обліковий запис користувача, він отримує доступ до функціоналу системи.

Таблиця 2.2 - Завантаження та відправка файлу

Діючі особи	Користувач
Мета	Завантажити новий файл для певного користувача або для себе
Предумова	Необхідність в відправці файлу собі до архіву або конкретному користувачу.

Успішний сценарій: Файл завантажується на сервер до певної директорії. Система зашифровує його конкретним відкритим ключем та зберігає. Користувач, якому був відправлений файл буде оповіщений про отримання нового документа.	
Результат	В директорії адресата з'являється зашифрований файл який може відкрити та відредагувати тільки він.

Таблиця 2.3 - Отримання файлу

Діючі особи	Користувач
Мета	Скачування файлу з серверу для подальшої обробки.
Предумова	Наявність файлу в директорії користувача.
Успішний сценарій: Користувач скачує файл з серверу та відкриває його за допомогою власного приватного ключа. Система розшифровує та відправляє файл користувачу в початковому вигляді.	
Результат	Користувач завантажуе собі файл який був йому адресований або зберігався в його директорії.

Таблиця 2.4 - Видалення файлу

Діючі особи	Користувач
Мета	Видалення файлу з директорії
Предумова	Втрата необхідності в зберіганні файлу.
Успішний сценарій: Файл повністю видаляється з сервера. Система отримавши запит на видалення, видаляє файл з сервера.	
Результат	Файл видаляється з певної директорії

Таблиця 2.5 - Адмістрування користувачів

Діючі особи	Адміністратор
Мета	Видалення файлів, адміністрування користувачів, зміна данних.
Предумова	Необхідність в редагуванні та контролі роботи користувачів.
Успішний сценарій: Видаляються користувачі, надаються права доступу, редагуються файли. Система надає адміністратору повний контроль та доступ до інформації але не надає доступу до зашифрованих файлів. Користувач, з інформацією якого або файлами були проведені зміни буде оповіщений про це.	

Результат	Буде виконана обробка та адміністрування над користувачами, їх доступом та реалізований контроль документообігу.

Всі вищеперераховані можливості відображені на діаграмі використання.

2.3.2 Розробка рівня бізнес-логіки

Рівень бізнес-логіки в спроектованій системі займає робота з файлами, а саме шифрування, розшифрування, прийом та відправка файлів, генерація ключів, реалізація алгоритму RSA та алгоритму генерації пари ключів, реєстрація користувачів. Реалізація данних модулів відображена в вигляді діаграмми класів.

с

2.3.3 Розробка рівня данних

Рівень даниих в системі спроектовано таким чином, що всі данні зберігаються на сервері. Для збереження та роботи з ними було обрано Oracle Database - об'єктно-реляційну систему для управління базами даних від компанії Oracle, так як вона підтримується великою кількістю апаратних платформ та є надійно захищеною. В базі данних в таблицях зберігаються логіни, паролі та публічні ключі користувачів, за якими здійснюється шифрування данних для кожного конкретного користувача. Самі ж файли зберігаються в цій же базі але окремо, в піддерикторіях в яких зберігаються файли зашифровані одним приватним ключем які зможе прочитати та завантажити тільки той хто має приватний ключ до ціх данних. Приватні ж ключі не зберігаються в базі для забезпечення більшої безпеки. Кожен користувач при реєстрації зберігає приватний ключ у себе на носії або

локально, а з системи він видаляється. В кожного користувача своя директорія. Користувач в свою чергу бачить лише список власних файлів, то-то директорію яка була створена конкретно для нього, (рис. 2.3).

Рисунок 2.3 – Відображення списку документів

В розробленому прототипі можна побачити реалізацію відображення та збереження файлів на сервері. На малюнку зображена директорія користувача в якій збережені файли тільки для нього, зашифровані його публічним ключем. Крім цього користувача, отримати доступ до цієї директорії не може ніхто, окрім адміністратора. Але навіть адміністратор не зможе відкрити данні файли так як в нього немає ключа, тільки якщо він надавав ці файли користувачу. Тоб-то на рівні данних системи, мі маємо базу данних з директоріями користувачів та таблиці логінів, праолів та публічних ключів. Користувачі ж взаємодіють лише з своїми директоріями, а сервер з таблицями реєстраційних данних. На діаграммі розгортання, відображено рівень роботи з данними та відображена система взаємодії компонентів системи.Також робота з базою данних присутня на діаграммі послідовності.

Висновки до розділу

В результаті моделювання було зпроєктовано безпечну систему призначену для обміну документами на підприємстві. Прототип системи було розроблено за трирівневою архітекторую, на рівні представлення реалізовано веб інтерфейс оснований на JSP. На рівні бізнес-логіки було розроблено серверний модуль шифрування, роботи з файловою системою та користувачами. На рівні данних ми маємо базу данних в якій зберігаються файли користувачів в зашифрованому вигляді, їх реєстраційні данні та відкриті ключі. Такі системи в наш час є дуже необхідними й попит на них стає тільки більшим, їх встановлюють, або вже користуються, підприємства та організації всіх типів. Загалом такі системи мають бути захищеними, гнучкими, надійними, багатофункціональними та вести підтримку власної системи.

РОЗДІЛ 3 ВИБІР ТЕХНОЛОГІЙ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ

Для розробки даної системи були обрані такі технології реалізації, як мова програмування Java, СУБД Oracle Database, сервер Apache Tomcat. Використовувалися бібліотеки та застосунки: javax.crypto, Ciper, java.security , KeyPairGenerator, KeyPair, Apache Commons.

3.1 Описання структур ПЗ

Програмне забезпечення складається з клієнтської та серверної частини. Данна структура дуже росповсюджена на теперішній час. Система електронного документообігу повинна бути надійно захищеною, простою в використанні, та розумінні.

Серверна частина в цій сиситемі реалізовує всі функції необхідні для роботи з файлами, та підтримує весь цикл життя документа. Будь-яка система електронного документообігу має мати як мінімум двохрівневу систему захисту, наприклад, логіном і паролем та фізичним ключем. Аби війти в цю систему необхідно ввести логін та пароль, а для отримання файлів необхідно скористатися ключем, який видається кожному користувачу при реєстрації. Кожен клієнт отримує свою директорію для зберігання власних файлів та файлів які він отримує від інших користувачів. Всі данні зберігаються в базі данних й доступ до них може отримати лише особа з найвищим рівнем прав.

На серверній частині розміщена система шифрування яка шифрує та розшифровує файли за допомогою ключа, який отримує від користувача. Данний криптографічний застосунок дозволяє підтримувати безпеку в системі належним чином. Будь-яка особа яка отримала доступ до сервера не зможе отримати матеріали які зберігаються в директоріях користувачів. Модуль шифрування є дуже важливою частиною системи, саме він робить систему електронного документообігу безпечною, тому її можна назвати системою безпечного електронного документообігу. В системі присутні засоби

логування та моніторингу роботи користувачів, за допомогою яких можна отримати повний контроль над документообігом. Реалізована система видачі завданнь користувачам, які створюють адміністративні особи, та контролюють процес їх виконання. Серверна частина також надає повну інформацію про завдання, таким чином, що, якщо користувач отримав завдання, вона його про це сповістить.

Клієнт в свою чергу бачить перед собою простий та зручний в користуванні веб інтерфейс, зображений на рисунку 2.1. Через невелику навантаженість робочої області досягається простота розуміння кожним користувачем. Користувач, після введення логіну та паролю отримує доступ до повного функціоналу системи, окрім адміністративних. Він отримує інформцію про всі файли які знаходяться в його директорії та завдання по обробці які йому біли видані. Після виконання завдання адміністративна особа відмічає його як виконане й воно видаляється з списку. При отриманні файлу, користувачу надсилається повідомлення про новий файл в директорії.

Адміністраторам ж наданий більш широкий функціонал, вони мають всі можливості користувачів, можливості видачі завданнь, та не мають безпосереднього доступу до змісту файлів з якими працюють користувачі, якщо вони не є власниками цих файлів.

Данні ж зберігаються в базі данних й з ними працює сервер, тоб-то розшифровує та зашифровує, проводить реєстрацію користувачів та реалізує документообіг. Користувачі ж працюють лише з власними директоріями.

Модуль генерації ключів розроблений таким чином, що він генерує файли ключів та зберігає відкритий ключ в системі, в таблиці поруч з логіном, паролем та адресою директорії користувача. Приватний ключ він надсилає користувачу й видаляє аби не зберігати його на сервері, таким чином реалізується захист інформації від шахраїв. Так як система розміщується локально на підприємстві то перехоплення данних унеможливлюється. А так як файли зберігаються в зашифрованому вигляді й кожен файл зашифрований

конкретним ключем, отримання данних шахраями в рази ускладнюється. Навіть якщо вони отримають доступ до сервера, отримання данних з нього буде потребувати дуже великих ресурсів.

3.2 Вибір мови програмування Java

Java являэться об'єктно-орієнтованою мовою програмування, написані на ній програми транслюються в байт-код, який виконує віртуальна машина - програма яка переробляє байт код й надає інструкції обладнанню в вигляді інтерпретатора.

Байт-код повністю незалежний від операційної системи й обладнання на якому він виконується, в сукупності з таким підходом, це дозволяє виконувати програми написані на Java, на будь-якому пристрої, для якого існує відповідна віртуальна машина.

Найважливішою причиною, чому для системи безпечного електронного документообігу варто обрати мову програмування Java є гнучка система безпеки, віртуальна машина тримає процес виконання програми під повним контролем. Операції які перевищують встановлені повноваження програми, це може бути несанкціонований доступ до файлів та даних або спроба підключитися до іншого пристрою, призводять до термінового завершення роботи.

Недоліком віртуальної машини, зазвичай, називають зниження продуктивності роботи. Це спричинило деякі вагання в виборі, але питання безпеки стояло на першому місці. Також, певні вдосконалення збільшили швидкість роботи та виконання програм на Java:

транслювання байт-коду в машинний в момент виконання програми, можливість збереження версій класу в вигляді машинного коду, велика кількість застосувань, що надають можливість прискореної обробки байт-коду.

Провівши анліз, можна сказати, що більшість завдань які виконуються на Java займають приблизно в півтора-два рази більше часу, ніж для C / C ++, є ситуації в яких Java швидше, та іноді вона може бути навіть в 7 разів повільніше. Програма яка виконується на Java-машині споживає в 10-30 разів більше пам'яті, ніж на C / C ++. Google, провели дослідження і зазначили що, в Java, дуже низька продуктивність відносно інших мов й вона потребує більше пам'яті, грунтуючись на тестових прикладах на Java в порівнянні з тими самими програмами на C ++. Java постійно покращується та отримує багато нововведень, наприклад, останнім часом було додано новий HTTP-клієнт з підтримкою HTTP 2.0, веб-сокетів і заміненим Http URL Connection.

Основними сімействами й технологіями Java є Java SE - Java Standard Edition, API, Java Runtime Environment, для створення користувачем додатків-настільних систем. Java EE - Java Enterprise Edition, набір специфікацій для написання програмного забезпечення на рівень вище, тобто програми підприємств та організацій. Для розробки системи електронного документообліку, якою, скоріш за все, будуть користуватися на підприємстві, Java Enterprise Edition являється найбільш підходящою.

Є платформи які пропонують апаратну підтримку виконання Java. Це мікроконтролери, які виконують та оброблюють код Java на апаратному забезпеченні не вівикористовуючи JVM. Також це ARM процесори, що виконують байт-код Java користуючись Jazelle.

Java варто обрати, бо вона дає нам можливості: автоматичне керування пам'яттю, розширені можливості обробки виняткових ситуацій, багатий набір засобів фільтрації введення-виведення, набір стандартних колекцій: масив, список, стек й багато іншого.

В ній є засоби для створення мережевих застосунків, та застосунків з використанням протоколу RMI. Велика кількість класів, для виконання HTTP-запитів й обробки наступних відповідей.

В Java вбудовані засоби для створення багатопоточних додатків, ці засоби навіть були перенесені на багато інших мов. Також, уніфікований доступ до баз даних на рівні певних SQL запитів які базуються на JDBC, SQLJ, та доступ на рівні концепції об’єктів, які мають здатність до зберігання в базі користуючись Java Data Objects і Java Persistence API. Є підтримка лямбда виразів, замикань, функції та можливості функціонального програмування, велика кількість застосунків для реалізації багатопотокових програм[6,7].

Враховуючи всю вище представлену інформацію можна зроблено висновок що Java, хоч й пряцює повільно, та потребуэ великої кількості пам’яті, але вона має великий рівень захищеності та велику кількість додатків та технологій які знадобляться нам для росробки системи електронного документообігу. Тому, вибір данної мови є повністю доцільним.

3.3 Система управління базами даних Oracle Database

Система керування базами даних (СКБД) – це програмні і лінгвістичні засоби спеціального або загального призначення, які забезпечують керування використання та створення баз данних. До основних функцій СУБД можна віднести: управління данними в зовнішній пам’яті, в оперативній пам'яті використовуючи дисковий кеш, журналізація внесених змін, резервне копіювання і відновлення бази даних після збоїв та втрати данних, підтримка мови бази данних для визначення даних та маніпулювання ними.

Загалом, СУБД складається з таких компонентів: ядро, яке управляє даними в зовнішній і оперативної пам'яті та журналізує всі процеси, процесор мови, він оптимізує запити на створення, видалення та зміну машинно-незалежного внутрішнього коду який виконується,

підсистему підтримки часу виконання, котра інтерпретує засоби маніпуляції даними, які створюють користувацький інтерфейс з системи управління базами данних.

Також до СУБД відносятся зовнішні утиліти, які надають велику кількість додаткових можливостей для обслуговування системи.
СУБД можуть бути ієрархічними, мережевими, реляційними, об'єктно-орієнтованими, об'єктно-реляційними, локальні - коли всі частини локальної СУБД розміщуються на одній машині, розподілені - коли всі частини СУБД можуть бути розміщені не тількі на одній машині а на двох і більше, файл-серверні – на данний момент вже застарілі, клієнт-серверні.

Клієнт-серверна СУБД розміщується поряд з БД на сервері й забезпечує доступ до самої БД. Усі запити клієнта по обробці даних клієнт-серверна СУБД обробляє централізовано.

Недоліком таких СУБД є високі вимоги до сервера. А до основних переваг може нвіднести меншу навантаженість локальної мережі, централізоване управління, яке є дуже зручним, легкість та простота реалізації високої надійності, доступності й висока безпека. Тому було вирішено використовувати клієнт-серверну СУБД для системи електронного документообігу. З усіх клієнт-серверних систем управління базами, а саме: Oracle Database, Firebird, Interbase, IBM DB2, Informix, MS SQL Server, Sybase Adaptive Server Enterprise, PostgreSQL, MySQL, Caché, Лінтера, було обрано Oracle Database.

Також є вбудовані СУБД - це СУБД яка може складати собою частину деякого програмного продукту, й не потребувати процесу встановлення. Така СУБД створена для локального зберігання даних,й не підходить для спільного користування в мережі.

Фізично вбудована СУБД виглядає як бібліотека яку ми підключаємо. через додаток и отримуємо достп до данних через SQL або за допомогою певних програмні інтерфейсів. До таких СУБД водносять: OpenEdge, SQLite, BerkeleyDB, Firebird Embedded, Microsoft SQL Server Compact, Лінтера[8].

Для на шої сиситеми електронного документообігу ми обрали Oracle Database - об'єктно-реляційну систему для управління базами даних від компанії Oracle.

Oracle підтримується великою кількістью програмно-апаратних платформ, так як раніше її дуже часто портували та підтримували, на данний момент це трох послабилось але підтримка на належному рівні. До таких платформ можна віднести: Linux x86, Linux x86-64, Linux на zSeries, Linux Itanium, Linux на POWER, Microsoft Windows, Windows NT, Windows NT, Solaris x86, Solaris AMD64 / EM64T, Solaris SPARC , AIX5L, HP-UX PA-RISC, HP-UX Itanium, HP, Tru64 UNIX, HP OpenVMS Alpha, IBM z OS, Mac OS X Server, та багато інших.

До основних особливостей можна віднести MVCC або MultiVersion Concurrency Control, секціонування, автономні транзакції, Automatic Storage Management - автоматичне керування зберіганням файлів бази данних, Oracle Enterprise Manager – засоби які спрощують та допомагають керувати й слідкувати за СУБД Oracle й серверами, на яких вони знаходятся, підтримка послідовностей, аналітичні функції в SQL, Profile manage, Oracle Label Security, Streams, Advanced Queuing, Flashback Query, Real Application Clusters.

Real Application Testing – для зменшення витрат на випробування нової конфігурації, яку необхідно ввести, програмне або апаратне забезпечення, вона чудово відтворює навантаження робочого сервера, Data Guard – застосування яке дозволить створити резервний сервердля роботи в парі з основним, тим самим знижуючи навантаження й в будь-якій критичній ситуації може автоматично взяти на себе обов’язки й роботу основного сервера, Total Recall – зменшує навантаження на базу від застарілої інформації, рідко використовуваної, не вилучаючи можливості доступу до неї, не розкриваючи змін користувачу, об'єктно-орієнтований підхід, Automatic Database Diagnostic Monitoring, підказки для зміни плану виконання запиту.

Тож, створення та підтримка в актуальному стані бази даних є основним призначенням СУБД. Існує велика кількість СУБД, всі вони працюють по різному з різними об’єктами та предоставляють різний спектр функцій й засобів, та загалом, СУБД керуються єдиним комплексом основних понять. Враховуючи все вищеперераховане я обрав Oracle Database.

3.4 Сервер Apache Tomcat

Apache Tomcat – це контейнер за допомогою якого ми можемо використовувати інтернет застосунки, такі як джава, сервлети та JSP серверні сторінки джава. Пакети Tomcat в Ubuntu підтримують декілька варіантів запуску Tomcat. Ми можемо встановити його як поодиночно, на всю систему, так і в варіанті при якому він буде завантажуватись з системою від певного користувача. Але ми можемо розгорнути часткові його екземпляри які будуть завантажуватись з правами вашого користувача, що дозволить вам включати й виключати його власноруч. Цей варіант дуже корисний для сервера розробки, в якому певним користувачам необхідно тестувати власні екземпляри Tomcat. Tomcat використовується як самостійний веб сервер, як сервер контенту разом з веб сервером Apache HTTP Server, та як контейнер сервлетів.

Він складається з: Catalina, який являє собою контейнер сервлетів Tomcat й реалізує специфікацію сервлетів Servlet API. Він являється основоним для всіх інших Java технологій зв'язаних з Web й надає можливість динамічного генерування будь-якого веб контенту, використовуючи всі бібліотеки які доступні в java.

Coyote, який являє собою компонент HTTP Tomcat, який підтримує протокол HTTP. Coyote прослуховує підключення на певному порті TCP, переадресує запити до механізму Tomcat для обробки запитів й відправляє відповідь до клієнту який відрправляв запит.

Jasper, який являє собою механізм JSP Tomcat. Tomcat використовує Jasper, який аналізує JSP файли, щоб далі скомпілювати їх в Java код, як сервлети які далі йдуть на обробку до Catalina. Під час виконання він може автоматично виявляти зміни в JSP файлах та перекомпільовувати їх. В Jasper наявні деякі дуже корисні для роботинад нашим проектом можливості.

JSP бібліотеки тегів об'єднання. Кожен тег в файлі JSP оброблюється спеціальним класом обробки тегів. Об'єкти цього класу можуть об'єднуватись й використовуватись велику кількість разів в цілому сервлеті.

Фонова JSP компиляція, тоб-то під час перекомпіляції JSP Java коду, стара версія все ще є доступною й може виконувати запити. Старий JSP сервлет видалится тільки пісял того як новий сервлет завершив свою перекомпиляцію.

Компілятор Java JDT, Jasper може використовувати компилятор Java замість ApacheAntAnt й JAVAC. Це є дуже комфортним в тестуванні та розробці[1,10].

Його дуже легко встановлювати й він дуже легкий в експлуатації. Так як я використовую IntelliJ IDEA для роботи над проэктом, а Apache Tomcat надає дуже комфортний застосунок для данної IDE, й враховуючи всі вищеперераховані його можливості, я вирішив використовувати саме його в розробці системи безпечного електронного документообігу.

3.5 Бібліотека класів Security

Предоставляє класи та інтерфейси для забезпечення безпеки. Всі представлені класи легкі в налаштуванні, мають тонку архітектуру та контроль доступу. В ній реалізовані функції створення і зберігання пар ключів, для реалізації криптографії. Представлений ряд методів які використовються в криптографічних операціях, наприклад, перевірка і генерація електронного цифрового підпису. Загалом, цей пакет надає класи, для роботи з цифровими підписами, захисту об'єктів й генерації випадкових чисел. Данна бібліотека

входить до складу JSSE, й надає функціонал по шифруванню данних, аутентифікації клієнта з сервером та перевірці цілістності повідомлень. Саме цей функціонал нам був необхідний для проектування та створення прототипу системи електронного документообігу для забезпечення безпеки. Данна бібліотека дуже добре працює з такими криптографічними протоколами як RSA, RC4, DES, Triple Des, DSA, Diffie-Helman. Нас з цього цікавила підтримка RSA.

Вона підтримує спеціальні засоби для забезпечення безпеки системи, яка нам необхідна так як ми пряцюемо з веб середовищем, та підтримує безпеку при роботі в комп’ютерних мережах.

3.6 Бібліотека Crypto

Данна бібліотека надає класи й інтерфейси для криптографічних операцій. Він включає в себе шифрування, генерацію ключів і їх узгодження, генерацію Message Authentication Code (MAC). Саме ці можливості генерації ключів та узгодження необхідні нам для реалізації безпеки в системі безпечного документообігу.

Бібліотека надає можливості для роботи з симетричними та асиметричними методами шифрування. До неї також входять методи для безпечної роботи з потоками й захищеними об'єктами.

Цей класс визначає інтерфейс за допомогою якого можна власноруч дописати свій функціонал. Тоб-то будь-яка стороння особа може створити власні методи й фвласний фукнціонал який може бути підключений бескоштовно таким чином яким він необхідний користувачу. Кожен може створювати та переписувати реалізацію як йому заманется. Це є дуже корисним в нашому випадку так як ми створюємо власну систему безпеки.

Архітектура криптографії є доступною для розробки власного криптографічного функціональналу для платформи Java й включає API для великої кількості криптографічних служб. До них входять алгоритми

моніторингу повідомлення, алгоритми цифрового підпису, симетричне шифрування великих обсягів даних, симетричне потокове шифрування, асиметричне шифрування, шифрування яке базується на паролі (PBE), шифрування за допомогою еліптичних кривих (ECC), алгоритми узгодження ключів, генератори ключів, коди аутентифікації повідомлень (MACs), псевдо генератори випадкових чисел[12].

Для контролю над єкспортом та криптографії створений API функціонал, який знаходиться в пакетаі java.security та javax.crypto. Цей пакет містить класи, які не можна експортувати. А javax.crypto включає в себе класи, які можна єкспортувати.

Криптографічні інтерфейси сформовані таким чином, аби була можливість багаторазової реалізації криптографії. Деякі можуть виконати криптографічні операції в програмному забезпеченні а інші можуть виконувати операції на апаратному рівні. Засоби для керування єкспортом підкріплені цифровим підписом.

Платформа Java включає вбудовані засоби для реалізації великої кількості криптографічних алгоритмів, включаючи RSA, DSA, і алгоритми підпису ECDSA, DES, AES, також алгоритми шифрування ARCFOUR, MD5, SHA 1, і SHA 256, Diffie-Hellman і алгоритми узгодження ключів ECDH. Ці засоби реалізують криптографічні алгоритми в коді Java[12].

Існує велика кількість засобів для реалізації криптографії в Java, але для данного проекту чудово підходить бібліотека Crypto, так як в ній дуже добре реалізований процес генерації ключів та він дуже комфортний в роботі з RSA.

Саме через це, доцільним було обрати саме її в парі з java.security, для розробки системи безпечного документообігу аби прискорити та спростити роботу, так як на розробку власних методів та реалізацію RSA була б витрачена велика кількість часу. За допомогою данної технології в цій системі реалізоване шифрування RSA та використовувався метод для генерації пари ключів keyPairGenerator.

3.7 MD5 хешування

MD5 являє собою алгоритм 128-бітного шифрування. Тоб-то вхідні данні перетворюються за допомогою первного алгоритму в рядок бітів певної довжини. При цьому отриманий в результаті підрахунків результат представляється в шіснадцятковій системі счислення. Ця назмвається хеш сумою або хеш кодом. В нашій системі данний алгоритм використовується для шифрування паролів.

Процес хешування найчастіше використовується в веб індустрії, в основному для створення унікальних значеннь в масивах, та ідентифікаторах авторів.

Хеш кодування використовується для створення електронних підписів, зберігання паролів в базах данних систем безмеки, в межах сучачної криптографії для онлайн створення унікальних ключів.

Хеш, який ми отримаємо від функції, робота якої основана на цьому алгоритмі, повертає нам 16 байтовий рядок, тоб-то 128 біт. Цей рядок складається з 16 шіснадцядкових чисел. Зміна хочаб одного символа цього рядка приводить до фатального змінені значень усіх інших бітів.

Цей алгоритм має певні проблеми з надійністю. Враховуючи все вище перераховане він має надавати 100 відсоткову надійність, але існує ймоіврність колізій. Недоліком є легкість в находженні колізій при шифруванні. Але в нашій системі розшифрування пароля не призведе до втрати файлів так як шахрай, отримавши доступ до пароля все одно не зможе отримати зміст документів без приватного клча, який в ідеалі користувач тримає на переносному носії.

Цей алгоритм застосовується для перевірки цілісності файлів отриманих через інтернет. Під час активації програми його значення порівнюється з значенням в базі данних розробника. Для пошуку в файловій системі

дубльованих файлів, кожен з файлів має свій хеш код. Спеціальний застосунок сканує файлову систему порівнючючи хеши всіх елементів.

Цей стандарт кодування є одним з найпоширеніших методів захисту даних в прикладному і веб-програмуванні. Тому не буде зайвим забезпечити безпеку свого md5 хешу від навмисного злому.

Основний спосіб, що гарантує безпеку хешу вашого паролю, є використання “солі”. Він заснований на додаванні до паролю випадкових символів і подальшого змішування результатуів.

У багатьох мовах програмування для цього використовуються спеціальні класи і функції. Не є винятком з правил і серверні мови програмування.

Створити хеш код можна за допомогою функцій md5() та crypt(). При використанні ціх функцій в PHP для створення значення солі, використовують методи генерації псевдо-випадкових чисел. Такі як rand()[16].

При отриманні хешу можна виділити таку важливу особливість, формула перетворення одностороння, тоб-то з паролю можна отримати його хеш, але з хеша не можна отримати пароль.

Виходить, що коли ви логінитесь в систему зі своїм паролем, з нього вираховується хеш. Отриманий хеш звіряється зі збереженим хешем в списку користувачів який збережений в системі. Якщо вони однакові - значить введено правильний пароль.

Якщо вже зловмисник отримав списки усіх паролів системи то побачить лише хеші паролів. Їх не можна "розшифрувати", та за допомогою них не можна зайти до системи.

3.8 Вказівки з експлуатації

Система показує найкращі показники продуктивності на операційній системі Linux. Рекомендується використовувати Java не менше 8 версії та

сервер Apace Tomcat 9. Для коректної роботи з великим обсягом користувачів необхідно не менше 16 гб оперативної пам’яті на сервері.

Рекомендується встановлювати систему локально на підприємстві, не підключаючи до мережі інтернет, так як збільшуються ризики перехоплення данних шахраями.

Зберігати приватні ключі які видає система, рекомендовавно на переносних носіях, так як збереження файлу ключа на машині користувача може бути дуже небезпечним, так як він надає фінальний та найголовніший доступ до файлів які знаходяться в директорії користувача.

Рекомендовано використовувати великі та складні паролі при реєстрації для більш надійного захисту, з використанням різних символів, верхнього та нижнього регістрів.

Для забезпечення повного контролю та достатнього рівня безпеки, в системі повинна бути мінімум одна особа з адміністративними правами на 50 користувачів.

Для коректного функціонування без збоїв та підвисаннь, сервер необхідно перезавантажувати кожні 24 години, та не перевищувати ліміт користувачів системи, якій тісно пов’язаний з апаратним забезпеченням.

Кількість одночасних запитів на обробку файла не обмежена але також необхідно враховувати можливості сервера згідно з навантаженням.

Сервер необхідно встановлювати в спеціальному, чистому, ізольованому, приміщенні з обмеженим доступом фізичних осіб до нього, це підвищить безпеку роботи системи та зменшить ймовірність виникнення проблем спричинених людським фактором, або умовами середовища.

Усі підключення до сервера мають бути конкретно визначеними та індентифікованими.

Висновки до розділу

Була обрана мова програмування Java, хоча й пряцює повільно, та потребуэ великої кількості пам’яті, але вона має великий рівень захищеності та велику кількість додатків та технологій які знадобляться нам для росробки системи електронного документообігу. Для роботи з данними дуже чудово підходить Oracle Database. Oracle підтримується великою кількістью програмно-апаратних платформ, так як раніше її дуже часто портували та підтримували, на данний момент це трох послабилось але підтримка на належному рівні. Як сервер було обрано Apache Tomcat, він дуже комфортний в роботі, надійний та швидкий. Для безпечного зберігання паролів доцільно використовувати MD5 а для спрощення реалізації криптографії в модулі шифрування та підвищення безпеки, було вірішено використовувати бібліотеки Securiti та Crypto.

РОЗДІЛ 4 ТЕСТУВАННЯ

На початку роботи з системою, нас зустрічає головна сторінка на якій відображене повідомлення яке пропонує зайти до системи або створити новий обліковий запис, (рис. 4.1).

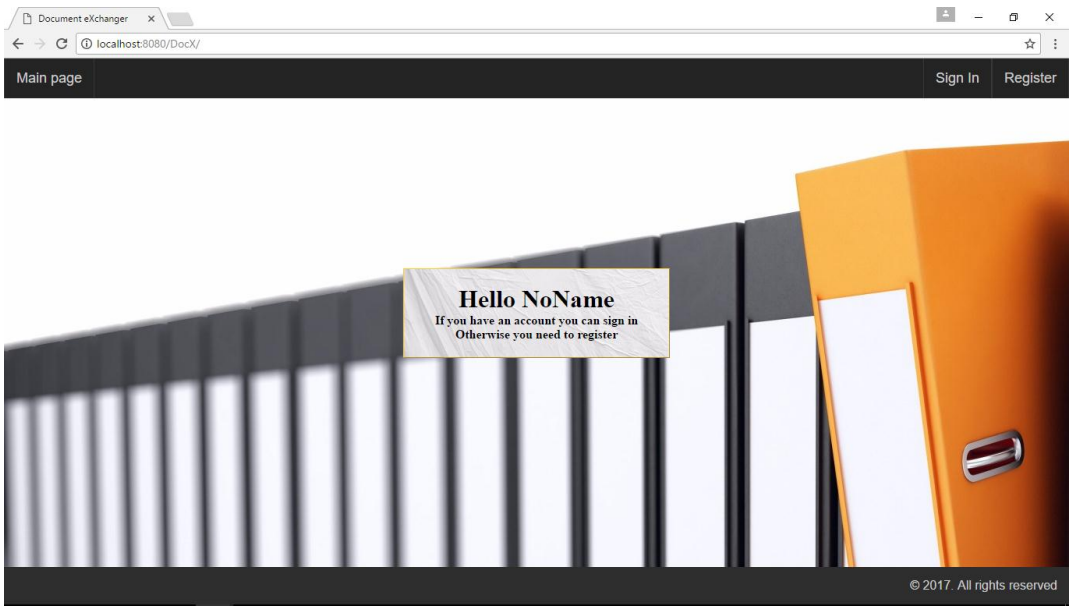

Рисунок 4.1 – Головна сторінка

Далі ми ми можемо обрати вхід або реєстрацію. Натиснувши кнопку реестрації ми потрапляємо до вікна з реестрацією, (рис. 4.2), на якому ми вводимо свій логін й пароль.

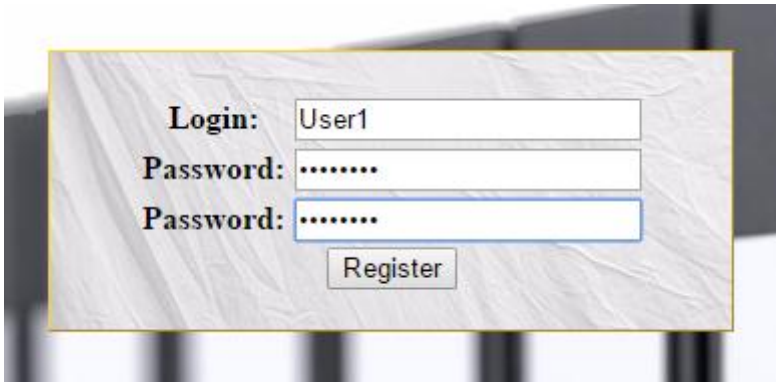

Рисунок 4.2 – Форма реєстрації

Натиснувши кнопку реєстрації, система створює новий обліковий запис, за яким далі користувач зможе працювати, та відправляє йому його приватний ключ, за яким він зможе отримувати доступ до файлів, (рис. 4.3).

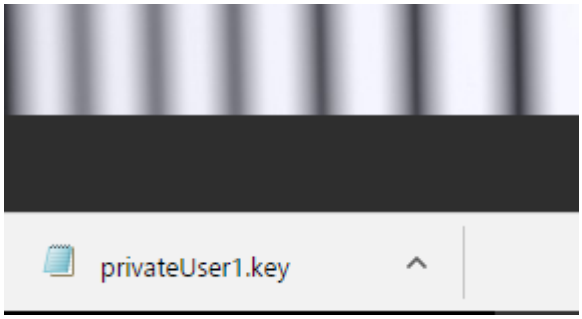

Рисунок 4.3 – Завантажений файл приватного ключа

Далі користувач може повноцінно працювати з файлами в системі. Відправлені для нього файли будуть зберігатися в його власній директорії, зашифровані за допомогою його приватного ключа який зберігся в системі, (рис. 4.4).

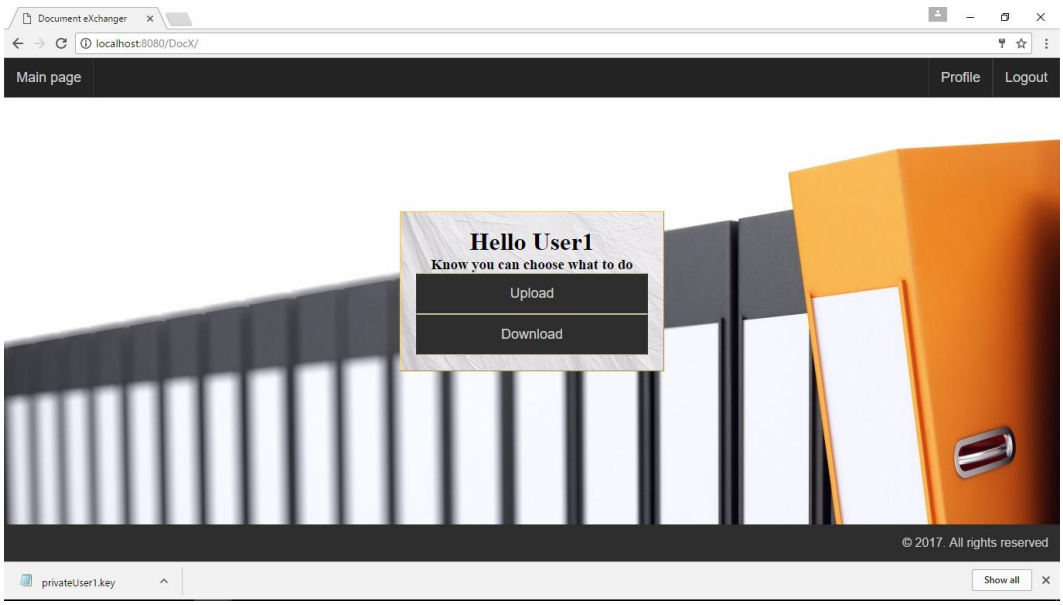

Рисунок 4.4 – Робоча область користувача

Після натискання кнопки завантаження фалу, користувач може обрати кому він буде відправляти файл, та обрати сам файл для відправки, спробуємо відправити файл самому собі, (рис. 4.5). Зміст файлу(рис. 4.6).

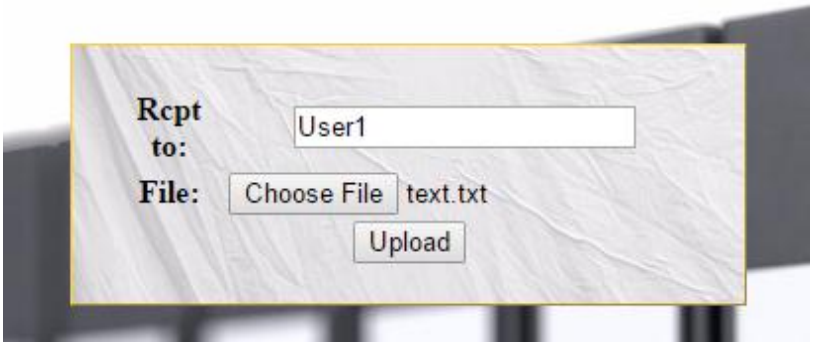

Рисунок 4.5 – Відправка або додання фалу до директорії користувача

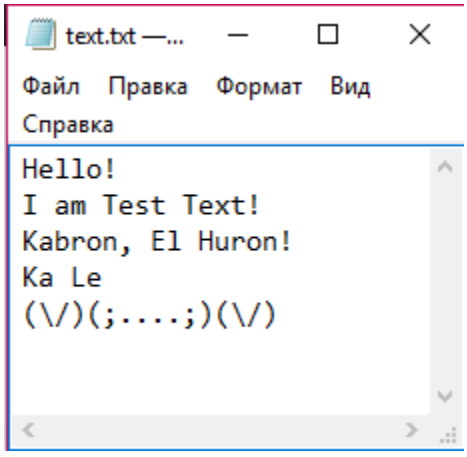

Рисунок 4.6 – Зміст файлу який ми відправляємо

Натиснувши кнопку підтвердження ми відправляємо файл на сервер де він зашифровується відкритим ключем користувача якому ми його відправляли, тобто нашим, так як ми відправили файл самому собі.

Переходячи до вкладки перегляду файлів, ми можемо побачити що нам прийшов файл з іменем відправника, датою та часом отримання (рис. 4.7).

Рисунок 4.7 – Відображення змісту директорії користувача

На сервері цей файл знаходиться в зашифрованому вигляді (рис. 4.8).

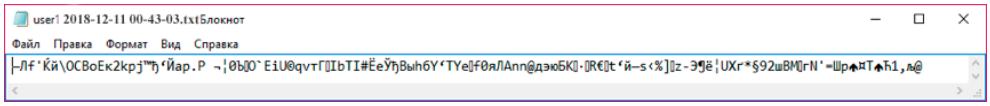

Рисунок 4.8 – Вигляд зашифрованого фалу

Якщо користувач хоче завантажити його собі, він натискає клавішу завантаження та вводить ім’я файлу та підтверджує право власності на цей документ своїм ключем, який він отримав при реєстрації (рис. 4.9).

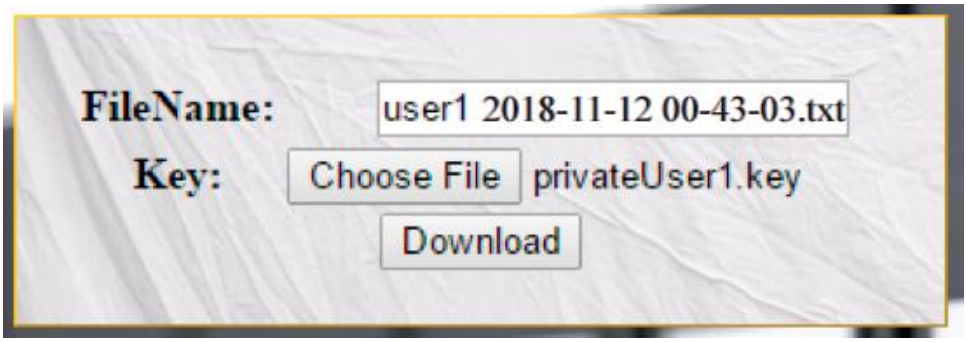

Рисунок 4.9 – Завантаження зашифрованого файлу

Натиснувши клавішу завантаження, сервер обробляє запит та розшифровує файл користувача, повертаючи йому оригінал документу (рис. 4.10).

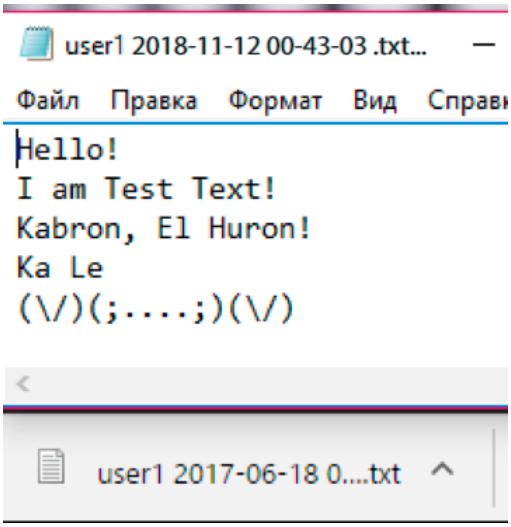

Рисунок 4.10 – Вихідний файл

Таким чином була проведена часткова демонстрація та тестування роботи системи. Також в системі наявна можливість формування завдань, логування, та адміністрування користувачів. Файли шифруються да дешифруються достатньо швидко, не більше хвилини, якщо файли об’ємом не більше 10 мб, при високій навантаженості системи, більше 100 користувачів.

Основне навантаження при роботі на процесорі, максимальна кількість користувачів системи залежить лише від апаратних ресурсів.

Загалом, можна сказати що система проста, злагоджено працює, не потребуючи занадто великих ресурсів, та швидка в використанні, захищена двохрівневим ступенем аутентифікації, що є достатнім для локальної системи безпечного електроного документообігу.

Висновки до розділу

Проведене тестування показало найважливіший елемент функціонування будь-якої системи електронного документообігу. Було зареєстровано нового користувача, створено та відправлено документ самому собі, файл був зашифрований його публічним ключем, й надалі, був завантажений за допомогою виданого при реєстрації приватного ключа. Таким чином, було продемонстровано безпечний обіг документами в системі.

РОЗДІЛ 5. МАРКЕТИНГОВИЙ АНАЛІЗ СТАРТАП-ПРОЕКТУ

5.1 Опис ідеї проекту

Таблиця 5.1. Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користучача
Створення модулю безпеки на основі алгоритму RSA в системі електронного документообігу який буде контролювати доступ до файлів користувачам та захищати данні від зловмисників. Зашифровка й розшифровка будуть займати значний час але рівень захищеності даних буде дуже високий.	Будь-які системи електронного документообігу. Будь-яких розмірів. Та всі програмні застосунки які в суті своєї роботи взаємодіють з файлами користувачів.	Користувач отримує програмний застосунок який зберігає його особисті данні та запобігає їх утраті, на розшифрування даних піде дуже велика кількість часу, тож можна сказати що він отримує максимальний рівень захищеності. Отримує функціонал безпечного обміну файлами між іншими користувачами системи.
	Використання модулю для обміну документами та збереження даних в особистих цілях.	

Таблиця 5.2. Опис ідеї стартап-проекту

№	Техніко-економічні характери-тики ідеї	Продукція конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	LanDocs	Діло	PZDC			
1	Рівень захищеності системи та файлів	95%	70%	50%	28%	-	-	+
2	Додатковий функціонал	1/5	4/5	5/5	1/5	+	-	-

Закінчення таблиці 5.2

3	Максимальна кількість користувачів	Не обмежена	2000	3000	100	-	-	+
4	Швидкість обробки документів	Низька	Середня	Высока	Низька	-	+	-
5	Простота налаштування та користування	Легкий інтерфейс	Наванта жений інтерфей с	Середній	Легкий	-	-	+
6	Ресурсоємність розміщення системи	Низька	Середня	Середня	Низька	-	-	+
7	Ціна за місяць використання системи	100$	205$	70$	120$	-	+	-

5.2 Технологічний аудит ідеї проекту

Таблиця 5.3. Технологічна здійсненність ідеї проекту

№	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Забезпечення найвищого рівня захищеності	Розробка криптографічного програмного модулю на Java з не стандартним выкористанням алгоритму шифрування RSA	Мова Java та доступні сторонні бібліотеки для розробки криптографічного модулю існують й описаний в роботі метод роботи з алгоритмом RSA, можливий.	Всі технології знаходяться в доступному та відкритому вигляді.
2	Забезпечення захищенного обміну файлами між користувачами	Розробка програмного модулю обміну на Java який буде пряцювати одночасно з модулем шифрування. Використовуючи стандартні бібліотеки по роботі з файлами	Для роботи з сервером існують бібліотеки для ApaceTomcat та сам сервер й база данних Oracle Database.	Всі технології знаходятся в відкритому доступі та безкоштовні.

		та сервером Apach Tomcat.		
3	Швидка робота системи	Реалізується за допомогою розміщення більшої частини модулів на персональному пристрої користувача	У кожного користувача має бути пристрій для роботи системи	В наш час майже кожна людина має персональний компьютер
4	Ізоляція всіх данних	Так як усі процеси обробки проходять на пристрої користувача, залишаємо передачу файлів в зашифрованому вігляді на сервер та в зворотньому порядку, таким чином усі данні ізольовані. Данні зберігаемо на сервері.	Існує велика кількість різних типів серверів та баз данних для зберігання та передачі файлів, майже усі підходять для реалцзації системи.	Існує велика кількість як платних так і безплатних аналогів. Усі вони знаходятся у відкритому доступі.
Обрана технологія реалізації ідеї проекту:1				

Висновок: технологічна реалізація продукту – можлива, вибрана технологія №1

5.3 Аналіз ринкових можливостей запуску стартап-проетку

Таблиця 5.4. Попередня характеристика потенційного ринку

№	Показники стану ринку	Характеристика
1	Кількість головних гравців, од	3
2	Загальний обсяг продаж, грн./ум.од	10235/23
3	Динаміка ринку	Позитивна
4	Наявність обмежень для входу	Відсутні
5	Специфічні вимоги до стандартизації та сертифікації	Авторське право
6	Середня норма рентабельності в галузі або по ринку, %	9%

Висновок: враховуючи кількість головних гравців по ринку, зростаючу динаміку ринку, невелику кількість конкурентів та середню норму рентабельності можна зробити висновок, що на даний момент, ринок для входження стартап-продукту є привабливим.

Таблиця 4.5. Характеристика потенційних клієнтів стартап-проекту

№	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці цільових груп клієнтів	Вимоги споживачів до товару
1	Недостатній рівень захищеності документів в мережі	Компанії, підприємства, навчальні заклади, установи та персональні користувачі яких цікавить безпека персональних даних	Деяких людей може не цікавити їх персональна безпека в міру їх не освідомленості та не знання негативних наслідків які можуть бути результатом їх нехтуванням питання безпеки	Отримати швидку, просту та найбезпечнішу систему для обміну документами, в якій вони можуть не переживати за захищеність своїх даних.
2	Повільна робота систем які мають хоча б мінімальний рівень захисту	Компанії, підприємства, навчальні заклади, установи та персональні користувачі	Якщо компанія або підприємство виконує велику кількість замовлень воно дуже непокоїться за власну швидкість роботи, якщо проігнорувати цю потребу можна втратити велику кількість потенційних кліеєнтів.	

3	Перенавантаженість існуючих систем	Компанії, підприємства, навчальні заклади, установи та персональні користувачі	Якщо це персональні користувачі то при знайомстві з перенавантаженою системою вони можуть не обрати її за основну й таким чином втрачається велика кількість звичайних людей яким міг би бути цікавий даний продукт.	

Таблиця 5.6. Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Конкуренти	Наявність конкурентів котрі надають схожі рішення	Зменшення ціни на поставлену послугу; Розробка унікальних характеристик товару; Надання ліцензій на обслуговування
2	Кошти на розробку та підтримку продукту	Закінчення грошей та недостатнє фінансування	Залучення додаткових інвесторів, мотивація роботи на перспективу; Ітеративна розробка продукту задля покрокового виведення продукту на ринок та отримання відповіді користувачів

Закінчення таблиці 5.6

3	Вихід аналогу	Вихід аналогу даного товару може призвести до знецінення та безідейності даного товару	Вихід товару на ринок в коротші строки з не повною, але достатньою, функціональністю для зацікавлення усіх цільових аудиторій; Проведення рекламної компанії

Таблиця 5.7. Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
1	Новий продукт	Вихід на ринок, Зменшення монополії, Надання нових рішень у сфері	Розробка нової функціональності; Вихід нової продукції на ринок; Надання різноманітних типів ліцензій в залежності від потреб користувача \ замовника.
2	Вихід аналогу	Надати продукт з певними характеристиками та можливостями що відсутні у компаній конкурентів	Аналіз ринку та користувачів задля задоволення їх потреб та надання функціональності у найкоротші строки за ціну, котра є дешевшою ніж у продуктів-замінників.
3	Зворотній зв’язок від користувачів	Можливість отримання необхідної інформації для вдосконалення продукту	Наявність вхідних даних та реакція на них з боку команди розробників задля задоволення потреб та бажань кінцевих користувачів системи кешування даних.
4	Грошова винагорода за рекламу	При достатньому попиту на систему кешування даних можлива	Точкова комерціалізація продукту; Введення реклами;

		комерціалізація продукту на основі реклами	Ведення додаткових коштів у проект задля його подальшого розвитку.

Таблиця 5.9. Ступеневий аналіз конкуренції на ринку

№	Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1	Тип конкуренції: монополістична	Товар від кожної компанії на ринку, являється недосконалим замінником товару, реалізованого іншими фірмами; На ринку є умови для входу та виходу; Ціна корелює між суперниками;	Розробка продукту з характеристиками, які покривають сфери вживання що не покривають інші товари-замінники; Кореляція цін у відповідності до товарів замінників; Різни типи ліцензій.
2	Рівень конкурентної боротьби: світовий	Всі продукти замінники розроблялись інтернаціональними командами з різних куточків світу, продукти не належать до певної держави, а належать команді розробників	Вихід на ринок збуту продукту з клієнто-необхідною функціональністю; Налагодження маркетингу на основних Інтернет ресурсах задля охоплення великої кількості потенційних користувачів; Надання бета-версій продукту.
3	Галузева ознака: внутрішньогалузева	Даний тип продукту може використовуватися	Надання зручного, інтуїтивно зрозумілого інтерфейсу;

		тільки у сфері розробки IT додатків \ продуктів	Підтримка всім відомих методів взаємодії з середовищем розробки; Наявність документації та он-лайн підтримки.
4	Конкуренція за видами товарів: товарно-видова	Дана конкуренція – конкуренція між товарами одного виду.	Впровадження функціональності яка відсутня у товарів-замінників; Спрощення інтерфейсів; Надання підтримки.
5	Характер конкурентних переваг: цінова та не цінова	Цінові переваги – точкова комерціалізація; Не цінова – надання функціональності, що відсутня у товарах-замінниках.	Надання платних ліцензій лише на критично важливу функціональність для клієнта з певним строком підтримки, що зазначена у відповідній ліцензії; Впровадження унікальної функціональності.
6	За інтенсивністю: марочна	Наявність унікального знаку що відрізняє даний продукт від продуктів-замінників	Впровадження власної назви та власного знаку.

Таблиця 5.10. Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Клієнти	Товари-замінники
	LanDocs	Діло,PZDC	Компанії, підприємства, установи та персональні користувачі яких цікавить безпека	GoogleDrive ICloudDrive YandexDisk OneDrive Усі хмарні застосунки для збереження файлів користувачів.

			персональних даних	
Висновки	Даний конкурент може надати досить високий рівень безпеки для роботи з даними але має перенавантажений інтерфейс та дуже велику кількість обхідних шляхів через які можна втратити персональні данні	Необхідно враховувати їх існування та як у світлі останніх подій, клієнти приділяють велику увагу безпеці, тож доцільним було б підвищити свій рівень безпеки, данні конкуренти можуть створити конкурентноспроможний аналог.	Аудиторія у даної системи дуже велика, тож проблем з виходом на ринок не може бути.	Дуже великі компанії які беруть захист під своє чесне слово та мають велетеньські бюджети, але все більша кількість людей втрачає довіру до таких систем й шукає доступні аналоги.

Проаналізувавши можливості роботи на ринку з огляду на конкурентну ситуацію можна зробити висновок: оскільки кожний з існуючих продуктів не впливає у великій мірі на поточну ситуацію на ринку в цілому, кожний з існуючих продуктів має свою специфічну сферу використання та свої позитивні та негативні сторони щодо рішення певних типів задач, то робота та вихід на даний ринок є можливою і реалізованою задачею.

Для виходу на ринок продукт повинен мати функціонал що відсутній у продуктів-аналогів, повинен задовольняти потреби користувачів, мати необхідний та достатній функціонал з конфігурування, підтримку зі сторони розробників та можливість розробки спеціального функціоналу за відповідною ліцензією.

Таблиця 5.11. Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування
1	Частка ринку	Система захопить велику частину ринку так як усі аналоги які присутні на даний момент не дають комплексного комфорту для користувача й не надають достатній рівень безпеки.
2	Ціна	Місячна підписка для доступу до роботи в системі є найбільш цільовою для аудиторії яка буде користуватися системою й є доступною для більшості користувачів, така сума не буде тягарем для будь-кого хто дійсно непокоїться власною безпекою.
3	Асортимент	Асортимент функціоналу системи не дуже великий, але він не є необхідним, весь функціонал надає система и вона гармонійно працює з сторонніми застосунками.
4	Репутація виробника	Так як у системі використовується найбезпечніший алгоритм який відомий майже усім, й мовою на якій написано застосунок написані найбезпечніші програмні застосунки, можна сказати що репутація й даної системи буде на рівні.

Таблиця 5.12. Порівняльний аналіз сильних та слабких сторін системи кешування мало змінних даних

№	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з запропонованим						
			-3	-2	-1	0	+1	+2	+3

1	Частка ринку	13	-	+	-	0	-	-	-
2	Ціна	16	-	-	-	0	-	-	-
3	Асортимент	6	-	-	-	0	-	+	-
4	Репутація виробника	19	-	-	+	0	-	-	-

Таблиця 5.13. SWOT аналіз стартап-проекту

Сильні сторони (S): – Відсутність функціональних аналогів, високий рівень реалізації рівня безпеки, відкритість роботи системи й доступність для будь-якої аудиторії, низький рівень технічних потреб та доступність інтерфейсу, простота використання, високий рівень довіри до технічних засобів на яких побудована система, гнучкість та універсальність модулю безпеки, можливість інтеграції в існуючі системи.	Слабкі сторони (W): – Не велика кількість влаштованого в систему функціоналу, наявність великих компаній які надають комфорт роботи з файлами з зафіксованим ім'ям та високим рівнем довіри, Швидкість роботи не достатня для автоматизованої роботи при інтеграції в великі системи.
Можливості (O): – Захист обміну та роботи з файлами, високий рівень захищеності передачі та збереження даних. Утримання стабільної позиції на ринку з охопленням великої частки аудиторії, та велика кількість однодумців.	Загрози (T): – Існують аналоги які також бачать ситуацію на ринку й можуть вкласти великі бюджети в створення аналогічних систем з схожими модулями безпеки які можуть стати більш конкурентноспроможними на даний момент.

Таблиця 5.14. Альтернативи ринкового впровадження стартап-проекту

1	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Безкоштовне надання певного функціоналу у користування	Головний ресурс – люди, даний ресурс - наявний	2-3 місяці

	споживачам на обмежений термін		
2	Реклама	Залучення власних коштів для реклами товару	1-2 місяці
3	Написання статей та опис товару на відомих ресурсах	Головний ресурс – час, даний ресурс - наявний	2-3 тижні
4	Презентація товару на хакатонах й інших ІТ заходах	Ресурс – час та гроші для участі, наявні	1-3 місяці

5.4 Розроблення ринкової стратегії проекту

Таблиця 5.15. Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Компанії, підприємства, установи та особи яких цікавить безпека їх даних.Це можуть бути люди які зацікавленні в веденні як власного обігу документів так і корпортаивного. Основною метою цільової аудиторії є збереження конфіденційності персональних даних	Споживачі на даний момент користуютьс я великою кількістю застосунків й комбінують їх, що є не дуже комфортним, й вони чекають на нього.	Можна сказати що більша частка сегменту цільової групи перейде на дану систему так як в основному це люди які достатньо ознайомлені з методами захисту	На даний момент інтенсивних дій в сегменті захисту персональної інформації окремих користувачів не відбувається, даний рух є в інших сферах	При в ході в сегмент не буде ніяких складнощів або перешкод, люди готові сприйняти продукт та чекають на нього.

Закінчення таблиці 5.15

Які цільові групи обрано: групу 1 (весь ринок)

Відповідно до проведеного аналізу можна зробити висновок, що підходящою цільовою групою для розповсюдження даного програмного продукту є компанії, підприємства, установи та особи яких цікавить безпека персональних даних, та гарантована надійність захисту системи при роботі з електронним документообігом. Відповідно до стратегії охоплення ринку збуту товару обрано стратегію масового маркетингу, оскільки для підприємств, окремих осіб, компаній у цілому надається стандартизований продукт з можливістю розширення функціональності (відповідно до ліцензії).

Таблиця 5.16. Визначення базової стратегії розвитку

Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
Надання функціональності що відсутня у товарів-замінників, підтримка клієнтів	Проведення реклами, освітлення унікальної функціональності через інтернет ресурси та інші канали, контакт напряму з споживачами; формування лояльності	Зниження ступеню замінності товару; Прихильність клієнтів; Відмітні властивості товару; Відмітні характеристики товару;	Стратегія диференціації

Таблиця 5.17. Визначення базової стратегії конкурентної поведінки

Чи є проект «першопрохідцем» на ринку	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, які?	Стратегія конкурентної поведінки
Ні, оскільки є товари-замінники, але дані товари замінники не мають деякого необхідного функціоналу	Так, ціль компанії знайти нових споживачів та, частково, забрати існуючих у конкурентів задля задоволення потреб останніх	Компанія частково копіює характеристики товару конкурента, основна ціль компанії розробка нового унікального функціоналу, з підтримкою основного функціоналу конкурентів	Стратегія заняття конкурентної ніші

Таблиця 5.18. Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту
1	Комфортна робота з файлами та їх швидкий й простий обмін	Сформувати простий і доступний інтерфейс та інструкції що до користування системою	Простота та не нагромадженість інтерфейсу, достатній рівень функціоналу для реалізації будь-яких потреб, гнучкість	Простота та гнучкість до інтеграцій.

			застосування та інтеграції	
2	Захищеність персональних даних та файлів	Описати простоту й складність алгоритмів захисту даних в системі.	Нестандартний підхід до використання методів шифрування який забезпечую дуже високий рівень безпеки роботи з файлами та захист персональних даних.	Надійність захисту й унеможливлювання доступу без вашого дозволу.
3	Швидкість роботі	Реалізувати швидкий обмін документами між клієнтом і сервером	Так як усі процеси по обробці відбуваються на вашому персональному компьютері швидкість обробки файлів залежить від ваших особистих ресурсів	Комфорт та безпека у руках користувача, повний контроль та швидкість роботи.

Відповідно до проведеного аналізу можна зробити висновок, що стартап-компанія вибирає як базову стратегію розвитку – стратегію диференціації, як базову стратегію конкурентної поведінки – стратегію заняття конкурентної ніші.

5.5 Розроблення маркетингової програми стартап-проекту

Таблиця 5.19. Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами
1	Захисту персональних даних, та обміну документами	Найвищий рівень безпеки при роботі з файлами.	Висока захищеність обміну файлами на всіх етапах роботи з файлом, від зберігання до редагування.

Таблиця 5.20. Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>1. Товар за задумом</td><td colspan="3">Система контролю доступу до файлів на мові програмування Java</td></tr>
<tr><td rowspan="9">2. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх/Тл/Е/Ор</td></tr>
<tr><td>Захищеність файлів</td><td>М</td><td>Тл</td></tr>
<tr><td>Швидкість роботи</td><td>М</td><td>Тх</td></tr>
<tr><td>Гнучкість до інтеграцій</td><td>Нм</td><td>Тл</td></tr>
<tr><td>Надійність виконаня</td><td>Нм</td><td>Тл</td></tr>
<tr><td>Зрозумілий інтерфейс</td><td>Нм</td><td>Е</td></tr>
<tr><td>Захищеність персональних даних</td><td>М</td><td>Тл</td></tr>
<tr><td colspan="3">Пакування: дані упаковані в файл формату RAR</td></tr>
<tr><td rowspan="2">3. Товар із підкріпленням</td><td colspan="3">До продажу: наявна повна документація, акції на придбання декількох ліцензій, знижки для певних сегментів на покупку товару</td></tr>
<tr><td colspan="3">Після продажу: додаткова підтримка спеціалістів налаштування, підтримка з боку розробника</td></tr>
<tr><td colspan="4">За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності, патент</td></tr>
</table>

Таблиця 5.21. Визначення меж встановлення ціни

Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
2800 грн	23666 грн	8000 грн/міс	13000грн/2000грн

Таблиця 5.22. Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Замовлення ліцензії через інтернет або придбання фізичного видання зважаючи на специфіку функціоналу застосунку.	Видання ключів доступу до системи користувачам які придбали систему, які йдуть у комплекті з кожною електронною або фізичною копією продукту.	Продаж копій компаніям які займаються організацією та налаштуванням документообігу на підприємствах, інтернет ресурсам по продажу програмного забезпечення та власна реалізація на сайті. Подарункові версії для медійних людей з даної сфери та конкретним великим компаніям.	Власноручна реалізація товару через інтернет сторінку застосунку на якій можна описати та презентувати застосунок, абі максимально донести до покупців сутність та переваги системи.

Таблиця 5.23. Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Скептицизм	Електронна пошта, соціальні	Налаштувати позиції на здивування	Показати на скільки безпека в мережі	Відображення важливості

		мережі, інтернет	клієнта, показати унеможливлювання зламу системи,	важливий елемент й як нехтування нею може призвести до негативних наслідків.	безпеки й захисту персональних даних та показаи на скільки це легко й доступно.
2	Довіра		Показати на скільки безпечнішим та комфортнішим можна зробити обіг документів.	Показати на скільки безпечнішим може бути обмін даними в наш час.	

Як результат було створено ринкову (маркетингову) програму, що включає в себе визначення ключових переваг концепції потенційного товару, опис моделі товару, визначення меж встановлення ціни, формування системи збуту та концепцію маркетингових комунікацій.

Висновки по розділу

В п’ятому розділі описано стратегії та підходи з розроблення стартап-проекту, визначено наявність попиту, динаміку та рентабельність роботи ринку, як висновок було вказано що існує можливість ринкової комерціалізації проекту. Розглянувши потенційні групи клієнтів, бар’єри входження, стан конкуренції та конкурентоспроможність проекту було встановлено що проект є перспективним. Розглянуто та вибрано альтернативу впровадження стартап-проекту та доведено доцільність подальшої імплементації проекту.

ВИСНОВКИ

В ході виконання магістрської роботи було проведено дослідження предметної галузі електронного документообігу, виділено головні ролі системи та бізнес-процеси.

Проаналізовано вимоги до системи в цілому, вимоги до функцій системи, програмного і технічного забезпечення. Було проведено дослідження технологій для побудови систем призначених для роботи з електронними документами. В результаті дослідження був обраний наступний стек засобів: Apache Tomcat, мова програмування Java, JSP, бібліотеки Crypto та Security, та Apache Comons. Ретельний огляд найпоширеніших СУБД дозволив обрати найбыльш підходящу - Oracle Database.

Використання принципу тришарової архітектури додатку, тобто поділу на рівень представлення, рівень бізнес-логіки та рівень данних дало можливість розробити гнучку та ефективну систему, адже на кожному шарі відбувається вирішення окремих локальних задач, що позитивно відображається на надійності системи.

Обравши мову програмування Java для розробки ми сильно підвищили безпеку роботи системи та зробили її кросплатформенною, також використання бібліотек дозволило нам спростити розробку модулю шифрування для роботи з файлами.

Результатом роботи над магістрською роботою стало створення системи безпечного електронного документообігу, що стала би важливою та дуже корисною для будь-якої організації яка хоче автоматизувати та забезпечити повну безпеку роботи з документами. Система є сучасною та зручною, задовольняє всі вимоги з точки зору функціональності, юзабіліті, дизайну та безпеки даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Apache Tomcat [Електронний ресурс] – Режим доступу до ресурсу: ru.bmstu.wiki/Apache_Tomcat.
2. Сучасні системи електронного документообігу [Електронний ресурс] – Режим доступу до ресурсу: http://mego.info/22.
3. Навчальний посібник За загальною редакцією професора В.Г. Іванова Харків [Електронний ресурс] – Режим доступу до ресурсу: http://www.ua.z-pdf.ru/7tehnicheskie/881360-3-pravova-informaciya-kompyuterni-tehnologii-yuridichniy-diyalnosti-navchalniy-posibnik-zagalnoyu-redakci-yu-profesora-ivanov.php.
4. Особливості захисту електронного документообігу [Електронний ресурс] – Режим доступу до ресурсу: http://easy-code.com.ua/2011/07/osoblivosti-zaxistu-elektronnogo-dokumentoobigu/.
5. Безпека електронного документообігу [Електронний ресурс] – Режим доступу до ресурсу: http://wiki.tneu.edu.ua/.
6. Java як мова програмування [Електронний ресурс] – Режим доступу до ресурсу: http://ukrbukva.net/page,3,65256-Java-yazyk-programmirovaniya.html.
7. Що таке Java [Електронний ресурс] – Режим доступу до ресурсу: http://vidpo.net/shho-take-java.html.
8. Документація по Oracle Database Express Edition [Електронний ресурс] – Режим доступу до ресурсу: http://www.oracle.com/technetwork/ru/database/express-edition/documentation/index.html.
9. Oracle Database [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Oracle_Database.
10. Apache Tomcat [Електронний ресурс] – Режим доступу до ресурсу: http://ru.bmstu.wiki/Apache_Tomcat.Бібліотека Crypto [Електронний

ресурс] – Режим доступу до ресурсу: https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html.

11. Огляд безпеки в Java [Електронний ресурс] – Режим доступу до ресурсу: http://spec-zone.ru/RU/Java/Docs/7/technotes/guides/security/overview/jsoverview.html.
12. И.В. Мархвид. Создание WEB – страниц: HTML, CSS, JavaScript. — Минск. ООО «Новое знание», 2002. — 352 с.
13. Java сервлети [Електронний ресурс] – Режим доступу до ресурсу: https://www.javatpoint.com/jsp-tutorial.
14. Налаштування бази данних [Електронний ресурс] – Режим доступу до ресурсу: http://studopedia.su/9_53377_nalashtuvannya-bazi-danih.html.
15. Стаття по шифруванню данних MD5 [Електронний ресурс] – Режим доступу до ресурсу: http://replace.org.ua/topic/6250/.

ДОДАТКИ

ДОДАТОК А

Діаграма використання

ДОДАТОК Б

UML діаграма класів

ДОДАТОК В

Діаграма послідовності

ДОДАТОК Г

Діаграма розгортання

ДОДАТОК Д

Інтерфейси аналогів

ДОДАТОК Е

Інтерфейс розробленої системи