

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

/С.Н. НОВИКОВ /

Разработка системы дистанционного электронного голосования

Новосибирск 2022

Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

КАФЕДРА

Безопасность и управление в телекоммуникациях

ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ СПЕЦИАЛИСТА

СТУДЕНТА А.А. Крылосова ГРУППЫ АБ-66

«УТВЕРЖДАЮ»

« 24 » мая 2021 г.

Зав. кафедрой БиУТ

/ С.Н. НОВИКОВ /

Новосибирск 2021

1. Тема выпускной квалификационной работы специалиста:

Разработка системы дистанционного электронного голосования

утверждена приказом по университету от « 24 » мая 2021 г. № 4/823о-21

2. Срок сдачи студентом законченной работы « 19 » января 2022 г.

3. Исходные данные по проекту (эксплуатационно-технические данные, техническое задание):

Язык программирования Python 3 и его документация

Python библиотеки: Flask, Tkinter

Облачная PaaS-платформа Heroku

База данных PostgreSQL

Методика определения угроз безопасности информации в информационных системах ФСТЭК России

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)	Сроки выполнения по разделам
Введение	13.09.2021 г.
1. Анализ предметной области	11.10.2021 г.
2. Разработка технического задания	08.11.2021 г.
3. Разработка системы дистанционного электронного голосования	06.12.2021 г.
4. Безопасность жизнедеятельности	13.12.2021 г.
5. Технико-экономическое обоснование работы	20.12.2021 г.
6. Заключение	27.12.2021 г.
7. Список литературы	09.01.2022 г.
8. Приложения	15.01.2022 г.

Консультанты по ВКР (с указанием относящихся к ним разделов):

1. Раздел по технико-экономическому обоснованию

2. Раздел по безопасности жизнедеятельности

Дата выдачи задания

«01» сентября 2021 г.

_____/ Г.В. Попков /
(подпись, Ф.И.О. руководителя)

Задание принял к исполнению

«01» сентября 2021 г.

_____/ А.А. Крылов /
(подпись, Ф.И.О. студента)

Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

ОТЗЫВ

О работе студента А.А. Крылосова в период подготовки выпускной квалификационной работы по теме «Разработка системы дистанционного электронного голосования»

Работа имеет практическую ценность
Работа внедрена
Рекомендую работу к внедрению
Рекомендую работу к опубликованию
Работа выполнена с применением ЭВМ

Тема предложена предприятием
Тема предложена студентом
Тема является фундаментальной
Рекомендую студента в магистратуру
Рекомендую студента в аспирантуру

Руководитель выпускной квалификационной работы специалиста

Доц. каф. БиУТ, к.т.н.

Глеб Владимирович Попков

«15» января 2022 г.

С Отзывом ознакомлен

/А.А. Крылосов/

«15» января 2022 г.

Уровень сформированности компетенций у студента

А.А. Крылосова

Компетенции		Уровень сформированности компетенций		
		высокий	средний	низкий
1		2	3	4
Профессиональные	ПК-1 - способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем			
	ПК-5 - способностью проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов			
	ПК-7 - способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования			
	ПК-12 - способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности			

АННОТАЦИЯ

Выпускной квалификационной работа студента А.А. Крылосова
по теме Разработка системы дистанционного электронного голосования

Объём работы – 73 страниц, на которых размещены 5 рисунков и 12 таблиц. При написании работы использовалось 9 источников.

Ключевые слова: электронное голосование, система защиты информации, персональные данные, аутентификация, базы данных, протоколы голосования.

Работа выполнена на: кафедре БиУТ СибГУТИ

Руководитель: доц. каф. БиУТ Попков Г.В.

Целью работы разработка системы дистанционного электронного голосования

Решаемые задачи: анализ предметной области, разработка технического задания, разработка системы дистанционного электронного голосования, безопасность жизнедеятельности, технико-экономическое обоснование работы.

Основные результаты: система дистанционного электронного голосования

Graduation thesis abstract

of A.A. Krylosov on the theme Development of a remote electronic voting system

The paper consists of 73 pages, with 5 figures and 12 tables/charts/diagrams. While writing the thesis 9 reference sources were used.

Keywords: electronic voting, information security system, personal data, authentication, databases, voting protocols.

The thesis was written at BIUT department SibSUTIS
(name of organization or department)

Scientific supervisor associate professor of the BiUT Popkov G.V.

The goal/subject of the paper is Development of a remote electronic voting system

Tasks: analysis of the subject area, development of technical specifications, development of a remote electronic voting system, life safety, feasibility study of work

Results remote electronic voting system

ОГЛАВЛЕНИЕ

Введение	4
1 Анализ предметной области	5
1.1 Постановка задачи	5
1.2 Определение объекта разработки.....	5
1.3 Анализ существующих систем голосования.....	6
1.4 Модель угроз и нарушителей безопасности информации.....	10
1.5 Выводы по разделу	20
2 Разработка технического задания	22
2.1 Постановка задачи	22
2.2 Сравнительный анализ протоколов электронного голосования.....	22
2.3 Разработка концепции модулей системы голосования.....	26
2.4 Выводы по разделу	30
3 Разработка системы дистанционного электронного голосования	31
3.1 Постановка задачи	31
3.2 Разработка сервиса авторизации	31
3.3 Разработка сервиса учета голосов.....	32
3.4 Разработка модуля аудита.....	34
3.5 Разработка модуля клиента.....	35
3.6 Выводы по разделу	38
4 Безопасность жизнедеятельности	40
4.1 Постановка задачи	40
4.2 Воздействие электронных систем на здоровье пользователей	40
4.3 Эргономические требования к системам отображения информации..	43
4.4 Режимы труда и отдыха при работе с электронными устройствами...	46
4.5 Экологические проблемы утилизации электронных гаджетов.....	47

Подп. и дата	3.2 Разработка сервиса авторизации	31
	3.3 Разработка сервиса учета голосов.....	32
	3.4 Разработка модуля аудита.....	34
	3.5 Разработка модуля клиента.....	35
	3.6 Выводы по разделу	38
	4 Безопасность жизнедеятельности	40
Инв. № дубл.	4.1 Постановка задачи	40
	4.2 Воздействие электронных систем на здоровье пользователей	40
	4.3 Эргономические требования к системам отображения информации..	43
	4.4 Режимы труда и отдыха при работе с электронными устройствами...	46
	4.5 Экологические проблемы утилизации электронных гаджетов.....	47

Подп. и дата						ИИВТ.10.05.02.066 ПЗ				
Из	Лист	№ докум.	Подп.	Дата		Разработка системы дистанционного электронного голосования Содержание	Лит	Лист	Листов	
Разраб.	А.А. Крылов								2	73
Пров.	Г.В. Попков									
Н/контр										
Рецензент										
Утвердил	С.В. Новиков									

4.6 Вывод	49
5 Технико-экономическое обоснование работы	49
5.1 Постановка задачи	49
5.2 Расчет трудоемкости и длительности работ	49
5.3 Расчет себестоимости программного продукта.....	53
5.4 Расчет цены программного продукта	57
5.5 Определение эффекта от разработки программного продукта	58
5.6 Оценка конкурентоспособности программного продукта	60
5.7 Выводы по разделу	62
Заключение	64
Список литературы	65
Приложение А client.py	67
Приложение Б protocol_client.py	70
Приложение В db.py	72
Приложение Г mask.py	73

Имя № подл	Подпись и дата	Взам или №	Имя № дубл	Подпись и дата	ИИВТ.10.05.02.066					Лист
										3
Изм.	Лист	№ докум.	Подпись	Дата						

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

Результатом исследований и экспериментов стали выводы о неоспоримых преимуществах электронного голосования:

- Однако, при этом возникает ряд специфических проблем, препятствующих честности выборов. Например, сомнения в истинности результатов, полученных с помощью машин. Также дистанционно намного сложнее авторизовать избирателя или удостовериться, что на ход голосования никто не повлиял.

Целью данной выпускной квалификационной работы является разработка системы дистанционного электронного голосования, которая бы отвечала необходимым требованиям и позволяла проводить прозрачные и честные выборы.

					<i>ИИВТ.10.05.02.066 ПЗ</i>						
Из	Лист	№ докум.	Подп.	Дата	Разработка системы дистанционного электронного голосования Содержание	Лит			Лист	Листов	
Разраб.	А.А. Крылосов								2	73	
Пров.	Г.В. Попков										
Н/контр											
Рецензент											
Утвердил	С.В. Новиков										

1.1 Постановка задачи

1.2 Определение объекта разработки

Электронное голосование часто рассматривается как инструмент повышения эффективности избирательного процесса и повышения доверия к нему. Правильно реализованные решения для электронного голосования могут повысить безопасность бюллетеня, ускорить обработку результатов и упростить само голосование.

Как и с бумажным голосованием система для дистанционного электронного голосования должна обеспечить:

- голосование только легитимных участников и при том, только один раз;
- тайну голосования, никто, кроме голосующего, не должен знать его выбор;
- аудит списка избирателей (поимённый перечень проголосовавших);
- аудит результатов голосования (возможность пересчёта бюллетеней);
- сокрытие результатов до окончания голосования (невозможность определения исхода до окончания голосования);
- решение голосующего не может быть тайно или явно кем-либо изменено (кроме, возможно, им самим). [2]

Также, как электронная система, она должна быть отказоустойчива в случае технических неисправностей (потеря электропитания), непреднамеренных (потеря избирателем ключа) и злоумышленных (намеренная выдача себя за другого избирателя, DoS/DDoS) атак.

1.3 Анализ существующих систем голосования

Системы голосования можно разделить на несколько типов:

- бумажную (традиционную);
- бумажно-электронную;
- электронную с прямой записью;
- электронную использующую публичные сети.

Обратим внимание на недостатки традиционной (бумажной) системы голосования. Главным недостатком является длительность подсчета голосов, заполнение соответствующих протоколов и т.д. При бумажном голосовании большое влияние на результат оказывает человеческий фактор – ошибки, возникающие как вследствие переутомления, недомогания и т.д., так и преднамеренные. К наиболее распространенным видам фальсификации можно отнести:

- подкуп избирателей;
- махинации со списком избирателей;
- вбрасывание в выносные урны фальшивых бюллетеней;
- подделка протокола;
- возможность использования «чистых» бюллетеней, не явившихся на избирательный участок граждан;
- порча бюллетеней.

Бумажно-электронная система подразумевает заполнение бюллетеней вручную и подсчет их в электронном виде. Избиратель делает отметку в бумажном бюллетене и вставляет его в электронную урну, результат считывается с помощью

Инв. № подл.	Подпись и дата				ИИВТ.10.05.02.066	Лист 6
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
Изм.	Лист	№ докум.	Подпись	Дата		

специального сканера, распознается. Результат хранится в памяти компьютера. Обработка одного бюллетеня занимает несколько секунд. По завершению времени голосования распечатываются результаты по участку и протокол, который подписывается членами комиссии. Протоколы сохраняются на электронном носителе. Обработка данных далее осуществляется посредством автоматизированной системы.

Система электронного голосования с прямой записью предусматривает использование избирателем механических или электрооптических компонентов для подачи своего голоса. Информация хранится на одном носителе и может передаваться на более высокие уровни избирательных комиссий. Такие системы применяются, в частности, в США, Нидерландах, Бразилии и Венесуэле. Отличие гибридной системы голосования состоит в том, что информация хранится на отдельном устройстве.

В Финляндии электронное голосование проходит на избирательном участке, дистанционное голосование не допустимо. Идентификация личности производится путем сканирования штрих - кода документа и сравнения с электронным списком избирателей. При этом выдается информация о том, имеет ли право голоса данный субъект. Избирателю выдается карточка с электронным кодом - ключом, с помощью которой можно проголосовать. Для этого необходимо вставить ее в электронную урну и выбрать номер кандидата, подтвердить свой выбор. Данные о кандидате и его номер выводятся на экране. После голосования карточка возвращается комиссии. Голос избирателя передается в Центральную избирательную комиссию. Проблема анонимности решается применением программы, отделяющей данные о пользователе от его голоса. Посмотреть результаты электронного голосования можно на официальном сайте сразу после окончания выборов.

В России был проведен эксперимент по внедрению комплекса электронного голосования (КЭГ). Голосование проводилось с помощью электронного табло. На сенсорный экран выводилась информация о кандидатах. Голос пользователя хранится в компьютерной памяти. Как и КОИБ, данный комплекс локальный, а при его создании использовалось программирование на уровне микроконтроллеров.

Инв. № подл.	Подпись и дата																		
	Инв. № дубл.																		
	Взам. инв. №																		
	Подпись и дата																		
<table border="1"> <tr> <td>Изм.</td> <td>Лис</td> <td>№ докум.</td> <td>Подпись</td> <td>Дата</td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </table>					Изм.	Лис	№ докум.	Подпись	Дата										
Изм.	Лис	№ докум.	Подпись	Дата															
ИИВТ.10.05.02.066																			
Лист																			
7																			

США имеют наиболее длительный опыт использования электронных систем голосования, при этом на сегодняшний день правительство Соединенных Штатов продолжает усовершенствование программного и аппаратного обеспечения, из-за обширной критики, отвергающей подобные нововведения и реформирования избирательной системы. Вопрос демократии и прозрачности подсчета голосов занимает в политике США одно из важнейших мест. В большинстве штатов США впервые электронное голосование было применено на президентских выборах в 2000 году. В ходе этих выборов американскими специалистами был установлен высокий процент ошибок и сбоев у старых карточных автоматов. В 2002 году в США был принят закон Help America Vote Act (Акт содействия голосованию), установивший обязательное использование электронного голосования во всех штатах.

В США используются системы электронного голосования компаний Diebold, ES & S. Эти системы включают в себя, как правило, одно или несколько устройств для голосования, используемых для фиксирования (записи) голосов. Отактильным экраном, на котором отображается электронный бюллетень. Избирателю следует сделать выбор, подтвердив свое решение нажатием кнопки на аппарате.

Системы электронного голосования, использующие публичные сети, применяют электронные бюллетени. Результаты голосования передаются по сетям. Примером таких систем является голосование через Интернет и SMS. Информация может передаваться как по одному голосу, так и периодически набором голосов или по окончании времени голосования.

Для того, чтобы проголосовать, пользователю необходимо иметь «открытый» и «закрытый» ключи. «Открытый» используется для регистрации на сайте голосования, «закрытый» - как правило, для шифрования результата голосования.

Впервые в Швейцарии на федеральном уровне, Интернет - голосование было успешно проведено в 2004 году. Именного списка голосующих через Интернет нет, только номера действительных карточек. Поэтому при прочтении результата голосования посторонним лицом, определить личность проголосовавшего нельзя. Для

Инв. № подл.	Подпись и дата																		
	Инв. № дубл.																		
	Взам. инв. №																		
	Подпись и дата																		
<table border="1"> <tr> <td>Изм.</td> <td>Лис</td> <td>№ докум.</td> <td>Подпись</td> <td>Дата</td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </table>					Изм.	Лис	№ докум.	Подпись	Дата										
Изм.	Лис	№ докум.	Подпись	Дата															
<div style="text-align: right; font-size: 1.2em; font-weight: bold;">ИИБТ.10.05.02.066</div>																			
<div style="text-align: right;"> <div>Лист</div> <div>8</div> </div>																			

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

СПГ идентифицирует личность избирателя при помощи идентификационной карты, предоставляет избирателю список кандидатов его избирательного округа и получает зашифрованный и подтвержденный цифровой подписью электронный голос. СПГ также проверяет информацию о том, имеет ли пользователь право голоса и проголосовал ли он уже. Если избиратель не имеет право голосовать, то выводится соответствующее сообщение и он направляется в службу, предоставляемую Системой учета населения. Если пользователь уже проголосовал, его об этом информируют. Электронный голос отсылается на сервер хранения голосов пользователю приходит подтверждение о том, что его голос засчитан. Цифровые подписи отделяются от зашифрованных голосов. Результаты электронного голосования

ИИВТ.10.05.02.066

определяет программа подсчета голосов. По завершении периода подачи жалоб секретный ключ уничтожается. [3]

В таблице 1.1 сравним по параметрам существующие системы голосования. «+» – параметр реализован в системе, «-» – не реализован.

Таблица 1.1 – Сравнение существующих систем голосования по параметрам

Параметр	Бумажное	Бумажно- электронное	Электронное с прямой запи- сью	Электронное через пуб- личные сети
Соответствует требованиям, предъявленным в разделе 1.2	+	+	+	+
Автоматизиро- ванный подсчет голосов	-	+	+	+
Автоматизиро- ванный сбор го- лосов	-	-	+	+
Возможно прого- лосовать дистан- ционно	-	-	-	+

1.4 Модель угроз и нарушителей безопасности информации

В соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для

Инов. № подл.	Подпись и дата
Инов. № дубл.	
Взам. инв. №	
Подпись и дата	
Инов. № подл.	

Изм.	Лис	№ докум.	Подпись	Дата

ИИВТ.10.05.02.066

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

- В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» установлено, что ПТК ДЭГ имеет следующие характеристики:

- При разработке Модели угроз применялись методики, определённые в методическом документе ФСТЭК России «Методика определения угроз безопасности информации в информационных системах».

Таблица 1.2 – Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации

№	Виды риска	Возможные последствия
У1	Ущерб физическому лицу	Нарушение конфиденциальности (утечка) персональных данных. «Травля» гражданина в сети «Интернет». Разглашение персональных данных граждан

Продолжение таблицы 1.2

№	Виды риска	Возможные последствия
У2	Риски юридическому лицу, индивидуальному предпринимателю	Нарушение законодательства Российской Федерации. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса Потеря клиентов, поставщиков. Потеря конкурентного преимущества.
У3	Ущерб государству в области обеспечения обороны страны, безопасности правопорядка, социальной, политической, сферах деятельности	Нарушение выборного процесса. Отсутствие доступа к государственной услуге. Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др. Появление негативных публикаций в общедоступных источниках. Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. Использование веб-ресурсов государственных органов для распространения и управления вредоносным программным обеспечением. Утечка информации ограниченного доступа. Непредставление государственных услуг

Определим объекты взаимодействия и виды воздействия на них таблице 1.3

Инов. № подл.	Подпись и дата	Взаим. инв. №	Инов. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						12

Таблица 1.3 – Объекты воздействия и виды воздействия на них

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан (У1)	База данных информационной системы, содержащая идентификационную информацию граждан	Утечка идентификационной информации граждан из базы данных
	Линия связи между сервером авторизации и обработки данных.	Перехват информации, содержащей идентификационную информацию и граждан, передаваемой по линиям связи.
	Приложение информационной системы, обрабатывающей идентификационную информацию граждан	Несанкционированный доступ к идентификационной информации граждан, содержащейся в приложении информационной системы
Непредставление государственных услуг (У3)	Приложение голосования	Отказ в обслуживании приложения
	Сервер баз данных портала государственных услуг	Отказ в обслуживании сервера управления базами данных
		Подмена информации в базах данных на недостоверную
		Утечка персональных данных граждан

Инов. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата

ИИБТ.10.05.02.066

Продолжение таблицы 1.4

Тип нарушителя	Вид нарушителя
Внешний	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ
	Конкурирующие организации
	Авторизованные пользователи систем и сетей
	Лица, обеспечивающие поставку, сопровождение и ремонт технических средств ПТК ДЭГ
Внутренний	Пользователи ПТК ДЭГ
	Бывшие работники
	Администраторы ПТК ДЭГ
	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ
	Обслуживающий персонал

При определении источников угроз безопасности информации необходимо исходить из предположения о наличии повышенной мотивации внешних и внутренних нарушителей, преднамеренно реализующих угрозы безопасности информации.

Кроме того, необходимо учитывать, что такие виды нарушителей как специальные службы иностранных государств и террористические, экстремистские группировки могут привлекать (входить в сговор) внутренних нарушителей, в том числе обладающих привилегированными правами доступа. В этом случае уровень возможностей актуальных нарушителей будет определяться совокупностью возможностей нарушителей, входящих в сговор.

В таблице 1.5 рассмотрим возможную мотивация рассмотренных выше нарушителей.

Инва. № подл.	Подпись и дата	Взаим. инв. №	Инва. № дубл.	Подпись и дата	<p>При определении источников угроз безопасности информации необходимо исходить из предположения о наличии повышенной мотивации внешних и внутренних нарушителей, преднамеренно реализующих угрозы безопасности информации.</p> <p>Кроме того, необходимо учитывать, что такие виды нарушителей как специальные службы иностранных государств и террористические, экстремистские группировки могут привлекать (входить в сговор) внутренних нарушителей, в том числе обладающих привилегированными правами доступа. В этом случае уровень возможностей актуальных нарушителей будет определяться совокупностью возможностей нарушителей, входящих в сговор.</p> <p>В таблице 1.5 рассмотрим возможную мотивация рассмотренных выше нарушителей.</p>
					<p>ИИВТ.10.05.02.066</p>
Изм.	Лис	№ докум.	Подпись	Дата	<p>15</p>

Таблица 1.5 – Возможные цели реализации угроз безопасности информации нарушителями

Виды нарушителя	Возможные цели реализации угроз безопасности информации
Специальные службы иностранных государств	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутривнутриполитического кризиса
Террористические, экстремистские группировки	Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций
Преступные группы (криминальные структуры) Отдельные физические лица	Получение финансовой или иной материальной выгоды. Желание самореализации

Инов. № подл.	Подпись и дата
Взаим. инв. №	Инов. № дубл.
Подпись и дата	
Инов. № подл.	

Изм.	Лис	№ докум.	Подпись	Дата

ИИБТ.10.05.02.066

Продолжение таблицы 1.5

Виды нарушителя	Возможные цели реализации угроз безопасности информации
Разработчики программных, программно-аппаратных средств	<p>Внедрение функциональных программные аппаратные средства на этапе разработки.</p> <p>Получение конкурентных преимуществ.</p> <p>Получение финансовой или иной материальной выгоды.</p> <p>Непреднамеренные, неосторожные или неквалифицированные действия</p>
<p>Лица, обеспечивающие поставку программных, программно- аппаратных средств, обеспечивающих систем</p> <p>Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ</p>	<p>Получение финансовой или иной материальной выгоды.</p> <p>Непреднамеренные, неосторожные или неквалифицированные действия.</p> <p>Получение конкурентных преимуществ</p>
<p>Авторизованные пользователи систем и сетей</p> <p>Системные администраторы и администраторы безопасности</p>	<p>Получение финансовой или иной материальной выгоды.</p> <p>Любопытство или самореализации.</p> <p>Месть за ранее совершенные действия.</p> <p>Непреднамеренные, неосторожные или неквалифицированные действия.</p>

Инов. № подл.	Подпись и дата
Взаим. инв. №	Инов. № дубл.
Подпись и дата	

Изм.	Лис	№ докум.	Подпись	Дата

ИИБТ.10.05.02.066

Организационные меры и средства защиты информации, применяемые в ПТК, должны обеспечивать защиту от угроз безопасности информации, связанных с действиями нарушителей с высоким потенциалом.

В качестве исходных данных для определения угроз безопасности информации использовался банк данных угроз безопасности информации (bdu.fstec.ru)

Рассматриваются угрозы:

- угроза внедрения кода или данных (УБИ. 006);
- угроза восстановления и/или повторного использования аутентификационной информации (УБИ. 008);
- угроза использования информации идентификации/аутентификации, заданной по умолчанию (УБИ. 030);
- угроза несанкционированного доступа к аутентификационной информации (УБИ. 074);
- угроза несанкционированного изменения аутентификационной информации (УБИ. 086);
- угроза обхода некорректно настроенных механизмов аутентификации (УБИ. 100);
- угроза перехвата данных, передаваемых по вычислительной сети (УБИ. 116);
- угроза удаления аутентификационной информации (УБИ. 152).

Также в ПТК ДЭГ рассматриваются угрозы, связанные с использованием протоколов голосования. К данным угрозам относятся:

- возможность со стороны нарушителя, используя ПО и технологические решения ПТК ДЭГ извлечь сведения о выборе избирателя, группы избирателей, всех избирателей, а также идентифицировать избирателя по выбору;
- возможность реализации голосования более одного раза;
- подмена голосов избирателей;
- некорректная запись голоса избирателя;

Инев. № подл.	Подпись и дата	Взам. инв. №	Инев. № дубл.	Подпись и дата

Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						18

- досрочное прекращение голосования;
- деанонимизация избирателя;
- установление промежуточных итогов голосования до его завершения.

В составе ПТК ДЭГ необходимо использовать сертифицированные по требованиям безопасности информации средства защиты информации:

- средства защиты информации не ниже 4 класса и соответствующие 4 уровню доверия;
- средства контроля съемных машинных носителей информации не ниже 4 класса;
- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений не ниже 4 класса;
- средства антивирусной защиты не ниже 4 класса;
- средства межсетевого экранирования не ниже 4 класса;
- средства доверенной загрузки не ниже 4 класса.

В ПТК ДЭГ предполагаемый к использованию класс криптографической защиты для нейтрализации угроз безопасности информации при передаче персональных и иных данных по каналам связи между ЦОД ПТК ДЭГ определен как КА.

Для реализации подсистемы подключения пользователей к порталам ЕПГУ и ПТК ДЭГ для авторизации пользователей и получения бюллетеня голосования предполагаемый к использованию класс криптографической защиты для серверной компоненты класс СКЗИ определен как КСЗ.

Предполагаемый к использованию класс криптографической защиты в сегменте пользователей ПТК ДЭГ (избиратель) для подключения пользователей к порталам ЕПГУ и ПТК ДЭГ, авторизации пользователей и получения бюллетеня голосования, для нейтрализации угроз безопасности информации при передаче персональных данных по каналам связи, а также наложения и проверки ЭП определен как КС1.

Предполагаемый к использованию класс криптографической защиты на стороне администраторов управления, председателей и членов ИК ДЭГ (председатель

Инва. № подл.	Подпись и дата
Взаим. инв. №	Инва. № дубл.
Подпись и дата	
Инва. № подл.	

Изм.	Лис	№ докум.	Подпись	Дата	ИИБТ.10.05.02.066	Лист 19

ИК ДЭГ, оператор ИК ДЭГ, администраторы ИТ, администраторы ИБ), при взаимодействии с ПТК ДЭГ по каналам связи выходящими за пределы ЦОД, ввиду регулярного характера взаимодействия с системой и категории обрабатываемых данных (управляющая информация) определен как КА.

Предполагаемый к использованию класс криптографической защиты на стороне администраторов управления, председателей и членов ИК ДЭГ (председатель ИК ДЭГ, оператор ИК ДЭГ, администраторы ИТ, администраторы ИБ), при взаимодействии с ПТК ДЭГ по каналам связи не выходящими за пределы контролируемой зоны ЦОД, ввиду регулярного характера взаимодействия с системой и категории обрабатываемых данных (управляющая информация) определен как КСЗ.

Предполагаемый к использованию класс криптографической защиты для ключевого центра определен как класс СКЗИ КА.

При разработке защищенного веб-приложения для электронного голосования необходимо руководствоваться моделями угроз и нарушителя, так как с их помощью удастся построить качественную систему защиты.

1.5 Выводы по разделу

В первом разделе был определен объект разработки, определены требования к ДЭГ. Произведен сравнительный анализ существующих систем голосования, в результате анализа делаем вывод, что из существующих систем голосования, можем использовать технологию голосования через публичные сети, так как только она обеспечивает возможность проголосовать дистанционно.

Спрогнозированы угрозы и уязвимости разрабатываемой системы и рассмотрены способы их предотвращения. Также была разработана модель потенциального нарушителя информационной безопасности веб-приложения для электронного голосования.

Инв. № подл.	Подпись и дата				ИИВТ.10.05.02.066	Лист 20
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
<div> <div>Изм.</div> <div>Лис</div> <div>№ докум.</div> <div>Подпись</div> <div>Дата</div> </div>						

В составе ПТК ДЭГ необходимо использовать сертифицированные по требованиям безопасности информации средства защиты информации средства защиты информации не ниже 4 класса и соответствующие 4 уровню доверия.

Для ПТК ДЭГ необходимо обеспечить выполнения требований, предъявляемых к 1 (первому) классу защищенности информационных систем.

В ПТК ДЭГ необходимо обеспечить третий уровень защищенности персональных данных при их обработке в ПТК ДЭГ (УЗ-3).

Инв. № подл.	Подпись и дата				<div>ИИБТ.10.05.02.066</div> <div>Лист 21</div>
	Инв. № дубл.				
	Взаим. инв. №				
	Подпись и дата				
Изм.	Лис	№ докум.	Подпись	Дата	

2.1 Постановка задачи

В данной главе необходимо проработать технические решения для разработки системы голосование, выбрать из существующих протоколов тайного голосования или разработать собственный в соответствии с требованиями, поставленными в разделе 1.3

Необходимо разработать концепцию модулей системы в соответствии с протоколом и требованиями к системе. Спланировать архитектуру разрабатываемого веб-приложения и отобразить принцип взаимодействия пользователя с системой. Учитывая эти сведения, нужно определить какая техническая база будет использоваться при разработке веб-приложения.

2.2 Сравнительный анализ протоколов электронного голосования

Целью данной главы является выбор протокола голосования, который отвечает требованиям выставленным нами в разделе 1.3

Рассмотрим алгоритм простого протокола электронного голосования:

Шаг 1. Агентство, проводящее электронное голосование (далее А) выкладывает списки возможных участников выборов.

Шаг 2. Участник, допущенный к выборам (далее В) сообщает о своем намерении участвовать в голосовании.

Шаг 3. А выкладывает списки зарегистрированных В.

Шаг 4. А создает закрытый ($K_{A_{\text{зак}}}$) и открытый ($K_{A_{\text{отк}}}$) ключ и выкладывает в общий доступ $K_{A_{\text{отк}}}$, чтобы любой мог зашифровать сообщение, но расшифровать мог только А.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Шаг 5. В создает свои ключи $K_{В_{зак}}$ и $K_{В_{отк}}$ и выкладывает в общий доступ $K_{В_{отк}}$, чтобы любой мог проверить его электронный избирательный бюллетень (далее С), но подписать мог только он сам.

Шаг 6. В формирует сообщение С, где выражает свой выбор, подписывает $K_{В_{зак}}$, шифрует $K_{А_{отк}}$ и отправляет А.

Шаг 7. А собирает С, расшифровывает с помощью $K_{В_{отк}}$ и публикует подсчитанные результаты.

Довольно простой протокол, помогает защититься от подделки голосов и внешнего вмешательства, но В должен доверять А, чья работа никем не контролируется. [4]

Далее рассмотрим алгоритм протокола Нурми-Салома-Сантина или другими словами протокола двух агентств:

Шаг 1. Валидатор (далее V) отправляет секретные опознавательные метки (далее М) всем В до голосования.

Шаг 2. V отправляет А весь набор М, но без информации о том, кому они принадлежат.

Шаг 3. В создает свои ключи $K_{В_{зак}}$, $K_{В_{отк}}$ и выкладывает в общий доступ $K_{В_{отк}}$, а также создает секретный ключ ($K_{В_{сек}}$), который нужен, чтобы никто не узнал содержимое бюллетеня до нужного момента.

Шаг 4. В формирует сообщение С, где выражает свой выбор, подписывает $K_{В_{зак}}$, прикладывает к нему полученную М и шифрует $K_{В_{сек}}$.

Шаг 5. К зашифрованному тексту В прикладывает М и отправляет А.

Шаг 6. А получает зашифрованный текст, по М определяет, что он пришел от В, но не знает от кого именно и как В проголосовал, после публикует его.

Шаг 7. Опубликованный зашифрованный текст служит информацией, чтобы В отправил $K_{В_{сек}}$.

Шаг 8. А собирает ключи, расшифровывает текст, подсчитывает голоса и присоединяет к опубликованному зашифрованному тексту С без М.

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						23

Следующим рассмотрим алгоритм протокола Фудзиока-Окамoto-Охта. Частично решает проблему сговора двух агентств. Работа протокола заключается в заранее выбранном способе маскирующего шифрования – это особый вид шифрования, который позволяет убедиться, что документ подлинный и был подписан авторизованным пользователем, но не дает информации о содержащихся данных. Алгоритм выглядит следующим образом:

Шаг 2. В создает свои ключи $K_{\text{Взак}}$, $K_{\text{Вотк}}$, $K_{\text{Всек}}$ и выкладывает в общий до-
 $K_{\text{Вотк}}$.

Шаг 4. V создает свои ключи $K_{V_{\text{зак}}}$, $K_{V_{\text{отк}}}$ и выкладывает в общий доступ $K_{V_{\text{отк}}}$.

Шаг 5. V удостоверяется, что С принадлежит В, который еще не голосовал, подписывает его $K_{V_{\text{зак}}}$ и отправляет В.

Шаг 6. В удаляет слой маскирующего шифрования и отправляет сообщение
С к А.

Шаг 7. А проверяет подписи В и V и помещает зашифрованный С в специальный список, который будет опубликован после голосования.

Шаг 8. После публикации списка, В отправляет А свой $K_{B_{сек}}$.

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата	ступ $K_{V_{отк}}$.	
					Шаг 3. В формирует сообщение С, где выражает свой выбор, шифрует его $K_{V_{сек}}$, маскирует, подписывает $K_{V_{зак}}$ и отправляет V.	
					Шаг 4. V создает свои ключи $K_{V_{зак}}$, $K_{V_{отк}}$ и выкладывает в общий доступ $K_{V_{отк}}$.	
					Шаг 5. V удостоверяется, что С принадлежит В, который еще не голосовал, подписывает его $K_{V_{зак}}$ и отправляет В.	
					Шаг 6. В удаляет слой маскирующего шифрования и отправляет сообщение С к А.	
Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата	Шаг 7. А проверяет подписи В и V и помещает зашифрованный С в специальный список, который будет опубликован после голосования.	
					Шаг 8. После публикации списка, В отправляет А свой $K_{V_{сек}}$.	
Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						24

Шаг 6. В формирует сообщение С, где выражает свой выбор, шифрует его созданным $K_{B_{сек}}$ и отправляет А набор состоящий из $K_{B_{отк}}$, зашифрованного $K_{B_{сек}}$ сообщениеСи зашифрованную $K_{B_{зак}}$ хэш-функцию от зашифрованного $K_{B_{сек}}$ сообщения С.

Шаг 7. А проверяет $K_{B_{отк}}$ со списком, созданным ранее, сравнивает хэш-функцию сообщения С зашифрованного $K_{B_{сек}}$ и хэш-функцию, полученную при помощи $K_{B_{зак}}$ и публикует весь набор в открытом списке.

Шаг 8. После публикации списка В отправляет А новый набор состоящий из $K_{B_{отк}}$, $K_{B_{сек}}$ и зашифрованную $K_{B_{зак}}$ хэш-функцию от $K_{B_{сек}}$.

Шаг 9. А проверяет подлинность $K_{B_{сек}}$, сравнивая хэш-функцию от $K_{B_{сек}}$ и хэш-функцию полученную при помощи $K_{B_{зак}}$, если все верно, то расшифровывает полученную ранее С, публикует все данные и подсчитывает голоса.

Шаг 10. После голосования V публикует утвержденный список В, а А – список авторизованных ключей. [8]

А и V не могут тайно сговориться, потому что публикуют списки, поэтому нельзя внести несуществующих избирателей и проголосовать за не пришедших. Минусами является уязвимость перед DoS-атаками, так как требуется большое количество ресурсов для поддержания работоспособности протокола из-за его сложности.

2.3 Разработка концепции модулей системы голосования

При бумажном голосовании тайна голосования обеспечивается физическим разрывом между двумя местами — местом, где избиратель удостоверяет своё право голосовать, и местом, где он отдаёт голос. В первом месте — это столик избирательной комиссии участка — избиратель идентифицируется по паспорту и ему выдаётся анонимизированный бюллетень. Во втором месте — урне для голосования

Инов. № подл.	Подпись и дата	Взаим. инв. №	Инов. № дубл.	Подпись и дата						
Изм.	Лис	№ докум.	Подпись	Дата	ИИБТ.10.05.02.066					Лист
										26

— сам факт наличия бюллетеня является подтверждением права на голосование, личность избирателя уже неважна и, собственно, неизвестна.

В абсолютном большинстве систем электронного голосования, этого разрыва нет: аутентификация и голосование проходят на одном и том же сервере, находящемся под контролем одних и тех же людей. Каковые, разумеется, могут иметь собственные политические интересы и, соответственно, быть потенциально нечистоплотными на руку.

В ДЭГ можно реализовать такой физический разрыв с помощью разделение системы на два разных сервера.

Сервер регистратор пользователей проверяет, может ли данный пользователь голосовать, а сервер учета голосов – производит учет и подсчет голосов

Сервер регистратор хранит в себе списки пользователей, а также публичный и приватные ключи.

Аутентификацией и авторизацией пользователей занимается сторонняя система, которой доверяют проводящие голосование, чтобы сама система электронного голосования могла быть использована в любых видах голосования. В зависимости от целей и важности голосования, аутентификация может проводиться:

– Парой логин-пароль или PIN-кодом по SMS (например, соцпросы или решение локальных вопросов городского хозяйства)

– По номеру партбилета пользователя, включая электронный партбилет на базе NFC/RFID (например, текущие внутрипартийные голосования)

– По аутентификации в ЕСИА (внутрипартийные праймериз, внепартийные голосования, включая общегосударственные выборы и референдумы)

ЕСИА — Единая система идентификации и аутентификации — это система авторизации в «Госуслугах»

Отметим, что биометрические датчики смартфонов (датчик отпечатка глаза, радужки глаза и т.п.) использоваться для аутентификации в электоральных системах не могут, т.к. не передают наружу собственно биометрические данные, а лишь подтверждают, что данное лицо является владельцем данного смартфона. Владелец

Инд. № подл.	Подпись и дата				Инд. № дубл.	Взаим. инв. №	Подпись и дата	Инд. № подл.						Лист 27
Изм.	Лис	№ докум.	Подпись	Дата	ИИБТ.10.05.02.066									

пяти смартфонов, соответственно, сможет аутентифицироваться пять раз. Эти датчики могут использоваться лишь для подтверждения доступа к приложению, используемому для голосования, чтобы посторонний человек, получивший доступ к смартфону, не отдал голос за его владельца.

Использование биометрических данных для аутентификации в системе голосования потенциально возможно, но лишь в случае добровольного предоставления их пользователями и обработки со стороны сервера аутентификации пользователей — например, по фотографии лица.

При успешном прохождении аутентификации и авторизации, сервис аутентификации выдает регистратору только уникальный идентификатор пользователя в любом формате. Этот идентификатор хешируется и попадает в список голосующих. Таким образом сервер регистратор не хранит в себе конфиденциальных данных голосующих. Даже в случае раскрытия списка голосующих, соотнести полученные идентификаторы с реальными людьми не представляется возможным.

Пользователь может подписывать свои бюллетени сколько угодно раз. Это необходимо на случай утери подписанного бюллетеня. Проверкой, что пользователь голосует только один раз, занимается сервер подсчета голосов.

Сервер учета голосов хранит в себе список с зашифрованными бюллетенями, а также список с зашифрованными приватными ключами пользователей. База данных с зашифрованными бюллетенями периодически реплицируется и отправляется на устройства наблюдателей. В конце голосования, сервер расшифровывает приватные ключи, отправляет их наблюдателям вместе с итоговым списком бюллетеней. Расшифровывает бюллетени и производит подсчет голосов.

Приложение голосующего, хранит в себе публичный и приватный ключ голосующего. А также бюллетень, полученный от сервера подсчета голосов, после удачной отправки бюллетеня. При проверке бюллетеня пользователем, приложение проверяет верность подписи сервера учета голосов, чтобы исключить подмену бюллетеня злоумышленниками. Во время голосования приложение сохраняет логи в зашифрованном виде, чтобы использовать их при расследовании случая, что

Инва. № подл.	Подпись и дата
Взаим. инв. №	Инва. № дубл.
Подпись и дата	

Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						28

голосующий утверждает, что его голос учтен неверно. В логах пишется действия пользователя в программе, а также процессы, которые делает программа. Это необходимо для обнаружения уязвимостей, а также для исключения саботажа выборов. Под саботажем в данном случае понимается, что голос учелся верно, но голосующий решил сорвать выборы и объявить их неверными в случае, если результаты выборов его не устроили.

В ходе голосования наблюдатели получают копию списка бюллетеней, и могут сравнивать реплики между собой, например, что бюллетени в прошлой реплике остались прежними в текущей. Так же по списку бюллетеней можно вести подсчет сколько участников уже проголосовало и исследовать количество голосов по времени. Технические специалисты могут следить за работой сервера учета голосов: смотреть сколько и какие бюллетени поступили на вход серверу учета голосов, сколько и какие были приняты, если есть непринятые, то по какой причине. Отправились ли голосующему подписанные бюллетени.

В момент окончания голосования и публикации его результатов приватные ключи для расшифровки списка бюллетеней, которые реплицировались в ходе голосования рассылается наблюдателям, так что они могут самостоятельно подсчитать результат голосования и сравнить его с опубликованным — это сделает невозможной подмену результата.

Кроме того, наблюдатели могут сверить число голосов, зарегистрированных сервером учёта голосов, с числом избирателей, зарегистрированных сервером аутентификации, чтобы исключить вариант вброса анонимных голосов владельцами сервера учёта голосов тем более, что потенциально они являются единственными людьми, способными отслеживать результаты голосования в реальном времени, и потому могут аккуратно подбрасывать голоса в нужную сторону так, чтобы это не было заметно.

Инев. № подл.	Подпись и дата				Инев. № дубл.	Взаим. инв. №	Подпись и дата	Инев. № дубл.	Взаим. инв. №	Подпись и дата	Инев. № подл.
Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066					Лист	
										29	

2.4 Выводы по разделу

В данном разделе были проработаны технические решения для разработки системы дистанционного электронного голосования.

Для реализации системы дистанционного электронного голосования выберем протокол Sensus. Так как он отвечает требованиям, предъявленным в главе 1.3. А также является самым подходящим протоколом с учетом большого количества устройств с различными вычислительными способностями и качеством соединения.

Система голосования представляет собой сервер регистратор, сервер учета голосов, систему аудита и клиентское приложение.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066					Лист
										30

3 Разработка системы дистанционного электронного голосования

3.1 Постановка задачи

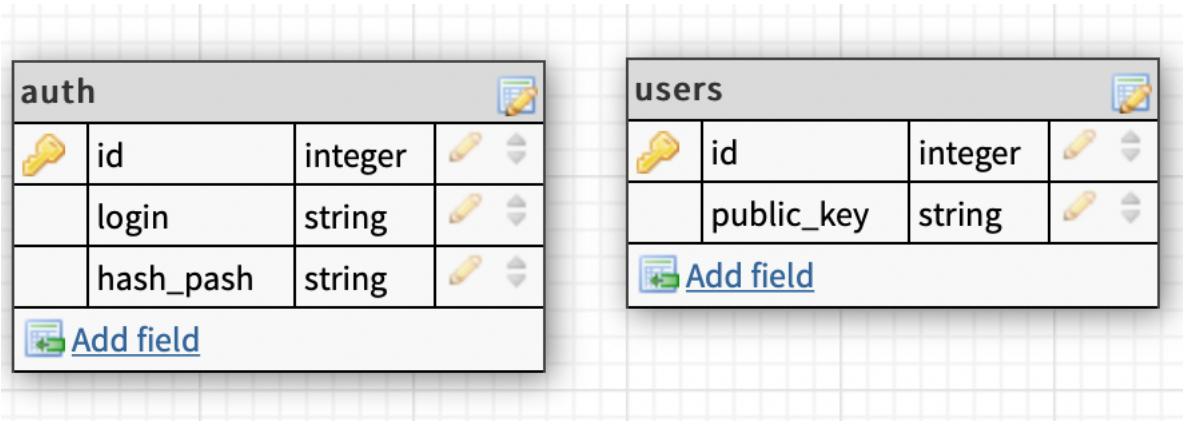
В данной главе необходимо разработать систему дистанционного электронного голосования в соответствии с техническими решениями, представленными в главе 2.

3.2 Разработка сервиса авторизации

Для начало необходимо спроектировать базу данных сервиса. По техническому заданию, в ней будут храниться идентификаторы голосующих. Так же заложим сюда модуль авторизации и регистрации, для случая, если систему голосования не будут использовать уже с существующей системой авторизации, например ЕСИА.

В соответствии с входными данными в качестве СУБД используется PostgreSQL. На рисунке 3.1 изображена схема базы данных.

Рисунок 3.1 – Схема базы данных сервиса авторизации



Основой таблицей сервиса является таблица users. В ней хранится некий идентификатор пользователя - id, чтобы идентифицировать его только во время голосования. За рамками процесса голосования этот идентификатор ничего не

значит. И так же хранится его публичный ключ, который пользователь публикует сам при своем голосовании.

Так же есть таблица `auth`, она используется в случае, если к системе не подключают сторонний сервис авторизации, например ЕСИА. В таком случае таблица `auth` представляет собой хранилище учетных данных пользователей. `Id` – ид пользователя, `login` – логин пользователя, `hash pass` – хеш от пароля.

Пользователь пришлет запрос на авторизацию, прислав свой логин и пароль, сервис авторизации перенаправит запрос к стороннему сервису, если он подключен, иначе авторизует через таблицу auth. В таблице auth хранится список пользователей, которым разрешено голосовать.







После прохождения авторизации, сервис подписывает своим ключом сообщение и отправляет его обратно пользователю. Исходный код представлен в приложении А, `authorisator.py`

В ходе голосования наблюдатели получают копию списка бюллетеней, и могут сравнивать реплики между собой, например, что бюллетени в прошлой реплике остались прежними в текущей. Так же по списку бюллетеней можно вести подсчет сколько участников уже проголосовало и исследовать количество голосов по времени. Технические специалисты могут следить за работой сервера учета голосов: смотреть сколько и какие бюллетени поступили на вход серверу учета голосов, сколько и какие были приняты, если есть непринятые, то по какой причине. Отправились ли голосующему подписанные бюллетени.

3.3 Разработка сервиса учета голосов

Так же начнем разработку со схемы базы данных. По техническому заданию в данном сервисе в процессе голосования хранятся зашифрованные бюллетени, рисунок 3.2

Рисунок 3.2 – Схема базы данных сервиса учета голосов

bulletins			
	id	integer	 
	secret_key	string	 
 Add field			

Получая запрос от пользователя, сервис проверяет подписи на сообщении, сохраняет бюллетень в таблицу `bulletins`, если подписи верны и запрашивает у пользователя ключ дешифрования сообщения, чтобы позже так же положить его в таблицу `bulletins`.

При успешном прохождении аутентификации и авторизации, сервис аутентификации выдает регистратору только уникальный идентификатор пользователя в любом формате. Этот идентификатор хешируется и попадает в список голосующих. Таким образом сервер регистратор не хранит в себе конфиденциальных данных голосующих. Даже в случае раскрытия списка голосующих, соотнести полученные идентификаторы с реальными людьми не представляется возможным.

Пользователь может подписывать свои бюллетени сколько угодно раз. Это необходимо на случай утери подписанного бюллетеня. Проверкой, что пользователь голосует только один раз, занимается сервер подсчета голосов.

Сервер учета голосов хранит в себе список с зашифрованными бюллетенями, а также список с зашифрованными приватными ключами пользователей. База данных с зашифрованными бюллетенями периодически реплицируется и отправляется на устройства наблюдателей. В конце голосования, сервер расшифровывает приватные ключи, отправляет их наблюдателям вместе с итоговыми списками бюллетеней. Расшифровывает бюллетени и производит подсчет голосов.

В ходе голосования наблюдатели получают копию списка бюллетеней, и могут сравнивать реплики между собой, например, что бюллетени в прошлой реплике остались прежними в текущей. Так же по списку бюллетеней можно вести подсчет сколько участников уже проголосовало и исследовать количество голосов по

[illegible]

времени. Технические специалисты могут следить за работой сервера учета голосов: смотреть сколько и какие бюллетени поступили на вход серверу учета голосов, сколько и какие были приняты, если есть непринятые, то по какой причине. Отправились ли голосующему подписанные бюллетени.

3.4 Разработка модуля аудита

В ходе голосования наблюдатели получают копию списка бюллетеней, и могут сравнивать реплики между собой, например, что бюллетени в прошлой реплике остались прежними в текущей. Так же по списку бюллетеней можно вести подсчет сколько участников уже проголосовало и исследовать количество голосов по времени. Технические специалисты могут следить за работой сервера учета голосов: смотреть сколько и какие бюллетени поступили на вход серверу учета голосов, сколько и какие были приняты, если есть непринятые, то по какой причине. Отправились ли голосующему подписанные бюллетени.

В момент окончания голосования и публикации его результатов приватные ключи для расшифровки списка бюллетеней, которые реплицировались в ходе голосования рассылается наблюдателям, так что они могут самостоятельно подсчитать результат голосования и сравнить его с опубликованным — это сделает невозможной подмену результата.

Кроме того, наблюдатели могут сверить число голосов, зарегистрированных сервером учёта голосов, с числом избирателей, зарегистрированных сервером аутентификации, чтобы исключить вариант вброса анонимных голосов владельцами сервера учёта голосов тем более, что потенциально они являются единственными людьми, способными отслеживать результаты голосования в реальном времени, и потому могут аккуратно подбрасывать голоса в нужную сторону так, чтобы это не было заметно.

Инев. № подл.	Подпись и дата				Инев. № докл.	Взам. инв. №	Инев. № дубл.	Подпись и дата	
Изм.	Лис	№ докум.	Подпись	Дата	ИИБТ.10.05.02.066				Лист
									34

В ходе голосования наблюдатели получают копию списка бюллетеней, и могут сравнивать реплики между собой, например, что бюллетени в прошлой реплике остались прежними в текущей. Так же по списку бюллетеней можно вести подсчет сколько участников уже проголосовало и исследовать количество голосов по времени. Технические специалисты могут следить за работой сервера учета голосов: смотреть сколько и какие бюллетени поступили на вход серверу учета голосов, сколько и какие были приняты, если есть непринятые, то по какой причине. Отправились ли голосующему подписанные бюллетени.

3.5 Разработка модуля клиента

В соответствии со входными данными в качестве клиентского приложения будет разработано приложение для компьютера с помощью библиотеки Tkinter.

Для клиента понадобится 4 экрана: авторизация, регистрация, голосование, результат голосования (экран, где пользователю показываем, что его голос успешно учтен).

Начнем с экрана авторизации. В рамках ВКР будем пользоваться, нами же разработанным модулем авторизации. Для авторизации пользователя будем использовать связку логин-пароль. Для реализации нам понадобится 2 поля для ввода, 2 текстовых поля и кнопка. Реализуем в виде класса LoginFrame. Исходный код находится в Приложении А client.py.

При инициализации класса отображаем два текстовых поля, для указания куда вводить логин и пароль, а под ними два поля ввода и еще ниже кнопку. Обработчик для кнопки обращается в сервис авторизации и в случае успеха уничтожает все созданные объекты и передает управление классу, отвечающему за следующий экран. В случае неудачи появится сообщение с текстом: «Неверный логин или пароль!». На рисунке 3.3 изображен интерфейс авторизации, а на рисунке 3.4— сообщение об ошибке

Инев. № подл.	Подпись и дата	Инев. № дубл.	Подпись и дата	Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист 35

Рисунок 3.3 – Интерфейс авторизации

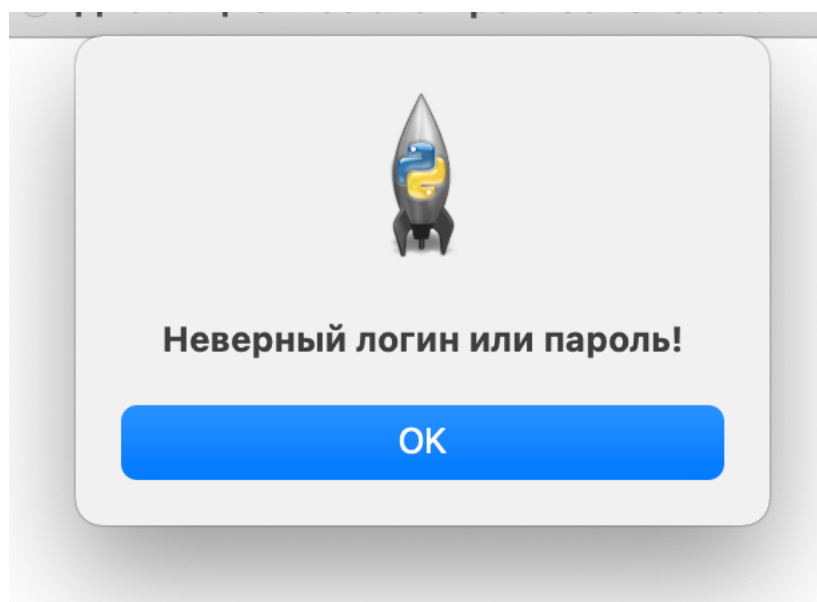
Дистанционное электронное голосование

Логин

Пароль

Войти

Рисунок 3.4 – Сообщение об ошибке

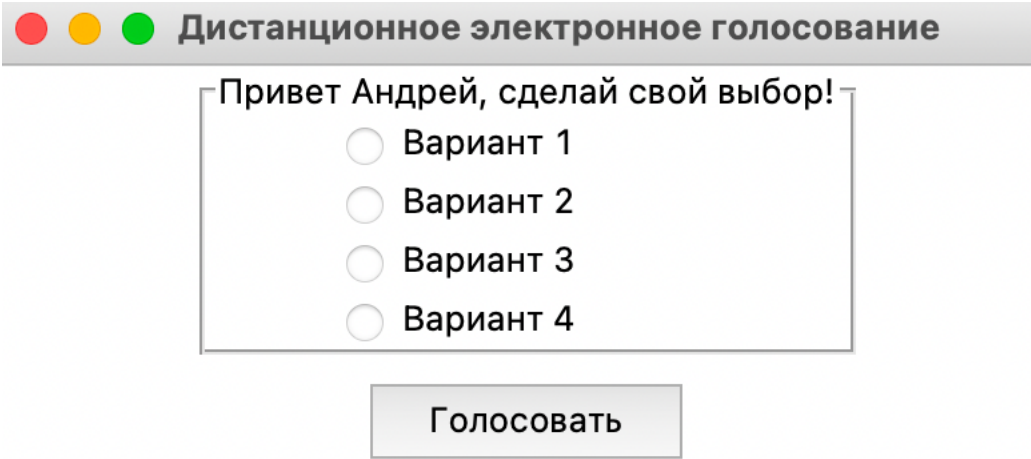


После авторизации пользователю сразу же предлагается произвести голосование, путем выбора одного из вариантов, рисунок 3.5

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

					ИИВТ.10.05.02.066	Лист
						36
Изм.	Лист	№ докум.	Подпись	Дата		

Рисунок 3.4 – Экран голосования с вариантами



За реализацию этого экрана отвечает класс ChoiceCandidate. Исходный код находится в Приложении А client.py. Варианты выбора были сделаны с помощью Radiobutton. Сами варианты были получены от сервиса учета голосов.

При выборе варианта и нажатии на кнопку «Голосовать» запускается протокол тайного голосования Sensus. Исходный код хранится в приложении А protocol_client.py.

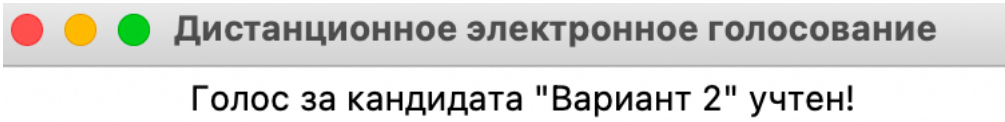
В соответствии с протоколом генерируется открытый и закрытый ключ для подписи RSA 2048 бит, а также ключ для шифрования RSA 2048 бит и ключ для ослепляющего шифрования. Сообщение шифруется, подписывается, и накладывается слой ослепляющего шифрования. Далее на сервис авторизации отправляется сообщение и публичный ключ отправляется публичный ключ. От сервиса авторизации получаем сообщение обратно, уже подписанное сервисом, снимается слой ослепляющего шифрования и сообщение с публичным ключом отправляется на сервис учета голосов. От сервиса получаем ответ, что сообщение принято, отправляем ключ для дешифрования и отображаем экран пользователю с сообщением, о том, что голос учтен, рисунок 3.5.

Для начало необходимо спроектировать базу данных сервиса. По техническому заданию, в ней будут храниться идентификаторы голосующих. Так же заложим сюда модуль авторизации и регистрации, для случая, если систему

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

голосования не будут использовать уже с существующей системой авторизации, например ЕСИА.

Рисунок 3.5 – Экран с результатом голосования.



За этот экран отвечает класс ResultVote, в котором есть только одно текстовое поле. Исходный код находится в Приложении А client.py. На этом процесс голосования для одного пользователя завершен, так же, как и бизнес-логика клиентского приложения.

Приложение голосующего, хранит в себе публичный и приватный ключ голосующего. А также бюллетень, полученный от сервера подсчета голосов, после удачной отправки бюллетеня. При проверке бюллетеня пользователем, приложение проверяет верность подписи сервера учета голосов, чтобы исключить подмену бюллетеня злоумышленниками. Во время голосования приложение сохраняет логи в зашифрованном виде, чтобы использовать их при расследовании случая, что голосующий утверждает, что его голос учтен неверно. В логах пишется действия пользователя в программе, а также процессы, которые делает программа. Это необходимо для обнаружения уязвимостей, а также для исключения саботажа выборов. Под саботажем в данном случае понимается, что голос учелся верно, но голосующий решил сорвать выборы и объявить их неверными в случае, если результаты выборов его не устроили.

3.6 Выводы по разделу

В данном разделе была разработана система дистанционного электронного голосования. Удалось решить все задачи, которые были поставлены в техническом

Подпись и дата	
Инв. № дубл.	
Взаим. инв. №	
Подпись и дата	
Инв. № подл.	

					ИИБТ.10.05.02.066	Лист 38
Изм.	Лис	№ докум.	Подпись	Дата		

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

Лист
39

4 Безопасность жизнедеятельности

4.1 Постановка задачи

В данном разделе необходимо рассмотреть следующие вопросы:

- Особенности воздействия электронных систем на здоровье пользователей;
- Эргономические требования к системам отображения информации;
- Режимы труда и отдыха при работе с электронными устройствами;
- Экологические проблемы утилизации электронных гаджетов.

4.2 Воздействие электронных систем на здоровье пользователей

На пользователя электронных систем может воздействовать ряд опасных и вредных факторов, наиболее значимые из которых следующие:

— Повышенный уровень напряжения в электрических цепях питания и управления ПК, который может привести к электротравме оператора при отсутствии заземления оборудования;

— Излучения от экрана монитора. Как показали результаты многочисленных научных работ с использованием новейшей измерительной техники зарубежного производства, монитор ПК является источником электромагнитного излучения в низкочастотном, высокочастотном и сверхвысокочастотном диапазоне, мягкого рентгеновского излучения от электроннолучевой трубки (ЭЛТ), ультрафиолетового излучения, инфракрасного излучения, электростатического поля

— Не соответствующие нормам параметры микроклимата: повышенная температура из-за постоянного нагрева деталей ПК, пониженная влажность.

— Нарушение норм по аэроионному составу воздуха, особенно в помещениях с разной системой приточно-вытяжной вентиляции и (или) с кондиционерами, при этом концентрация полезных для организма отрицательно заряженных легких

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ИИБТ.10.05.02.066	Лист 40
Изм.	Лис	№ докум.	Подпись	Дата		

ионов кислорода воздуха (аэроионов) может быть в 10-50 раз ниже нормы, а концентрация вредных положительных ионов значительно превышать норму.

— Пониженный или повышенный уровень освещенности в помещении; не соответствующие санитарным нормам визуальные параметры дисплея. Деятельность оператора предполагает, прежде всего, визуальное восприятие отображаемой на экране монитора информации, поэтому значительной нагрузке подвергается зрительный аппарат работающих с ПК.

— Повышенный уровень шума в системном блоке компьютера.

— Повышенный уровень загазованности воздуха; повышенное содержание в воздухе патогенной особенно зимой при повышенной температуре в помещении, плохом проветривании, пониженной влажности, нарушении аэроионного состава воздуха.

Трудовой кодекс обязывает работодателей обеспечить безопасные условия и охрану труда работников на каждом рабочем месте (ст. 212 ТК РФ)

В соответствии с СанПиНом 2.2.2/2.4.1340–03 выдвигаются следующие требования к помещениям для работы с ПЭВМ:

— В производственных помещениях, в которых работа с использованием ПЭВМ является основной (диспетчерские, операторские, расчетные, кабины и посты управления, залы вычислительной техники и др.) и связана с нервно-эмоциональным напряжением, должны обеспечиваться оптимальные параметры микроклимата для категории работ 1а и 1б в соответствии с действующими санитарно-эпидемиологическими нормативами микроклимата производственных помещений. На других рабочих местах следует поддерживать параметры микроклимата на допустимом уровне, соответствующем требованиям указанных выше нормативов.

— В помещениях всех типов образовательных и культурно-развлекательных учреждений для детей и подростков, где расположены ПЭВМ, должны обеспечиваться оптимальные параметры микроклимата, указанные в приложении 2 СанПиН.

Инв. № подл.	Подпись и дата													
	Инв. № дубл.													
	Взам. инв. №													
	Подпись и дата													
<table border="1"> <tr> <td>Изм.</td> <td>Лист</td> <td>№ докум.</td> <td>Подпись</td> <td>Дата</td> </tr> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </table>					Изм.	Лист	№ докум.	Подпись	Дата					
Изм.	Лист	№ докум.	Подпись	Дата										
<div style="text-align: right; font-size: 1.2em; font-weight: bold;">ИИВТ.10.05.02.066</div>														
<div style="display: flex; justify-content: space-between;"> Лист 41 </div>														

— В помещениях, оборудованных ПЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ.

— Уровни положительных и отрицательных аэроионов в воздухе помещений, где расположены ПЭВМ, должны соответствовать действующим санитарно-эпидемиологическим нормативам.

— Содержание вредных химических веществ в воздухе производственных помещений, в которых работа с использованием ПЭВМ является вспомогательной, не должно превышать предельно допустимых концентраций вредных веществ в воздухе рабочей зоны в соответствии с действующими гигиеническими нормативами.

— Содержание вредных химических веществ в производственных помещениях, в которых работа с использованием ПЭВМ является основной (диспетчерские, операторские, расчетные, кабины и посты управления, залы вычислительной техники и др.), не должно превышать предельно допустимых концентраций загрязняющих веществ в атмосферном воздухе населенных мест в соответствии с действующими гигиеническими нормативами.

В таблице 4.1 приведены временные допустимые уровни ЭМП, создаваемых ПЭВМ на рабочих местах, а в таблице 4.2 – визуальные параметры ВДТ, контролируемые на рабочих местах.

Таблица 4.1 – Временные допустимые уровни ЭМП, создаваемых ПЭВМ на рабочих местах

Наименование параметров		ВДУ
Напряженность электрического поля	в диапазоне частот 5 Гц - 2 кГц	25 В/м
	в диапазоне частот 2 кГц - 400 кГц	2,5 В/м
Плотность магнитного потока	в диапазоне частот 5 Гц - 2 кГц	250 нТл
	в диапазоне частот 2 кГц - 400 кГц	25 нТл
Напряженность электростатического поля		15 кВ/м

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Продолжение таблицы 4.1

Параметры	Допустимые значения
Яркость белого поля	Не менее 35 кд/кв. м
Неравномерность яркости рабочего поля	Не более +/- 20%
Контрастность (для монохромного режима)	Не менее 3:1
Временная нестабильность изображения (мелькания)	Не должна фиксироваться
Пространственная нестабильность изображения (дрожание)	Не более 2 x 1E(-4L), где L – проектное расстояние наблюдения, мм

4.3 Эргономические требования к системам отображения информации

Эргономические требования описаны в ГОСТ Р 50948-2001.

При необходимости распознавания или идентификации цветовых параметров прикладная программа должна предлагать устанавливаемый по умолчанию набор цветов, который соответствует требованиям настоящего стандарта. Если цвет может быть изменен пользователем, то должна быть предусмотрена возможность восстановления назначенного по умолчанию набора цветов.

При необходимости точной идентификации цвета в рядах буквенно-цифровых знаков и в полях ввода данных высота символа должна быть не менее 20' при проектном расстоянии наблюдения.

При необходимости точной идентификации цвета обособленного изображения (например, знака или символа) угловой размер изображения должен быть не менее 30' при проектном расстоянии наблюдения (предпочтительно - 40').

Следует избегать применения насыщенного синего цвета для изображений, имеющих угловой размер менее 2°.

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						43

Для чтения текстов, буквенно-цифровых знаков и символов при отрицательной полярности изображения не следует применять синий и красный цвета спектра на темном фоне и красный цвет спектра на синем фоне.

Для чтения текстов, буквенно-цифровых знаков и символов при положительной полярности изображения не следует применять синий цвет спектра на красном фоне.

Насыщенные крайние цвета видимого спектра приводят к нежелательным эффектам глубины изображаемого пространства и не должны применяться для изображений, которые требуют непрерывного просмотра или чтения.

Для точного распознавания и идентификации цветов должны применяться цветное изображение переднего плана на ахроматическом фоне или ахроматическое изображение переднего плана на цветном фоне.

Число цветов, одновременно отображаемых на экране дисплея, должно быть минимальным. Для точной идентификации цвета каждый заданный по умолчанию набор цветов должен включать не более 11 цветов.

При необходимости проведения быстрого поиска, основанного на распознавании цветов, следует применять не более 6 различных цветов.

При необходимости вызова параметров цвета из памяти ЭВМ следует применять не более 6 различных цветов

Яркость знака должна быть не менее 35 кд/м для дисплеев на ЭЛТ и не менее 20 кд/м для плоских дискретных экранов.

Неравномерность яркости рабочего поля экрана должна быть не более 20%.

Неравномерность яркости элементов знака должна быть не более 20%.

Яркостный контраст изображения должен быть не менее 3:1 (для плоских дискретных экранов при угле наблюдения от минус 40° до плюс 40°). Яркостный контраст внутри знака и между знаками должен быть не менее 3:1.

Ширина контура знака должна быть от 0,25 до 0,5 мм.

Степень несведения цветов в любом месте многоцветного экрана для дисплеев на ЭЛТ должна быть не более 3,4' при проектном расстоянии наблюдения.

Инв. № подл.	Подпись и дата				ИИВТ.10.05.02.066	Лист 44
	Инв. № дубл.					
	Взам. инв. №					
	Подпись и дата					
Изм.	Лис	№ докум.	Подпись	Дата		

Изменение размеров однотипных знаков по рабочему полю должно быть в пределах $\pm 5\%$ высоты знака.

Максимальная разность длин строк текста на рабочем поле должна быть не более 2% средней длины строки.

Максимальная разность длин столбцов текста на рабочем поле должна быть не более 2% средней длины столбца.

Отклонение формы рабочего поля от прямоугольника определяют по следующим формулам:

по вертикали

$$\Delta H = 2 \frac{H_1 - H_2}{H_1 + H_2} \leq 0,02 \quad (4.1)$$

по горизонтали

$$\Delta B = 2 \frac{B_1 - B_2}{B_1 + B_2} \leq 0,02 \quad (4.2)$$

по диагонали

$$\Delta D = 2 \frac{D_1 - D_2}{D_1 + D_2} \leq 0,04 \frac{H_1 + H_2}{B_1 + B_2} \quad (4.3)$$

где H_1, H_2, B_1, B_2, D_1 и D_2 - значения длин крайнего левого и крайнего правого столбца, верхней, нижней строки и диагоналей на рабочем поле соответственно, мм.

Временная нестабильность изображения (мелькания) для дисплеев на ЭЛТ и на плоских дискретных экранах не должна быть зафиксирована. Для дисплеев на ЭЛТ частота обновления изображения должна быть не менее 75 Гц при всех режимах разложения, гарантируемых нормативной документацией на конкретный тип дисплея и не менее 60 Гц для дисплеев на плоских дискретных экранах.

Амплитуда смещения изображения (пространственная нестабильность изображения - дрожание) должна быть не более $2 \cdot 10$, где - проектное расстояние наблюдения, мм.

Методы контроля эргономических параметров и параметров безопасности описаны в ГОСТ Р 50949.

Изм.	Лист	№ докум.	Подпись	Дата
Инев. № подл.	Подпись и дата	Взам. инв. №	Инев. № дубл.	Подпись и дата

При работе за компьютером ночью (с 22 до 6 часов) продолжительность регламентированных перерывов следует увеличить на 30% (п. 1.6 Приложения № 7 к СанПиН 2.2.2/2.4.1340-03).

Также время работы за компьютером регулировал такой документ, как Типовая инструкция по охране труда при работе на персональном компьютере (ТОИ Р-45-084-01, утв. Приказом Минсвязи РФ от 02.07.2001 N 162). В ней сказано, что время непрерывной работы за компьютером без регламентированного перерыва не может превышать 2 часов (п. 3.2 ТОИ Р-45-084-01).

Эта инструкция с 01.01.2021 г. утратила силу.

То есть с 2021 г. вопрос установления перерывов во время работы за компьютеры нормативно не урегулирован. Работодатель может самостоятельно установить порядок предоставления перерывов в работе за компьютером для отдыха в правилах внутреннего трудового распорядка. Важно помнить, что указанные перерывы включаются в рабочее время. То есть они не продлевают продолжительность рабочего дня сотрудника. Во время этих перерывов работник не должен выполнять другую работу. Перерыв предоставляется ему для отдыха (Письмо Минтруда от 14.06.2017 № 14-2/ООГ-4765).

Кроме того, важно помнить, что перерывы в работе для отдыха от компьютера нужно предоставлять отдельно от перерыва на обед (ст. 108, 109 ТК РФ).

4.5 Экологические проблемы утилизации электронных гаджетов.

Устаревшие персональные компьютеры или их элементы должны быть правильно утилизированы в целях предотвращения вредного воздействия отходов производства и потребления на здоровье человека и окружающую среду, а также вовлечения таких отходов в хозяйственный оборот в качестве дополнительных источников сырья. За несоблюдение законодательства России по утилизации офисной техники на организацию могут быть наложены штрафные санкции. Выбрасывание компьютерной техники ведет к загрязнению окружающей среды. Персональный

Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист		
							ИИВТ.10.05.02.066	
								ИИВТ.10.05.02.066
Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	47		

компьютер включает в свой состав как органические составляющие (пластик различных видов, материалы на основе поливинилхлорида, фенол формальдегида), так и почти полный набор металлов, в том числе и драгоценных. В связи с этим организации требуется документально контролировать оборот средств компьютерной техники от поступления до выбытия. Согласно Приказу ГТК РФ от 19.11.2002 N 1224 «О порядке учета и хранения изделий и материалов, изготовленных с применением драгоценных металлов и драгоценных камней», организация вправе:

- самостоятельно обрабатывать (перерабатывать) собранный лом, содержащий драгоценные металлы;
- реализовывать лом, содержащий драгоценные металлы;
- передавать на давальческой основе аффинажным организациям или организациям, осуществляющим деятельность по заготовке лома и отходов, первичной обработке и переработке, для дальнейшего производства и аффинажа.

Процесс утилизации компьютерной техники включает следующие пункты:

- создание внутренней комиссии в организации, которая решит, что нужно списать;
- составление экспертного заключения и подтверждение невозможности дальше пользоваться компьютерным оборудованием;
- осуществление списания компьютерной техники, которое будет отражено в бухгалтерском учете;
- утилизация мусора на лицензированном предприятии и получение документального подтверждения о проведенных действиях (акт выполненной работы, приема-передачи).
- утилизация персональных компьютеров имеет определенные сложности в реализации, но это необходимый этап в поддержании экологической ситуации. [9]

Инов. № подл.	Подпись и дата
Взам. инв. №	Инов. № дубл.
Подпись и дата	
Инов. № подл.	

Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист 48

4.6 Вывод

В данном разделе были описаны особенности воздействия электронных систем на здоровье пользователей, выдвинуты эргономические требования к системам отображения информации в соответствии с нормативными документами. Выяснили, что в данный момент режимы труда и отдыха при работе с электронными устройствами нормативно не урегулирован. Проанализировали экологические проблемы утилизации электронных гаджетов.

5 Технико-экономическое обоснование работы

5.1 Постановка задачи

Целью выпускной квалификационной работы являлась разработка веб-приложения для защищенного электронного голосования. Веб-приложение является программным кодом, который, согласно ст. 1259 ГК РФ, относится к объектам авторских прав, таким образом, является интеллектуальной собственностью.

В данном разделе будут рассмотрены следующие вопросы:

- расчет трудоемкости и длительности работ;
- расчет себестоимости и цены программного продукта;
- эффект от разработки программного продукта;
- конкурентоспособность продукта.

5.2 Расчет трудоемкости и длительности работ

В первую очередь необходимо составить план по разработке программного продукта, который представлен в таблице 5.1.

Подпись и дата						
Инв. № дубл.						
Взам. инв. №						
Подпись и дата						
Инв. № подл.						
Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						49

Таблица 5.1 – План разработки программного продукта

Наименование этапов	Виды работ	Исполнитель	Количество исполнителей
Анализ предметной области	Определение объекта разработки	Студент	1
	Анализ основных угроз и уязвимостей	Студент	1
	Разработка модели нарушителя информационной безопасности	Студент	1
Проектирование	Проработка концепции	Студент	1
	Выбор протокола голосования	Студент	1
	Планирование архитектуры приложения	Студент	1
Разработка	Разработка сервера авторизации	Студент	1
	Разработка сервера учета голосов	Студент	1
	Разработка системы аудита	Студент	1
Тестирование	Тестирование работоспособности	Студент	1
	Тестирование защищенности	Студент	1
Внедрение	Улучшение, оптимизация, устранение ошибок	Студент	1

Далее требуется рассчитать трудоемкость и длительность работ. Поскольку трудоемкость этапов и видов работ носит вероятностный характер, то предпочтительным будет использование метода экспертных оценок.

Изм.	Лист	№ докум.	Подпись	Дата
Инва. № подл.	Подпись и дата	Взаим. инв. №	Инва. № дубл.	Подпись и дата

ИИБТ.10.05.02.066

В этом методе для каждого этапа требуется экспертным путем определить три оценки трудоемкости, в днях:

Далее для каждого из этапов определены три величины:

- наименее возможная величина затрат, a_i ;
- наиболее вероятная величина затрат, m_i ;
- наиболее возможная величина затрат, b_i .

На основании экспертных оценок средняя величина для a_i , m_i и b_i определяется по формуле (5.1):

$$\bar{T} = \frac{3T_{\text{рук}} + 2T_{\text{авт}}}{5}, \quad (5.1)$$

где \bar{T} – среднее время, полученное на основании экспертных оценок;

$T_{\text{рук}}$ – оценка затрат времени, данная руководителем;

$T_{\text{авт}}$ – оценка затрат времени, данная автором проекта.

Результаты расчета средней оценки затрат времени на разработку программного продукта приведены в таблице 5.2 (оценка производится в днях).

Таблица 5.2 – Время, затраченное на разработку программного продукта

Этапы разработки программного продукта	Наименее возможная величина затрат (a_i), дни			Наиболее вероятная величина затрат (m_i), дни			Наиболее возможная величина затрат (b_i), дни		
	$T_{\text{авт}}$	$T_{\text{рук}}$	\bar{T}	$T_{\text{авт}}$	$T_{\text{рук}}$	\bar{T}	$T_{\text{авт}}$	$T_{\text{рук}}$	\bar{T}
1 Анализ предметной области	2	2	2	3	4	3,6	5	6	5,6
2 Проектирование	2	3	2,6	3	5	4,2	4	6	5,2
3 Разработка	4	5	4,6	5	6	5,6	7	7	7
4 Тестирование	1	1	1	2	3	2,6	4	5	4,5
5 Внедрение	2	3	2,6	3	4	3,6	5	5	5

Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист	51
Изм.	Лист	№ докум.	Подпись	Дата			

На основе средних оценок рассчитываются математическое ожидание и отклонение по каждому этапу разработки программного продукта. Формула расчета математического ожидания для i-го этапа:

$$MO_i = \frac{a_i + 4m_i + b_i}{6}, \quad (5.2)$$

где MO_i – математическое ожидание для i-го этапа;

a_i, m_i, b_i – средние значения.

Стандартное отклонение для каждого этапа разработки программного продукта определяется по формуле:

$$G_i = \frac{b_i - a_i}{6}, \quad (5.3)$$

где G_i – стандартное отклонение по i-му этапу.

Зная математическое ожидание по каждому этапу, рассчитывается общая величина математического ожидания в целом по программному средству:

$$MO = \sum MO_i, \quad (5.4)$$

где MO – общая величина математического ожидания.

Стандартное отклонение G в целом по программному средству рассчитывается по следующей формуле:

$$G = \sqrt{\sum G_i^2}, \quad (5.5)$$

где G – стандартное отклонение;

G_i – стандартное отклонение по i-му этапу.

На основе расчетов математического ожидания (5.2) и стандартного отклонения (5.3) рассчитывается коэффициент вариации – коэффициент согласованности мнения экспертов. Коэффициент вариации рассчитывается по формуле:

$$v_i = \frac{G_i}{MO_i}, \quad (5.6)$$

где v_i – коэффициент вариации по i-му этапу.

Инов. № подл.	Подпись и дата
Взаим. инв. №	Инов. № дубл.
Подпись и дата	
Инов. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата	ИИБТ.10.05.02.066	Лист
						52

Теперь можно произвести расчеты на основе таблицы 5.3 и формул (5.2 – 5.6) и свести эти расчеты в таблицу 5.3.

Таблица 5.3 – Затраты на разработку программного продукта

Этапы разработки программного продукта	Средняя величина затрат по этапам, дни			Матем. ожидание (MO_i , дни)	Станд. Отклонение (G_i , дни)	Коэффициент вариации (v_i)
	Наименее возможная величина затрат (a_i , дни)	Наиболее вероятная величина затрат (m_i , дни)	Наиболее возможная величина затрат (b_i , дни)			
1 Анализ предметной области	2	3,6	5,6	3,67	0,6	0,16
2 Проектирование	2,6	4,2	5,2	4,1	0,43	0,1
3 Разработка	4,9	5,6	7	5,72	0,35	0,06
4 Тестирование	1	2,6	4,5	2,65	0,58	0,22
5 Внедрение	2,6	3,6	5	3,67	0,4	0,11
Итого	13,1	19,6	27,3	19,81	1,08	0,13

Коэффициент вариации равен 0,13 и не превосходит **0,33**. Поэтому мнения экспертов считают согласованными.

5.3 Расчет себестоимости программного продукта

Себестоимость программного продукта – это все виды затрат, понесённые при разработке продукта. Себестоимость включает в себя:

- затраты на материалы;
- трудовые затраты;
- амортизацию основных средств;

Инов. № подл.	Подпись и дата	Взаим. инв. №	Инов. № дубл.	Подпись и дата

Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						53

– прочие (накладные расходы, затраты сторонних организаций и т.д.).

Чтобы определить себестоимость разработки программного продукта применяется метод экспертных оценок. Данный метод заключается в следующем: оценка затрат производится несколькими экспертами на основании собственного опыта и знаний. В данном случае в качестве экспертов выступают автор проекта и руководитель. Использование данного метода оправдано, так как процесс написания программы является творческим и поэтому сложно ввести нормативы для оценки затрат.

Себестоимость программного продукта определяется по формуле

$$C = \frac{3}{m} \cdot k \cdot k_{\text{ТЕР}} \cdot k_{\text{ПР}} \cdot (t_1 + t_2 + t_3 + t_4) \cdot (1 + k_n) + 8 \cdot t_3 \cdot C_m + 8 \cdot t_4 \cdot C_{\text{и}},$$

(5.7)

где 3 - среднемесячная заработная плата разработчика программы = 40000;

$k_{\text{ТЕР}}$ - территориальный коэффициент, $k_{\text{ТЕР}} = 1,2$ (для НСО);

$k_{\text{ПР}}$ - коэффициент премии $k_{\text{ПР}} = 1$;

k - коэффициент, учитывающий страховые взносы (фонды пенсионного, социального и медицинского страхования), $k = 1,3$

m - количество рабочих дней в месяце, $m = 22$;

K_n - коэффициент, учитывающий накладные расходы (отопление, освещение, уборка и т. д.), $K_n = 0,4$;

t_1 - время, затраченное разработчиком на разработку требований к программе, т.е. подготовительное время, которое необходимо потратить, чтобы приступить к написанию программы и отладки программы, чел./дни;

t_2 - сборка устройства, составление алгоритма в программе, время, затраченное на написание и отладку программы, чел./дни;

t_3 - время, затраченное на разработку программы с использованием машинного времени, чел./дни;

t_4 - время работы в сети интернет, дни;

Инов. № подл.	Подпись и дата
Взам. инв. №	Инов. № дубл.
Подпись и дата	
Инов. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						54

$C_{и}$ - стоимость 1 часа работы в сети интернет, руб. Стоимость работы в сети Internet оценивается по входящему трафику (количество мегабайт информации, либо через абонентскую плату).

C_m - стоимость одного часа машинного времени.

δ – количество рабочих часов в день.

Для расчета стоимости одного часа машинного времени необходимо определить затраты на эксплуатацию ПК за год.

$$C_m = \frac{Z_{эл} + Z_a + Z_{компл} + Z_{пр}}{T_{общ}}, \quad (5.8)$$

где C_m – стоимость одного часа машинного времени;

$T_{общ}$ – общее время работы компьютера в год;

$Z_{эл}$ – затраты на электроэнергию за год работы;

Z_a – амортизационные отчисления;

$Z_{компл}$ – затраты на комплектующие материалы;

$Z_{пр}$ – прочие расходы.

Общее время работы компьютера за год составляет:

$$T_{общ} = 22 * 12 * 8 = 2112 \text{ часов.}$$

Затраты на электроэнергию за год работы (на данный момент тариф $C_{эл}$ составляет 2,49 руб. за кВт-ч):

$$Z_{эл} = T_{общ} * C_{эл} * P \quad (5.9)$$

где P - потребляемая мощность компьютера по паспортным данным в час, в среднем P составляет: 450 Вт*ч.

По формуле (5.9) затраты на электроэнергию за год работы составляют:

$$Z_{эл} = 2112 * 2,49 * 0,45 = 2366,5 \text{ руб.}$$

Амортизационные отчисления в год определяются как процент отчисления на амортизацию от первоначальной стоимости основных производственных фондов. Процент отчисления на амортизацию (P_p) согласно статье 258 НК РФ составляет 34-50% от первоначальной стоимости ПК (компьютер относится ко второй

Инов. № подл.	Подпись и дата	Взам. инв. №	Инов. № дубл.	Подпись и дата						
Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066					Лист
										55

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

Цена с учетом налога на добавленную стоимость находится по формуле (5.13):

$$\mathbb{C}_{\text{HDS}} = \mathbb{C} \cdot \mathbb{K}_{\text{HDS}}, \quad (5.13)$$

где C – цена программного продукта;

$K_{\text{НДС}}$ – коэффициент, учитывающий ставку налога на добавленную стоимость (НДС), $K_{\text{НДС}} = 1,20$.

Цена с учетом налога на добавленную стоимость составит:

$$\Pi_{\text{ндс}} = 101955,48 * 1,20 = 122346,56 \text{ руб.}$$

5.5 Определение эффекта от разработки программного продукта

Эффект характеризуется экономией рабочего времени при использовании программного продукта. При использовании данной программы автоматизируются стандартные и повседневные операции, что позволяет экономить денежные средства и сокращать время для решения повседневных задач.

Использование электронной системы для голосования даст эффект, как для конечного пользователя, так и для организатора голосования.

Рассмотрим положительные и отрицательные стороны. Для клиентов эффектом будет экономия времени. Появляется возможность проголосовать без непосредственного выезда на место проведения. При выполнении голосования в бумажном виде. Необходимо подготовить место голосования, бюллетени, выдать бюллетени подсчитать их. С авторской программой большинство действий полностью автоматизировано и не требует участия человека.

Подпись и дата	Инв. № дубл.	Взаим. инв. №	Подпись и дата	Инв. № подл.	<p>Эффект характеризуется экономией рабочего времени при использовании программного продукта. При использовании данной программы автоматизируются стандартные и повседневные операции, что позволяет экономить денежные средства и сокращать время для решения повседневных задач.</p> <p>Использование электронной системы для голосования даст эффект, как для конечного пользователя, так и для организатора голосования.</p> <p>Рассмотрим положительные и отрицательные стороны. Для клиентов эффектом будет экономия времени. Появляется возможность проголосовать без непосредственного выезда на место проведения. При выполнении голосования в бумажном виде. Необходимо подготовить место голосования, бюллетени, выдать бюллетени подсчитать их. С авторской программой большинство действий полностью автоматизировано и не требует участия человека.</p>	<p>ИИВТ.10.05.02.066</p>	Лист
							58
Изм.	Лист	№ докум.	Подпись	Дата			

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

Шаг	Описание процессов	Время, час.
1	Составление списка голосующих	1
2	Организация места проведения	1
3	Выдача бюллетеней для голосования	0,5
4	Подсчет результатов голосования	1
5	Уведомление о результатах голосования	0,5
	Итого	4

Таблица 5.5 - Оценка затрат времени на выполнение алгоритма работы голосования после внедрения автоматизированного программного средства

Шаг	Описание	Время, час.
1	Составление списка голосующих	0,5
2	Организация места проведения	0
3	Выдача бюллетеня для голосования	0
4	Подсчет результатов голосования	0
5	Уведомление о результатах голосования	0
	Итого	0,5

Экономия времени при проведении одного голосования

$$\Delta T_1 = 3,5 \text{ ч.}$$

Определим общую экономию времени:

$$\Delta T_{\text{общ}} = \Delta T_1 \cdot n, \quad (5.14)$$

где ΔT_1 – экономия времени при проведении одного голосования;

n – среднее количество голосований за день.

Метод наблюдения позволил определить среднее количество голосований за день: 5 ед. Соответственно экономия времени за день составляет:

$$\Delta T = 3,5 \cdot 5 = 17,5 \text{ ч.}$$

Общая экономия времени за месяц составляет:

$$\Delta T_{\text{общ}} = 17,5 \cdot 24 = 420 \text{ ч.}$$

По формуле (3.2) определим условную экономию численности персонала:

$$\Delta \chi_{\text{усл}} = \frac{420 \cdot 12}{1970} \cdot 1,08 = 2,76,$$

По формуле (3.3) находим годовую экономию по оплате труда с учетом страховых взносов:

$$\Delta \mathcal{E}_{\text{от}} = 2,76 \cdot 35000 \cdot 12 \cdot 1,30 \cdot 1,2 = 1808352 \text{ руб.}$$

Таким образом, при использовании разрабатываемого программного продукта, на производстве происходит условная экономия численности персонала, равная 2,76 шт.ед., а также условная экономия денежных средств в размере 1808352 рублей в год. Использование данного программного средства позволяет значительно повысить эффективность проведение голосования.

5.6 Оценка конкурентоспособности программного продукта

После расчета себестоимости и цены программного продукта, необходимо проанализировать рынок конкурентов по данному направлению и выявить конкурентные преимущества авторского продукта.

Инов. № подл.	Подпись и дата	Инов. № дубл.	Взаим. инв. №	Инов. № дубл.	Подпись и дата	Инов. № подл.
Изм.	Лис	№ докум.	Подпись	Дата	ИИБТ.10.05.02.066	
					Лист	
					60	

Анализ рыночной ситуации показал, что на рынке имеется 3 аналога авторского приложения.

Аналогами являются программные продукты:

- дистанционное электронное голосование ЦИК РФ;
- E-voting;
- ВТБ регистратор.

С помощью методики анализа потребительских характеристик товаров (услуг) проведем сравнительный анализ авторского приложения с его аналогами и занесем результаты в таблицу 5.5.

В качестве параметров, оказывающих влияние на уровень конкурентоспособности продукции, были выделены следующие:

- доступ к приложению с любого компьютера, имеющего выход в сеть интернет;
- тайна голосования;
- сокрытие результатов до окончания голосования;
- аудит хода голосования;
- данные авторизации и результаты голосования отделены друг от друга;
- Возможность подключения различных способов авторизации;
- голосующий может удостовериться в том, что его голос был учтен верно.

Цену приложения как параметр не используем, потому что голосование от ЦИК РФ является бесплатным для пользователей, и авторское приложение может быть использовано так же и для государственных выборов.

Инв. № подл.	Подпись и дата				ИИВТ.10.05.02.066	Лист 61
	Инв. № дубл.					
	Взаим. инв. №					
	Подпись и дата					
Изм.	Лист	№ докум.	Подпись	Дата		

Таблица 5.6 – Сравнительная характеристика аналогов

№	Параметры сравнения	Программы			
		Авторское приложение	ДЕГ ЦИК РФ	E-voting	ВТБ регистратор
1	Доступ к приложению с любого компьютера, имеющего выход в сеть интернет	+	+	+	+
2	Тайна голосования	+	+	+	+
3	Соккрытие результатов до окончания голосования	+	+	-	-
4	Аудит хода голосования	+	+	+	+
5	Данные авторизации и результаты голосования отделены друг от друга	+	-	-	-
6	Возможность подключения различных способов авторизации	+	-	-	-
7	Голосующий может удостовериться в том, что его голос был учтен верно	+	-	-	-

5.7 Выводы по разделу

В данном разделе определили, что разработка данного программного продукта займет около 20 дней, по себестоимости 84962,9 руб. С учетом налога на добавленную стоимость цена составит 122346,56 руб.

Инов. № подл.	Подпись и дата	Взаим. инв. №	Инов. № дубл.	Подпись и дата

Изм.	Лис	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						62

При использовании разрабатываемого программного продукта происходит условная экономия денежных средств в размере 1808352 рублей в год.

Так же выяснили, что продукт конкурентоспособен. Продукт имеет те же параметры, что и у конкурентов, а также обладает параметрами, которых у конкурентов – нет.

В связи с этим делаем вывод, что разработка данного программного продукта является экономически обоснованным.

Инв. № подл.	Подпись и дата				<div>ИИВТ.10.05.02.066</div> <div>Лист 63</div>
	Инв. № дубл.				
	Взаим. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	

Заключение

В результате выполнения выпускной квалификационной работы была достигнута поставленная цель и ее задачи.

В первой главе был определен объект разработки, определены требования к ДЭГ, спрогнозированы угрозы и уязвимости разрабатываемой системы и рассмотрены способы их предотвращения. Также была разработана модель потенциального нарушителя информационной безопасности веб-приложения для электронного голосования.

В второй главе были проработаны технические решения для разработки системы дистанционного электронного голосования. Для реализации системы дистанционного электронного голосования выберем протокол Sensus.

В третьей главе была разработана система дистанционного электронного голосования. Система голосования представляет собой сервер регистратор, сервер учета голосов, систему аудита и клиентское приложение.

В четвертой главе были проработаны вопросы безопасности жизнедеятельности

В пятой главе было выполнено технико-экономическое обоснование и сделан вывод, что разработка данного программного продукта является экономически обоснованным.

Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						64

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

- | | | | | | |
|-------------|-------------|-----------------|----------------|-------------|--------------------------|
| | | | | | <i>ИИВТ.10.05.02.066</i> |
| | | | | | |
| <i>Изм.</i> | <i>Лист</i> | <i>№ докум.</i> | <i>Подпись</i> | <i>Дата</i> | |

client.py

```
from tkinter import *
import tkinter.messagebox as tm
from source.auth.auth import auth

CANDIDATES = {
    1: 'Вариант 1',
    2: 'Вариант 2',
    3: 'Вариант 3',
    4: 'Вариант 4',
}

class LoginFrame(Frame):
    def __init__(self, master):
        super().__init__(master)
        self.label_username = Label(self, text="Логин")
        self.label_password = Label(self, text="Пароль")
        self.entry_username = Entry(self)
        self.entry_password = Entry(self, show="*")
        self.label_username.grid(row=0, sticky=E)
        self.label_password.grid(row=1, sticky=E)
        self.entry_username.grid(row=0, column=1)
        self.entry_password.grid(row=1, column=1)
        self.login_btn = Button(self, text="Войти", command=self.btn_clicked)
        self.login_btn.grid(columnspan=2)
        self.pack()

    def btn_clicked(self):
        username = self.entry_username.get()
        password = self.entry_password.get()
```

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата	<pre> self.label_password = Label(self, text="Пароль") self.entry_username = Entry(self) self.entry_password = Entry(self, show="*") self.label_username.grid(row=0, sticky=E) self.label_password.grid(row=1, sticky=E) self.entry_username.grid(row=0, column=1) self.entry_password.grid(row=1, column=1) self.login_btn = Button(self, text="Войти", command=self.btn_clicked) self.login_btn.grid(columnspan=2) self.pack() def btn_clicked(self): username = self.entry_username.get() password = self.entry_password.get() </pre>
					<div>ИИВТ.10.05.02.066</div> <div>67</div>
Изм.	Лист	№ докум.	Подпись	Дата	

```

if not username or not password:
    tm.showerror('Ошибка', 'Неверный логин или пароль!')

```

```

user = auth(username, password)
if not user:
    tm.showerror('Ошибка', 'Неверный логин или пароль!')

```

```

self.destroy()
ChoiceCandidate(self.master, user)

```

```

class ChoiceCandidate:

```

```

    def __init__(self, master, user=None):
        self.master = master
        self.var = IntVar()
        self.frame = LabelFrame(master, text=f'Привет {user["login"]}, сделай свой вы-
бор!', padx=50)
        self.frame.pack()
        for id_candidate, candidate in CANDIDATES.items():
            Radiobutton(self.frame, text=candidate, variable=self.var, value=id_candi-
date).pack(anchor=W)

        self.btn = Button(master, text='Голосовать', padx=20, pady=5, com-
mand=self.btn_clicked)
        self.btn.pack(pady=10)

    def btn_clicked(self):
        value = self.var.get()
        print(value)

```

Инва. № подл.	Подпись и дата	Взам. инв. №	Инва. № дубл.	Подпись и дата					
Изм.	Лист	№ докум.	Подпись	Дата	ИИБТ.10.05.02.066				
					Лист				
					68				

```

if value:
    self.frame.destroy()
    self.btn.destroy()
    ResultVote(self.master, value)
else:
    tm.showerror('Ошибка', 'Пожалуйста, выберите один из предложенных ва-
риантов')

class ResultVote:
    def __init__(self, master, id_candidate=None):
        self.var = IntVar()
        self.label = Label(master, text=f'Голос за кандидата "{CANDIDATES[id_candi-
date]}" учтен!')
        self.label.grid(row=0, sticky=E)
        self.label.pack()

```

```

root = Tk()
root.title('Дистанционное электронное голосование')
root.geometry('400x230')
lf = LoginFrame(root)
root.mainloop()

```

Инва. № подл.	Подпись и дата	Взаим. инв. №	Инва. № дубл.	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066					Лист
										69

db.py

```
import psychpg2
```

```
import psychpg2.extras
```

```
def connect():
```

```
conn = psycopg2.connect(dbname='registrator', user='raldenprog',  
                        password='Nedlar_proG', host='localhost')
```

```
return conn, conn.cursor(cursor_factory=psycopg2.extras.DictCursor)
```

```
def select(sql: str):
```

```
conn, cursor = connect()
```

```
cursor.execute(sql)
```

```
return cursor.fetchall()
```

```
def select_one(sql: str):
```

```
conn, cursor = connect()
```

```
cursor.execute(sql)
```

```
return cursor.fetchone()
```

```
def insert(sql: str):
```

```
conn, cursor = connect()
```

```
cursor.execute(sql)
```

```
conn.commit()
```

Подпись и дата			conn, cursor = connect() cursor.execute(sql) return cursor.fetchall()
Инв. № дубл.			def select_one(sql: str): conn, cursor = connect() cursor.execute(sql) return cursor.fetchone()
Взаим. инв. №			
Подпись и дата			def insert(sql: str): conn, cursor = connect() cursor.execute(sql) conn.commit()
Инв. № подл.			

Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066	Лист
						72

Инв. № подл.	Подпись и дата	Взаим. инв. №	Инв. № дубл.	Подпись и дата

mask.py

					<i>ИИВТ.10.05.02.066</i>
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>	

```
# user computes
```

```
msg_signature = pub.unblind(msg_blinded_signature[0], r)
```

```
# Someone verifies
```

```
hash = SHA256.new()
```

```
hash.update(msg)
```

```
msgDigest = hash.digest()
```

```
print("Message is authentic: " + str(pub.verify(msgDigest, (msg_signature,))))
```

					Подпись и дата		
					Инв. № дубл.		
					Взаим. инв. №		
					Подпись и дата		
					Инв. № подл.		
Изм.	Лист	№ докум.	Подпись	Дата	ИИВТ.10.05.02.066		Лист
							74

