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

Кафедра БиУТ

Допустить к защите зав. кафедрой

/С.Н. Новиков /

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА  
специалиста**

Разработка системы дистанционного электронного голосования

Пояснительная записка

Студент / А.А. Крылосов /

Факультет АЭС Группа АБ-66

Руководитель / Г.В. Попков /

Консультанты:

– по экономическому обоснованию

/ И.С. Мухина /

– по безопасности жизнедеятельности

/ Н.Н. Симакова /

Рецензент / /

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»

« 28 » июля 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 « 28 » июля 2021 г. № 4/1011о-21

2. Срок сдачи студентом законченной работы « 15 » января 2022 г.

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

Количество участников, нагрузка, конкуренты, сюда пишем то, что не можем или не хотим обосновать (когда будут докапываться

|  |  |
| --- | --- |
| 4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов) | Сроки выполнения по разделам |
| Введение | 13.09.2021 г. |
| 1. Анализ существующего состояния объекта проектирования | 11.10.2021 г. |
| 2. Разработка системы защиты информации | 08.11.2021 г. |
| 3. Выбор оборудования и программного обеспечения | 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. | Задание принял к исполнению  « 01 » сентября 2021 г. |
| / О.И. Солонская /  (подпись, Ф.И.О. руководителя) | / И.И. Иванов /  (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)

**рецензия**

на выпускную квалификационную работу студента А.А. Крылосова

по теме «Разработка системы дистанционного электронного голосования»

Доц. каф. ПМиК, к.т.н. Нечта Иван Васильевич

« 18 » января 2022 г.

С Рецензией ознакомлен /И.И. Иванов/

« 18 » января 2022 г.

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 |  | Тема предложена предприятием |  |
| Работа внедрена |  | Тема предложена студентом |  |
| Рекомендую работу к внедрению |  | Тема является фундаментальной |  |
| Рекомендую работу к опубликованию |  | Рекомендую студента в магистратуру |  |
| Работа выполнена с применением ЭВМ |  | Рекомендую студента в аспирантуру |  |

Руководитель выпускной квалификационной работы специалиста

Доц. каф. БиУТ, к.т.н. Солонская Оксана Игоревна

« 15 » января 2022 г.

С Отзывом ознакомлен /И.И. Иванов/

« 15 » января 2022 г.

Приложение к Отзыву

**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 – 121 страниц, на которых размещены 9рисунков и 15 таблиц. При написании работы использовалось 25источников.

Ключевые слова: система защиты информации, система контроля управления доступом, система видионаблюдения, антивирусная защита, политика безопасности, аутентификация.

Работа выполнена на: кафедре БиУТ СибГУТИ

Руководитель: доц. каф. БиУТ Солонская О.И.

Целью работы Разработка системы дистанционного электронного голосования

Решаемые задачи: анализ существующего состояния объекта проектирования, разработка системы защиты информации, выбор оборудования и программного обеспечения, безопасность жизнедеятельности, технико-экономическое обоснование работы

Основные результаты: модернизированная система защиты информации на предприятии

**Graduation thesis abstract**

of I.I.Ivanov on the theme Modernization of information security systems in the enterprise

The paper consists of 121 pages, with 9figures and 15tables/charts/diagrams. While writing the thesis 25 referencesources were used.

Keywords: information protection system, access control system, video surveillance system, antivirus protection, security policy, authentication

The thesis was written at BIUT department SibSUTIS

(name of organization or department)

Scientific supervisor associate professor of the BiUT Solonskaya Oxana

The goal/subject of the paper is modernize the information security system in the enterprise

Tasks: analysis of the existing state of the design object, development of an information protection system, selection of equipment and software, life safety, technical and economic justification of work

Results modernized information security system in the enterprise

Оглавление

[Введение 4](#_Toc87040308)

[1 Анализ предметной области 5](#_Toc87040309)

[1.1 Постановка задачи 5](#_Toc87040310)

[1.2 Определение объекта разработки 5](#_Toc87040311)

[1.3 Анализ требований ДЭГ 5](#_Toc87040312)

[1.5 Выводы по разделу 6](#_Toc87040313)

[2 Разработка концепции реализации модулей дистанционного электронного голосования 7](#_Toc87040314)

[2.1 Постановка задачи 7](#_Toc87040315)

[В рамках данной главы необходимо проанализировать угрозы и уязвимости, разработать модель нарушителя, выбрать из существующих протоколов тайного голосования или разработать собственный в соответствии с требованиями, поставленными в главе 1.3 7](#_Toc87040316)

[2.2 Анализ основных угроз и уязвимостей существующих веб-приложений 7](#_Toc87040317)

[2.3 Разработка модели нарушителя информационной безопасности 8](#_Toc87040318)

[2.1 Простой протокол тайного цифрового голосования 11](#_Toc87040319)

[TODO 11](#_Toc87040320)

[2.1 Протокол двух агентств. 11](#_Toc87040321)

[TODO 11](#_Toc87040322)

[2.1 Фудзиоки — Окамото — Оты 11](#_Toc87040323)

[TODO 11](#_Toc87040324)

[2.1 Sensus 11](#_Toc87040325)

[TODO 11](#_Toc87040326)

[2.1 Хэ — Су 11](#_Toc87040327)

[TODO 11](#_Toc87040328)

[2.1 ANDOS 11](#_Toc87040329)

[TODO 11](#_Toc87040330)

[2.1 Прочие протоколы 11](#_Toc87040331)

[TODO 11](#_Toc87040332)

[1.5 Выводы по разделу 11](#_Toc87040333)

[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. TODO БОЛЬШЕ ПРО ТО ПОЧЕМУ SENSUS 11](#_Toc87040334)

[2 Разработка концепции модулей дистанционного электронного голосования 12](#_Toc87040335)

[2.1 Постановка задачи 12](#_Toc87040336)

[2.2 Сервер регистратор 12](#_Toc87040337)

[2.4 Сервер подсчета голосов 13](#_Toc87040338)

[Сервер 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 списков бюллетеней. Расшифровывает бюллетени и производит подсчет голосов. 13](#_Toc87040339)

[2.5 Приложение голосующего. 13](#_Toc87040340)

[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. 13](#_Toc87040341)

[2.4 Аудит хода голосования 13](#_Toc87040342)

[2.5 Аудит результатов голосования 13](#_Toc87040343)

[2.7 Выводы по разделу 15](#_Toc87040344)

[3 Разработка системы дистанционного электронного голосования 16](#_Toc87040345)

[3.1 Постановка задачи 16](#_Toc87040346)

[3.2 Сервер аутентификации 16](#_Toc87040347)

[3.3 Сервер учета голосов 16](#_Toc87040348)

[3.4 Модуль Аудита 16](#_Toc87040349)

[3.5 Выводы по разделу 16](#_Toc87040350)

[4 Тестирование и оценка защищенности 17](#_Toc87040351)

[5 Технико-экономическое обоснование работы? 17](#_Toc87040352)

[6 БЖ? 17](#_Toc87040353)

[Заключение 17](#_Toc87040354)

[Список сокращений и условных обозначений 18](#_Toc87040355)

[Список литературы 19](#_Toc87040356)

# Введение

Говорим о том как сейчас важно разработать такую систему, пандемия, современные технологии позволяют.

К разработкам, в которых требование анонимности не просто обязательно, а является основополагающим, относятся системы электронного голосования. В настоящее время в некоторых странах есть опыт внедрения и использования подобных систем. Например, в Эстонии с осени 2005 года муниципальные выборы проводятся через Интернет [1, 29], в Казахстане система электронного голосования «Сайлау», закупленная в Белоруссии, впервые испытывалась на 10% избирательных участков на выборах депутатов в 2004-м году и с тех пор активно внедряется по всей республике [2]. Внедряемые в России врамках проекта «ГАС Выборы» двумерные считыватели заполненных бюллетеней КОИБ. автоматизируют лишь процедуру подсчета результатов по\* участку и» имеют высокую стоимость (около\* 70,0 тыс. руб.). В ряде регионов Л 2-го октября? 2008 года по> инициативе Тульской\* областной избирательной комиссии, поддержанной, центральной избирательной комиссией России, в порядке' эксперимента было пррведено электронное' голосование, для\*- которого использовались возможности сети Интернет [8]. Для тоге чтобьь принять участие в электронном голосовании, избирателю1 необходимо было получить специальный диск электронного опроса и воспользоваться любым компьютером« с выходом в интернет. Этой системой воспользовалось 5,4% от общего' количества граждан, принявших участие в выборах. Позже этот эксперимент был повторен 1 марта 2009 года в Вологодской, Волгоградской и Томской областях, а также 11 октября 2009 года в городе Кингисепп Ленинградской области. К возможности проголосовать с использованием диска электронного опроса добавились технологии голосования с использованием мобильного телефона и электронной социальной карты. Однако эти технологии не подходят, например, для выборов всероссийского масштаба, в первую очередь потому, что задачей экспериментов являлось, прежде всего, изучение отношения избирателей к новым формам голосования, и поэтому выполнение перечисленных выше требований было далеко не самым важным. Таким образом, в России нет разработанной и готовой для внедрения системы тайного электронного голосования, позволяющей осуществлять подачу голоса и его подсчет в электронном виде.

Поэтому исследования, направленные на создание системы тайного электронного голосования, являются весьма актуальными.

Так же упомянем [Московский опыт](https://habr.com/ru/company/analogbytes/blog/504328/)

# 1 Анализ предметной области

1.1 Постановка задачи

В данной главе необходимо определить объект разработки и описать его возможности. Произвести сравнительный анализ существующих систем голосования.

1.2 Определение объекта разработки

Под электронным голосованием понимают такое голосование, в котором используются электронные средства, помогающие или обеспечивающие подачу и подсчет голосов. [11]

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. [5]

1.3 Анализ требований ДЭГ

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); статья 17

– 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)

Также, как электронная система, она должна быть:

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

1.5 Выводы по разделу

В первом разделе был определен объект разработки, определены требования к ДЭГ.

# 2 Разработка концепции реализации модулей дистанционного электронного голосования

# 2.1 Постановка задачи

# В рамках данной главы необходимо разработать модели потенциальных угроз и нарушителя, на основе которых будет строиться система защиты разрабатываемого веб-приложения. Так же выбрать из существующих протоколов тайного голосования или разработать собственный в соответствии с требованиями, поставленными в главе 1.3

2.2 Анализ основных угроз и уязвимостей существующих веб-приложений

Согласно ГОСТ Р 50922-2006, угрозой безопасности информации является совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Уязвимость же является свойством информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации. [8]

Все источники угроз безопасности информации можно разделить на три основные группы:

1) обусловленные действиями субъекта (антропогенные источники угроз);

2) обусловленные техническими средствами (техногенные источники угрозы);

3) обусловленные стихийными источниками. [7]

Наибольший интерес с точки зрения организации защиты представляют антропогенные источники угроз безопасности информации, так как в роли таких источников выступают субъекты, действия которых всегда можно оценить, спрогнозировать и принять адекватные меры.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации, могут быть:

– внешние;

– внутренние. [7]

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации.

Внутренние субъекты, как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети.

Уязвимости безопасности информации могут быть:

– объективными;

– субъективными;

– случайными.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации.

Субъективные уязвимости зависят от действий сотрудников и, в основном устраняются организационными и программно-аппаратными методами.

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию, угрозам информационной безопасности. [7]

Следует рассмотреть угрозы и уязвимости, отталкиваясь от особенностей разрабатываемого веб-приложения.

TODO нужно больше про уязвимости

2.3 Разработка модели нарушителя информационной безопасности

Согласно ГОСТ Р 53114-2008, нарушителем информационной безопасности является физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности. [9]

В свою очередь, модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д.

Целью разработки модели нарушителя является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

С учетом наличия прав доступа и возможностей по доступу к информации и/или к компонентам информационной системы нарушители подразделяются на два типа:

1) внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

2) внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

– нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

– нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

– нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

Обратимся к банку данных угроз безопасности информации (УБИ), разработанный Федеральной службой по техническому и экспортному контролю России. В банке описаны угрозы и соответствующий им тип нарушителя и его минимально необходимый потенциал. Угрозы, которые можно отнести к разрабатываемому веб-приложению:

– угроза внедрения кода или данных (УБИ. 006);

– угроза восстановления и/или повторного использования аутентификационной информации (УБИ. 008);

– угроза доступа/перехвата/изменения HTTP cookies (УБИ. 017);

– угроза использования информации идентификации/аутентификации, заданной по умолчанию (УБИ. 030);

– угроза межсайтового скриптинга (УБИ. 041);

– 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).

Приведенным угрозам соответствуют следующие типы нарушителей и их минимально необходимый потенциал:

1) внешний нарушитель с низким потенциалом;

2) внутренний нарушитель с низким потенциалом;

3) внешний нарушитель со средним потенциалом.

Внешними нарушителями с низким потенциалом могут быть:

– внешние субъекты (физические лица);

– бывшие работники.

Внутренними нарушителями с низким потенциалом могут быть:

– лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора;

– пользователи;

– лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ.

Внешними нарушителями со средним потенциалом могут быть:

– преступные группы;

– конкуренты;

– разработчики, производители, поставщики программных, технических и программно-технических средств.

В таблице 1.3 приведена возможная мотивация рассмотренных выше нарушителей.





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

2.4 Сравнительный анализ существующих протоколов электронного голосования

Целью данной главы является выбор протокола голосования, который отвечает требованиям выставленный нами в предыдущей главе.

Протокол двух агентств.

TODO

Фудзиоки — Окамото — Оты

TODO

Sensus

TODO

Хэ — Су

TODO

ANDOS

TODO

Прочие протоколы

TODO

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. TODO БОЛЬШЕ ПРО ТО ПОЧЕМУ SENSUS

# 2 Разработка концепции модулей дистанционного электронного голосования

2.1 Постановка задачи

В рамках данной главы необходимо разработать модули 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 Сервер регистратор

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, соцопросы 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 отдают наружу собственно биометрические данные, а лишь подтверждают, что данное лицо является владельцем данного смартфона. Владелец 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.

Пользователю 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.

2.4 Сервер подсчета голосов

Сервер 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 списков бюллетеней. Расшифровывает бюллетени и производит подсчет голосов.

2.5 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.

2.4 Аудит хода голосования

В ходе голосования наблюдатели получают реплику 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.

2.5 Аудит результатов голосования

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.

2.7 Выводы по разделу

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

TODO Сформулировать конкретные тех. решения исходя из всей главы

# 

# 3 Разработка системы дистанционного электронного голосования

3.1 Постановка задачи

TODO Ставим задачу на разработку исходя из тех решения раздела 2

3.2 Сервер аутентификации

TODO Разрабатываем сервер аутентификации

3.3 Сервер учета голосов

TODO Разрабатываем сервер учета голосов

3.4 Модуль Аудита

TODO Разрабатываем функционал аудита

3.5 Выводы по разделу

TODO Делаем выводы по реализованной системе

# 

# 4 Тестирование и оценка защищенности

# 5 Технико-экономическое обоснование работы?

Интелектуальная собственность

# 6 БЖ?

Работа за компом

# Заключение

TODO Делаем заключение

TODO в первой главе подробно описываем плюсы минусы других решений

И в заключении говорим что мы все поправили и сделали круче

# Список сокращений и условных обозначений

|  |  |
| --- | --- |
| ДЭГ | Дистанционное электронное голосование |

# Список литературы

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. – М.: Госстандарт России, 1996. – 17 с.
2. Гольдштейн, Б.С. Сети связи: учебник / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. – СПб.: БХВ-Петербург, 2010. – 399с.
3. Роговский, Е.А. Кибербезопасность: экономические риски и эффективность / Е.А. Роговский, М.Е. Соколова // США – Канада: экономика, политика, культура. – 2008. – № 4. – С. 83-91.
4. Никитович, Н. Онлайн-банкинг: защиты много не бывает / Н. Никитович // Information Security/ Информационная безопасность – 2012. –№ 5. – URL: http://www.itsec.ru/articles2/Inf\_security/onlayn-banking-zaschity-mnogo-ne-byvaet/ (дата обращения: 12.