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 / А.А. Буров /

Консультанты:

– по экономическому обоснованию

/ /

– по безопасности жизнедеятельности

/ /

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):

|  |  |
| --- | --- |
| 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](#_Toc71840236)

[1 Анализ дистанционного электронного голосования 5](#_Toc71840237)

[1.1 Постановка задачи 5](#_Toc71840238)

[1.2 Определение объекта разработки 5](#_Toc71840239)

[1.3 Анализ требований ДЭГ 5](#_Toc71840240)

[1.4 Анализ основных угроз и уязвимостей веб-приложения 6](#_Toc71840241)

[1.4 Разработка модели нарушителя информационной безопасности 8](#_Toc71840242)

[1.5 Выводы по разделу 13](#_Toc71840243)

[2 Проработка ТЗ 14](#_Toc71840244)

[2.1 Постановка задачи 14](#_Toc71840245)

[2.2 Тайна голосования 14](#_Toc71840246)

[2.3 Аутентификация пользователя 16](#_Toc71840247)

[2.4 Аудит хода голосования 17](#_Toc71840248)

[2.5 Аудит результатов голосования 18](#_Toc71840249)

[2.6 Голосование под давлением 19](#_Toc71840250)

[2.7 Выводы по разделу 19](#_Toc71840251)

[3 Разработка системы дистанционного электронного голосования 21](#_Toc71840252)

[3.1 Постановка задачи 21](#_Toc71840253)

[3.2 Сервер аутентификации 21](#_Toc71840254)

[3.3 Сервер учета голосов 21](#_Toc71840255)

[3.4 Аудит голосования 21](#_Toc71840256)

[3.5 Выводы по разделу 21](#_Toc71840257)

[4 Тестирование и оценка защищенности 22](#_Toc71840258)

[5 Технико-экономическое обоснование работы? 22](#_Toc71840259)

[Заключение 22](#_Toc71840260)

[Список сокращений и условных обозначений 23](#_Toc71840261)

[Список литературы 24](#_Toc71840262)

[Приложение А Схема локальной сети предприятия 25](#_Toc71840263)

[Приложение Б План помещений предприятия 26](#_Toc71840264)

# Введение

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

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

# 1 Анализ дистанционного электронного голосования

1.1 Постановка задачи

В данной главе необходимо определить объект разработки и описать его возможности. А также разработать модели потенциальных угроз и нарушителя, на основе которых будет строиться система защиты разрабатываемого веб-приложения.

1.2 Определение объекта разработки

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

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.

1.3 Анализ требований ДЭГ

Классическое бумажное голосование обеспечивает нам, как минимум:

тайну голосования (разрыв между аутентификацией избирателя и фиксацией его голоса);

аудит списка избирателей (поимённый перечень проголосовавших);

аудит результатов голосования (возможность пересчёта бюллетеней);

сокрытие результатов до окончания голосования (невозможность определения исхода до окончания голосования).

Обязательные:

1. никто, кроме голосующего, не должен знать его выбор;
2. только [легитимные](https://ru.wikipedia.org/wiki/%D0%9B%D0%B5%D0%B3%D0%B8%D1%82%D0%B8%D0%BC%D0%BD%D0%BE%D1%81%D1%82%D1%8C) участники могут проголосовать, и притом только один раз;
3. решение голосующего не может быть тайно или явно кем-либо изменено (кроме, возможно, им самим).
4. аудит списка избирателей (поимённый перечень проголосовавших);
5. аудит результатов голосования (возможность пересчёта бюллетеней);
6. сокрытие результатов до окончания голосования (невозможность определения исхода до окончания голосования).

Желательные:

1. каждый легитимный участник может проверить, правильно ли зачтён его голос;
2. каждый легитимный участник может передумать и изменить свой выбор в течение определённого периода времени;
3. система должна быть защищена от продажи голосов избирателями;
4. в случае, если голос зачтён неправильно, каждый легитимный участник может сообщить об этом системе, не раскрывая своей анонимности;
5. невозможно отследить, откуда дистанционно проголосовал избиратель;
6. [аутентификация](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) оператора;
7. можно узнать, кто принимал участие в голосовании, а кто — нет;
8. поддержание системы не должно требовать много ресурсов;
9. система должна быть [отказоустойчива](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BA%D0%B0%D0%B7%D0%BE%D1%83%D1%81%D1%82%D0%BE%D0%B9%D1%87%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D1%8C) в случае технических неисправностей (потеря электропитания), непреднамеренных (потеря избирателем ключа) и злоумышленных (намеренная выдача себя за другого избирателя, [DoS](https://ru.wikipedia.org/wiki/DoS" \o "DoS)/[DDoS](https://ru.wikipedia.org/wiki/DDoS" \o "DDoS)) атак.

TODO Подробнее и более конструктивно со ссылками на источники

1.4 Анализ основных угроз и уязвимостей веб-приложения

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.

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.

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.

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.

Следует рассмотреть угрозы и уязвимости, отталкиваясь от особенностей разрабатываемого веб-приложения. В таблице 1.1 приведены особенности будущей системы и прогнозируемые угрозы и уязвимости.

TODO нужно больше про уязвимости

1.4 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.

1.5 Выводы по разделу

В первом разделе 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.

# 2 Проработка ТЗ

2.1 Постановка задачи

В рамках данной главы необходимо проработать решения в соответствии с требованиями поставленными в главе 1.3. 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 Тайна голосования

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

В абсолютном большинстве систем ДЭГ, внедрявшихся как властями, так и оппозицией, как в России, так и за её пределами, 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.

Единственным критичным требованием к реализации является наличие двух серверов, находящихся под управлением независимых друг от друга сил (это могут быть, например, две фракции или два комитета внутри партии, если речь о внутрипартийной системе).

**Cервер аутентификации пользователей** проверяет, может ли данный пользователь голосовать, и если да — генерирует две половинки ключа. Одна половинка отправляется на **сервер учёта голосов**, вторая передаётся избирателю на устройство, с которого он голосует.  
  
В момент отдачи голоса этот голос подписывается ключом избирателя и отправляется на сервер голосования, который сверяет ключи и учитывает голос. Сам факт наличия у избирателя его половинки ключа является подтверждением его права на голосование; знать личность избирателя сервер учёта голосов не знает и знать не может.  
  
В случае, если проводится открытое голосование, после получения голоса сервер учёта голосов отправляет информацию о нём на сервер аутентификации пользователей, который сопоставляет ключ с ФИО и публикует эту информацию в списке прошедших аутентификацию избирателей.  
  
В случае тайного голосования **сервер учёта голосов** только подтверждает серверу аутентификации факт свершившегося голосования.  
  
Важным нюансом в реализации такой схемы является учёт возможности атак по косвенным данным, в которые могут входить отпечаток устройства пользователя, IP-адрес пользователя и время голосования. При обеспечении независимости двух используемых серверов здесь критично лишь время голосования — можно сопоставить время аутентификации пользователя и время внесения в базу голоса; поэтому схема взаимодействия серверов и пользователей должна предусматривать разрушение этой связи в явном виде, как минимум, через добавление случайной задержки между аутентификацией и отправкой голоса со стороны устройства, используемого пользователем для голосования.  
  
В остальном же схема с двумя независимыми серверами — и только она! — позволяет реализовать тайну голосования в электронной форме.  
  
Схемы, в которых используется единый сервер, **доверенными в этом контексте считаться не могут по определению**; все заявления их авторов об отсутствии регистрации имён избирателей в связке с отданными ими голосами держатся исключительно на доверии к чистоплотности и аккуратности данных авторов (и все мы помним, что в IT-индустрии — тысячи примеров, когда автор сервиса не имел в виду ничего плохого, просто забыл в релизной сборке отключить отладочное логгирование).  
  
Корректно реализованная схема с независимыми серверами обеспечивает тайну голосования всегда, если владельцами обоих серверов не были сознательно предприняты меры к её устранению.

2.3 Аутентификация пользователя

Это — самая простая часть системы. 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 внутрипайртийные 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»; партиям недавно разрешили использовать её для праймериз и сбора подписей)  
  
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.

2.4 Аудит хода голосования

Одним из способов фальсификации результатов голосования являются вбросы «лишних» бюллетеней и так называемые «карусели».  
  
Влияние внешних сил в данной схеме может быть исключено проработкой системы аутентификации пользователей.  
  
Вместе с тем, даже при очень высокой надёжности системы аутентификации пользователей **владельцы сервера аутентификации могут начать генерировать «виртуалов»**, выдавая им ключи и отправляя их на сервер учёта голосов для голосования за нужный владельцам этих серверов пункт.  
  
Предотвратить это можно несколькими способами:  
  
выгрузкой с сервера аутентификации пользователей поимённого списка зарегистрировавшихся и проголосовавших избирателей, аналогичного бумажным спискам избирательной комиссии (ИК), на устройства наблюдателей и членов ИК;

анализом со стороны сервера учёта голосов аномалий в поведении пользователей (большое число пользователей с однотипных устройств, одинаковых IP-адресов, ненормальное распределение пользователей по времени голосования);

отсутствием возможности для наблюдателей или владельцев сервера аутентификации узнать текущее распределение голосов до окончания голосования.

Здесь мы впервые сталкиваемся с понятием «наблюдатель» — на дистанционных голосованиях наблюдатели также нужны, и нужны с той же целью, что на и голосованиях бумажных. Однако, в данном случае они контролируют происходящее не очно, а по выгрузке данных на их устройства с серверов аутентификации и учёта голосов.

2.5 Аудит результатов голосования

Наиболее важна роль наблюдателей в аудите результатов голосования. Очевидно, что **владельцы сервера учёта голосов потенциально могут просто подменить числа** перед их публикацией.  
  
Чтобы не допустить этого, в течение всего хода голосования на устройства наблюдателей регулярно реплицируется текущая база данных голосов (при желании как раз сюда можно прикрутить блокчейн — но в общем не обязательно). Чтобы не допустить утечек результатов раньше окончания голосования, база криптографически защищается.  
  
В момент окончания голосования и публикации его результатов ключ от базы 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).  
  
В этой же системе может решаться и задача недопущения **подмены голосов реальных пользователей** — возможна реализация так называемой аудируемой системы голосования, в которой пользователь может, использую индивидуальный криптографический ключ, проверить, за кого был засчитан его голос, при этом не раскрывая свою личность и не имея возможности проверить голоса других избирателей. Подчеркнём, что во многих статьях такой проверкой возможности аудита исчерпываются — это неверно, т.к. **личная проверка не исключает возможности вброса «мёртвых душ» или подмены итоговых результатов**.

2.6 Голосование под давлением

Типичной проблемой дистанционных, да и очных голосований является голосование под давлением — в ситуации, когда руководитель (например, директор предприятия) предписывает сотрудникам голосовать за конкретного кандидата, отчитываясь фотографиями бюллетеней.  
  
Что интересно, в случае с дистанционными голосованиями эта угроза может быть нивелирована **возможностью изменения голоса** в течение всего хода голосования. То есть, пользуясь выданным ему ключом, избиратель может проголосовать несколько раз — и учтён будет только последний отданный ему голос, что позволит продемонстрировать начальнику «правильное» голосование, а далее отдать голос уже за реально желаемого кандидата.  
  
Кроме того, постфактумное обнаружение массовых переголосованный (база данных фиксирует *все* голоса, последний отданный учитывается уже при подсчёте) может указывать на наличие явной проблемы и повод для начала расследования.

Распределённый характер системы (независимая работа двух серверов, устройств наблюдателей и устройств пользователей) обеспечивает защиту от таких примитивных и типовых приёмов, как подмена кода или запуск сторонних приложений, модифицирующих работу системы, уже после проверки её экспертами — попытки вмешательства лишь в один из компонентов системы могут нарушить его работу, но не могут незаметно для эксплуатантов остальных компонентов системы фальсифицировать данные.  
  
При модульном построении системы она позволит проводить голосования с разными способами аутентификации, тайные и открытые, с разным уровнем доверия — в зависимости от решаемых вопросов.

2.7 Выводы по разделу

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 Аудит голосования

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?

# Заключение

TODO Делаем заключение

# 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: 12.12.18).

Приложение А  
Схема локальной сети предприятия

На рисунке А.1 представлена подробная схема локальной сети предприятия, расположенного по адресу: ул. Кирова, 86.

Приложение Б  
План помещений предприятия