|  |  |
| --- | --- |
|  | **Российский государственный социальный университет** |

**Итоговое практическое задание № 1.**

**по дисциплине «Информационная безопасность»**

**на тему «Методы компьютерной стеганографии. LSB-метод»**

|  |  |
| --- | --- |
| **ФИО студента** | Салов Артём Владимирович |
| **Направление подготовки** | Программная инженерия |
| **Группа** | ПИН-Б-О-Д-2021-1 |

**Москва 2023**

Оглавление

[Введение. 3](#_Toc153726551)

[Стенография и LSB-метод. 4](#_Toc153726552)

[Что такое стеганография. 4](#_Toc153726553)

[LSB-метод. 5](#_Toc153726554)

[Плюсы и минусы LSB-метода. 5](#_Toc153726555)

[Способы стегоанализа и защиты от него. 6](#_Toc153726556)

[Способы стегоанализа. 6](#_Toc153726557)

[Способы защиты от стегоанализа. 7](#_Toc153726558)

[Заключение 8](#_Toc153726559)

# Введение.

В эпоху цифровых технологий, в которой информационный обмен стал неотъемлемой частью нашей повседневной жизни, вопросы безопасности данных приобретают особенное значение. Угрозы кибер-безопасности, перехват конфиденциальных данных и несанкционированный доступ к информации заставляют нас постоянно совершенствовать методы обеспечения безопасности. Одним из инновационных и недооцененных средств обеспечения конфиденциальности информации является компьютерная стеганография.

Методы компьютерной стеганографии предоставляют механизмы для незаметного внедрения информации в различные типы файлов, сохраняя при этом внешний вид носителя. Этот подход открывает новые перспективы для защиты конфиденциальности данных и обеспечения безопасности информационных потоков.

Цель данного доклада — более глубокое понимание LSB-метода в компьютерной стеганографии. Мы рассмотрим основные принципы этой техники, рассмотрим ее применение в различных сферах, а также обсудим потенциальные угрозы и методы обнаружения стеганографии. Проанализировав технические аспекты метода, мы сможем оценить его возможности и ограничения, а также более глубоко вникнуть в современные вопросы безопасности и защиты данных в цифровом мире.

# Стенография и LSB-метод.

## Что такое стеганография.

*Стеганография* — это область информационной безопасности, посвященная скрытой передаче данных с минимизацией заметности факта их существования. В отличие от криптографии, которая фокусируется на шифровании данных для защиты от несанкционированного доступа, стеганография стремится сохранить конфиденциальность, скрывая сам факт наличия информации.

Слово "стеганография" происходит от греческих слов "steganos" (скрытый) и "graphia" (письмо), что подчеркивает суть этой техники — скрытая передача информации. Основной задачей стеганографии является внедрение скрытого контента в носитель (например, изображение, аудиофайл или текст), при этом изменения должны быть невидимыми или незаметными для человеческого восприятия.

Сегодня стеганография находит применение в различных сферах, включая кибер-безопасность, медицину, цифровую форензику, и даже в военных операциях. Однако, вместе с ее потенциальными пользами, возникают и риски, такие как скрытая передача вредоносных данных или нарушение авторских прав. Развитие методов стеганографии и стеганализа становится неотъемлемой частью борьбы за безопасность и контроль над цифровой информацией.

Методы стеганографии разнообразны и эволюционируют вместе с развитием технологий. Они направлены на скрытое внедрение информации в различные типы данных, при этом минимизируя заметность изменений. Ниже приведены основные методы стеганографии:

1. Frequency Domain Steganography:

Этот метод использует преобразование Фурье для внедрения информации в частотной области сигнала. Применяется к изображениям, аудиофайлам и видео. Методы, такие как изменение амплитуды или фазы в определенных частотных компонентах, могут быть использованы для внедрения данных.

1. Spread Spectrum Steganography:

Этот метод аналогичен принципу работы спред-спектра в коммуникационных системах. Информация распределяется по всему спектру сигнала, что делает ее менее заметной. В контексте стеганографии, это может включать в себя изменение фазы, частоты или амплитуды.

1. Transform Domain Steganography:

Этот метод внедрения информации в основном применяется к изображениям и аудиофайлам. Он основан на изменении коэффициентов преобразования (например, вейвлет-преобразования) сигнала. Это позволяет эффективно скрывать данные, используя особенности в различных областях сигнала.

1. Text Steganography:

Скрытая передача информации может также происходить в текстовых данных. Это может включать в себя изменение форматирования, шрифта, размера или даже внедрение скрытого текста в невидимую область текстового документа.

1. Network Steganography:

В данном случае, стеганография применяется к передаче данных через сетевые протоколы. Это может включать в себя изменение размера пакетов, времени задержки и других параметров для скрытой передачи информации.

1. Artificial Intelligence (AI) Steganography:

С использованием методов машинного обучения и искусственного интеллекта, разрабатываются более сложные методы стеганографии, способные адаптироваться и обходить методы стеганализа.

## LSB-метод.

*LSB-метод* в стеганографии представляет собой эффективную технику внедрения скрытой информации в цифровые носители, такие как изображения, аудиофайлы или видео, путем модификации наименее значащих битов этих данных. Акроним "LSB" расшифровывается как "Least Significant Bit" (наименее значащий бит). Этот метод основан на простой, но мощной идее: заменять наименее значащие биты в бинарном представлении пикселей (в случае изображений) или отсчетов (в случае аудиофайлов) на биты скрытого сообщения.

Одной из главных привлекательных черт LSB-метода является его незаметность для человеческого восприятия. Изменения в наименее значащих битах обычно незаметны для человеческого глаза или уха, что позволяет сохранить визуальное или звуковое качество оригинальных данных. Таким образом, LSB-стеганография обеспечивает деликатный баланс между сокрытием информации и сохранением естественного вида или звучания.

Применение LSB-метода может быть широким: от обеспечения конфиденциальности данных и водяных знаков в изображениях до скрытой передачи метаданных или даже хранения дополнительной информации в цифровых файлах. Тем не менее, с увеличением возможностей стеганографии возрастают и риски, связанные с ее злоупотреблением в киберпространстве.

Важно отметить, что LSB-метод, несмотря на свою эффективность, не является безупречным, и существуют методы стеганализа, направленные на обнаружение скрытых данных. Следовательно, постоянное развитие и совершенствование методов стеганографии и стеганализа остаются ключевыми аспектами в обеспечении цифровой безопасности и контроле за передачей информации в современном информационном обществе.

## Плюсы и минусы LSB-метода.

Плюсы LSB-метода в стеганографии:

1. Невидимость для человеческого восприятия: Изменения, внесенные в наименее значащие биты, обычно не заметны для человеческого глаза или уха, что обеспечивает высокую степень незаметности внедрения скрытой информации.
2. Простота реализации: LSB-метод является относительно простым в реализации, что делает его доступным и понятным для широкого круга пользователей.
3. Универсальность: Метод применим к различным типам данных, включая изображения, аудиофайлы и видео, что расширяет его область применения.
4. Отсутствие необходимости в дополнительных ключах: В отличие от некоторых криптографических методов, LSB-стеганография не требует дополнительных ключей для внедрения и извлечения скрытой информации.

Минусы LSB-метода в стеганографии:

1. Низкая устойчивость к стеганализу: LSB-метод является относительно уязвимым для методов стеганализа, направленных на обнаружение скрытых данных. Атакующие могут использовать статистические методы для выявления изменений в наименее значащих битах.
2. Ограниченная вместимость данных: Поскольку информация встраивается в младшие биты, объем доступного места для скрытых данных ограничен. Это может быть недостаточным для встраивания больших объемов информации.
3. Чувствительность к сжатию: Процессы сжатия данных, такие как алгоритмы JPEG для изображений, могут повлиять на наименее значащие биты и стереть скрытую информацию.
4. Не устойчив к некоторым видам атак: Например, при применении атаки сжатия и последующего повторного встраивания информации, может произойти потеря данных и ухудшение качества стеганографического изображения.
5. Неэффективность при работе с текстом: В случае текстовых данных встраивание информации в наименее значащие биты может привести к видимым изменениям в тексте и его структуре.
6. Ограниченность в контексте видео- и аудиостеганографии: В случае видео и аудиофайлов, изменения в наименее значащих битах могут быть заметны при проигрывании контента, особенно при использовании высококачественного оборудования.

# Способы стеганоанализа и защиты от него.

## Способы стеганоанализа.

LSB-метод, несмотря на свою популярность и широкое использование, подвержен риску взлома различными методами стеганализа. Вот несколько методов, которые могут использоваться для взлома LSB-метода:

1. *Статистический анализ* – это анализ статистических характеристик изображения, таких как распределение битов или гистограмма, может выявить аномалии, связанные с внедрением скрытой информации. Если изменения в LSB-битах не соответствуют естественной статистике изображения, это может стать признаком наличия стеганографии.
2. Анализ фрактальной размерности: Изменения, внесенные LSB-методом, могут влиять на фрактальную размерность изображения. Сравнение этой размерности с ожидаемой может выявить скрытые данные.
3. Атаки на сжатие: Алгоритмы сжатия, такие как JPEG, могут изменять LSB-биты при обработке изображения. Процессы сжатия могут привести к потере данных и ухудшению качества стеганографического изображения. Атаки, направленные на такие изменения, могут выявить наличие скрытой информации.
4. Частотный анализ: Анализ частотных компонент изображения может выявить изменения в LSB-битах. Атакующие могут использовать методы фурье-анализа для выделения изменений, связанных с внедрением данных.
5. Атаки на размер файла: Если ожидается, что файл имеет определенный размер, а размер увеличивается из-за внедрения скрытой информации, это может быть признаком стеганографии.
6. Анализ энтропии: Изменения в LSB-битах могут влиять на энтропию изображения. Несоответствие ожидаемой энтропии может быть использовано для обнаружения стеганографии.
7. Особенности формата: Некоторые форматы изображений имеют структуру, которая может быть использована для выявления изменений, связанных с внедрением данных. Например, в BMP-изображениях изменения в заголовках могут выдать стеганографию.
8. Атаки на повторное встраивание: Повторное внедрение данных в стеганографическое изображение может привести к потере части информации. Атаки, направленные на повторное встраивание, могут раскрывать наличие стеганографии.

## Способы защиты от стегоанализа.

Защита от стегоанализа в контексте LSB-метода в стеганографии требует внимательности и использования дополнительных методов для сокрытия внедрения данных. Вот несколько способов защиты от стегоанализа в рамках LSB-метода:

1. Использование случайного выбора битов: Вместо внедрения информации только в наименее значащие биты каждого компонента, можно использовать случайный выбор битов для внедрения. Это делает статистический анализ более сложным, поскольку изменения распределены более случайным образом.
2. Использование адаптивного подхода: Адаптивные методы изменения количества встраиваемых бит в зависимости от конкретных характеристик изображения или звукового файла могут сделать стегоанализ более сложным.
3. Добавление шума: Добавление случайного шума к наименее значащим битам может затруднить стегоанализ. Однако, важно контролировать уровень шума, чтобы сохранить незаметность изменений.
4. Использование дополнительных слоев шифрования: Внедрение дополнительных слоев шифрования поверх LSB-метода может усложнить анализ и обеспечить дополнительный уровень защиты.
5. Смешивание с данными: Перед встраиванием данных можно применить методы, которые смешивают стеганографические изменения с естественными данными, чтобы сделать их менее заметными.
6. Избегание равномерного распределения: Избегание равномерного распределения изменений по всему изображению может снизить эффективность статистических методов стегоанализа.
7. Использование различных каналов: Вмешивание информации в различные цветовые каналы (RGB, YUV и т. д.) может сделать стегоанализ более сложным, поскольку изменения будут распределены по различным компонентам.
8. Динамическая адаптация параметров: Изменение параметров внедрения, таких как количество изменяемых битов, в зависимости от свойств изображения, может сделать анализ более трудным.

# Заключение

В итоге, проведенный анализ методов компьютерной стеганографии, с фокусом на LSB-методе, позволяет сделать несколько важных выводов. LSB-метод, основанный на замене младших битов пикселей изображения, представляет собой эффективный и относительно простой способ внедрения скрытой информации. Его применение широко распространено в различных областях, включая передачу данных в цифровых изображениях, аудиофайлах и видео.

Однако, несмотря на свою популярность, LSB-метод не лишен определенных недостатков. В первую очередь, его уязвимость к атакам, направленным на выявление и извлечение скрытой информации. Существующие методы анализа LSB-стеганографии могут поддаваться современным методам криптоанализа, что подчеркивает важность дополнительных механизмов защиты и усовершенствования техник стеганографии.

В свете растущих угроз безопасности данных и прогрессирующих технологий, изучение методов компьютерной стеганографии, включая LSB-метод, является ключевым элементом в обеспечении информационной безопасности. Перспективы развития данной области связаны с поиском новых методов стеганографии, способных устойчиво сокрыть информацию и предоставить высокий уровень защиты данных от несанкционированного доступа.

Таким образом, дальнейшие исследования в области компьютерной стеганографии, в том числе с учетом LSB-метода, могут способствовать созданию более совершенных и безопасных методов передачи и хранения конфиденциальной информации в цифровой среде.

*Список источников:*

1. Скрывать не скрывая. Еще раз о LSB-стеганографии, хи-квадрате и… сингулярности? – URL: <https://habr.com/ru/articles/422593/>
2. Что такое стеганография? Определение и описание - <https://www.kaspersky.ru/resource-center/definitions/what-is-steganography>
3. Стеганография – URL: <https://ru.wikipedia.org/wiki/Стеганография>
4. Стегоанализ метода сокрытия информации в изображении замены наименьшего значащего бита (LSB) – URL: <https://cyberleninka.ru/article/n/stegoanaliz-metoda-sokrytiya-informatsii-v-izobrazhenii-zameny-naimenshego-znachaschego-bita-lsb>
5. Стеганография в цифровых изображениях – URL: <https://ru.wikipedia.org/wiki/Стеганография_в_цифровых_изображениях>
6. Применение LSB в информационной безопасности – URL: <https://uralchip.ru/faq/lsb-cto-eto-znacit-i-kak-eto-rabotaet>

|  |  |
| --- | --- |
|  | **Российский государственный социальный университет** |

**Итоговое практическое задание № 2.**

**по дисциплине «Информационная безопасность»**

**на тему «Обеспечение безопасности при использовании мобильных устройств в корпоративных ИС»**

|  |  |
| --- | --- |
| **ФИО студента** | Салов Артём Владимирович |
| **Направление подготовки** | Программная инженерия |
| **Группа** | ПИН-Б-О-Д-2021-1 |

**Москва 2023**

Оглавление

[Введение. 3](#_Toc153735027)

[1. Текущий статус мобильных технологий в корпоративных ИС. 4](#_Toc153735028)

[1.1. Основные тренды в использовании мобильных устройств в рабочей среде. 4](#_Toc153735029)

[1.2. Преимущества и риски, связанные с интеграцией мобильных технологий в корпоративные ИС. 4](#_Toc153735030)

[2. Угрозы безопасности мобильных устройств. 5](#_Toc153735031)

[2.1. Обзор основных угроз, таких как потеря устройств, несанкционированный доступ, вредоносные приложения и т.д. 5](#_Toc153735032)

[2.2. Технологические аспекты обеспечения безопасности. 6](#_Toc153735033)

[Организационные меры по обеспечению безопасности. 8](#_Toc153735034)

[Разработка политик безопасности для мобильных устройств. 8](#_Toc153735035)

[Обучение персонала и повышение осведомленности о безопасности. 8](#_Toc153735036)

# Введение.

В эпоху стремительного развития цифровых технологий, мобильные устройства стали неотъемлемой частью рабочей жизни, предоставляя гибкость и доступность в обмене информацией в корпоративных информационных системах (ИС). Однако, с увеличением роли мобильных устройств в корпоративной среде возникают существенные вопросы безопасности, требующие внимательного анализа и эффективных решений.

Тема обеспечения безопасности при использовании мобильных устройств в корпоративных информационных системах становится предметом все возрастающего интереса исследователей и специалистов по информационной безопасности. Настоящее исследование направлено на углубленное рассмотрение технологических, организационных и стратегических аспектов, связанных с обеспечением безопасности в сфере использования мобильных устройств в корпоративном контексте.

Основываясь на современных вызовах и тенденциях, мы сосредоточим внимание на разнообразных методах и инструментах, предназначенных для защиты корпоративных данных при использовании мобильных устройств.

# Текущий статус мобильных технологий в корпоративных ИС.

## Основные тренды в использовании мобильных устройств в рабочей среде.

Основные тренды в использовании мобильных устройств в рабочей среде представляют собой динамичный пейзаж изменений, отражающих современные потребности бизнеса и технологические возможности. Вот несколько ключевых трендов:

* + 1. Быстрое развитие рабочих приложений: С постоянным ростом числа мобильных устройств, предприятия активно инвестируют в разработку высокопроизводительных и интуитивно понятных рабочих приложений. Эти приложения предоставляют сотрудникам доступ к корпоративным ресурсам, управление проектами, коммуникации и другие инструменты прямо с их мобильных устройств.
    2. Тенденция к гибкому рабочему графику: С мобильными устройствами сотрудники все больше имеют возможность работать вне офиса, что приводит к увеличению гибкости в организации рабочего времени. Виртуальные офисы и возможность удаленной работы становятся стандартом для многих компаний, обеспечивая сотрудникам доступ к рабочим ресурсам в любое время и из любой точки мира.
    3. Безопасность и управление устройствами (MDM): Растущая озабоченность безопасностью данных приводит к усилению инвестиций в системы управления устройствами (MDM). Компании всё более осознают важность защиты корпоративных данных на мобильных устройствах и внедряют строгие политики безопасности, включая шифрование данных и удаленное управление утерянными устройствами.
    4. Интеграция технологий искусственного интеллекта (ИИ): Развитие технологий искусственного интеллекта привносит в мобильные устройства инновационные функции, такие как голосовые помощники, персональные рекомендации и автоматизированные задачи. Использование ИИ в бизнес-приложениях может улучшить производительность и оптимизировать бизнес-процессы.
    5. BYOD (Bring Your Own Device): Многие организации переходят к модели BYOD, позволяя сотрудникам использовать свои собственные мобильные устройства для работы. Это снижает расходы на оборудование и повышает удовлетворенность сотрудников, однако требует дополнительных усилий по обеспечению безопасности и управлению устройствами.
    6. Расширенная реальность (AR) и виртуальная реальность (VR): В некоторых отраслях, таких как обучение, медицина и проектирование, мобильные устройства внедряются для работы с технологиями расширенной и виртуальной реальности. Это открывает новые возможности для обучения, визуализации данных и решения сложных задач.

## Преимущества и риски, связанные с интеграцией мобильных технологий в корпоративные ИС.

Преимущества интеграции мобильных технологий в корпоративные информационные системы (ИС):

1. Повышение производительности: Мобильные технологии обеспечивают сотрудникам постоянный доступ к корпоративным ресурсам, что повышает эффективность и оперативность выполнения задач в любом месте и в любое время.
2. Гибкость и мобильность: Интеграция мобильных устройств позволяет сотрудникам работать удаленно или в пути, не теряя доступа к необходимой информации. Это особенно важно в условиях современного бизнеса, требующего гибких рабочих условий.
3. Улучшение коммуникации: Мобильные приложения облегчают коммуникацию внутри команд и организации. Быстрый обмен сообщениями, видеозвонки и общий доступ к данным способствуют более эффективному общению между сотрудниками.
4. Развитие BYOD-подхода: Интеграция мобильных технологий позволяет внедрять BYOD (Bring Your Own Device), что снижает расходы на оборудование и повышает удовлетворенность сотрудников, использующих свои собственные устройства для работы.
5. Сокращение бумажной работы: Внедрение мобильных технологий часто сопровождается переходом к электронным документам и формам, что снижает использование бумажной документации и упрощает процессы обработки информации.

Риски, связанные с интеграцией мобильных технологий в корпоративные ИС:

1. Потеря устройств и конфиденциальных данных: Мобильные устройства могут быть потеряны или украдены, что представляет угрозу для конфиденциальных корпоративных данных. Отсутствие соответствующих мер безопасности может привести к утечкам информации.
2. Угрозы вредоносных программ: Мобильные устройства подвергаются риску вредоносных программ и вирусов. Атаки через приложения, фишинг и другие методы могут стать источником угроз для безопасности данных.
3. Сложности управления безопасностью: Управление безопасностью на мобильных устройствах может быть более сложным, чем на традиционных компьютерах. Необходимость внедрения систем управления устройствами (MDM) и обучения сотрудников использованию безопасных практик становится критической.
4. Компрометация личной информации: BYOD-подход может повлечь за собой риск компрометации личной информации сотрудников, особенно в случаях, когда на их устройствах хранятся и личные, и корпоративные данные.
5. Сложности с совместимостью и интеграцией: Разнообразие мобильных устройств и операционных систем может создавать трудности в обеспечении совместимости и интеграции с существующими корпоративными ИС.

# Угрозы безопасности мобильных устройств.

## Обзор основных угроз, таких как потеря устройств, несанкционированный доступ, вредоносные приложения и т.д.

* + 1. Потеря устройств:
* Сценарий: Утеря или кража мобильного устройства с корпоративной информацией.
* Последствия: Потеря конфиденциальных данных, угроза безопасности корпоративной сети.
  + 1. Несанкционированный доступ:
* Сценарий: Несанкционированный доступ к мобильным устройствам сотрудников или к корпоративным ресурсам через уязвимости в сетевой безопасности.
* Последствия: Кража данных, нарушение конфиденциальности, потенциальные финансовые потери.
  + 1. Вредоносные приложения:
* Сценарий: Установка вредоносных приложений на мобильные устройства, представляющих угрозу для безопасности данных.
* Последствия: Потеря контроля над устройством, утечка информации, возможные атаки на корпоративные сети.
  + 1. Фишинг и социальная инженерия:
* Сценарий: Атаки, направленные на обман сотрудников и получение доступа к корпоративным учетным записям.
* Последствия: Утеря данных, компрометация учетных записей, возможные финансовые потери.
  + 1. Неаккуратное использование устройств:
* Сценарий: Несанкционированное распространение корпоративной информации через мобильные устройства (например, через социальные сети).
* Последствия: Репутационные потери, утечка конфиденциальных данных, нарушение политик безопасности.
  + 1. Угрозы сетевой безопасности:
* Сценарий: Атаки на беспроводные сети, использование уязвимостей в сетевых протоколах.
* Последствия: Несанкционированный доступ к корпоративным данным, подмена данных, атаки на сервисы.
  + 1. Утрата управления утерянным устройством:
* Сценарий: Невозможность удаленного управления утерянным устройством, в том числе удаленная блокировка или удаление данных.
* Последствия: Угроза утечки данных, возможность несанкционированного использования утерянного устройства.
  + 1. Недостатки в управлении устройствами (MDM):
* Сценарий: Недостаточное управление безопасностью на стороне MDM, неспособность обнаруживать и реагировать на новые угрозы.
* Последствия: Уменьшение эффективности системы MDM, риск безопасности данных.
  + 1. Низкая осведомленность сотрудников:
* Сценарий: Недостаточная осведомленность сотрудников о практиках безопасности на мобильных устройствах.
* Последствия: Больше вероятность попадания в схемы социальной инженерии, небрежное обращение с конфиденциальными данными.

## Технологические аспекты обеспечения безопасности.

* + 1. Современные методы шифрования данных на мобильных устройствах.

1. AES (Advanced Encryption Standard):

* Описание: AES является одним из наиболее распространенных и безопасных методов симметричного шифрования. Он использует блочный шифр с ключом длиной 128, 192 или 256 бит, что делает его эффективным для шифрования данных на мобильных устройствах.
* Применение: Шифрование данных в хранилищах устройства, передача данных через сеть.

1. RSA (Rivest–Shamir–Adleman):

* Описание: RSA является асимметричным методом шифрования, использующим пару открытого и закрытого ключей. Он часто применяется для обеспечения безопасности ключей шифрования и подписи данных.
* Применение: Защита ключей шифрования, создание цифровых подписей.

1. Diffie-Hellman:

* Описание: Метод Diffie-Hellman обеспечивает безопасный обмен ключами между устройствами в открытом канале связи. Он часто используется в комбинации с другими методами шифрования для создания безопасных каналов связи.
* Применение: Обмен ключами для симметричного шифрования.

1. ECC (Elliptic Curve Cryptography):

* Описание: ECC представляет собой метод асимметричного шифрования, использующий эллиптические кривые для генерации ключей. Он обеспечивает высокую степень безопасности при меньших вычислительных ресурсах по сравнению с классическими методами.
* Применение: Шифрование данных, создание электронных подписей.

1. Технология TPM (Trusted Platform Module):

* Описание: TPM — это аппаратный модуль, встроенный в мобильные устройства, который обеспечивает хранение и защиту ключей шифрования. Он используется для укрепления безопасности процесса аутентификации и шифрования данных.
* Применение: Хранение ключей, подпись данных, аутентификация устройства.

1. End-to-End Encryption (E2EE):

* Описание: E2EE представляет собой метод шифрования, при котором данные шифруются на уровне отправителя и дешифруются только на уровне получателя. Это обеспечивает максимальную конфиденциальность данных в течение всего процесса передачи.
* Применение: Шифрование сообщений в мессенджерах, электронная почта.

1. VPN (Virtual Private Network):

* Описание: VPN обеспечивает шифрование данных в туннеле между устройством пользователя и сервером, что защищает информацию от прослушивания на пути передачи.
* Применение: Защита данных при передаче по открытым сетям, обеспечение безопасного доступа к корпоративным ресурсам.

Эти методы могут применяться отдельно или в комбинации для создания многоуровневой системы шифрования, обеспечивающей надежную защиту данных на мобильных устройствах.

* + 1. Аутентификация и управление доступом к корпоративным ресурсам.

Аутентификация:

1. Многофакторная аутентификация (MFA):

* Описание: MFA включает использование нескольких методов подтверждения личности пользователя, таких как пароль, биометрические данные, токены или одноразовые коды.
* Применение: Усиление безопасности за счет комбинации различных факторов аутентификации.

1. Биометрическая аутентификация:

* Описание: Использование уникальных физиологических или поведенческих характеристик, таких как отпечатки пальцев, распознавание лица, голосовые данные.
* Применение: Более надежное и удобное средство аутентификации.

1. Усиление аутентификации при входе:

* Описание: Дополнительные шаги аутентификации при входе, такие как ответ на дополнительный вопрос или ввод временного кода.
* Применение: Укрепление защиты при входе в систему.

Управление доступом:

1. Принцип наименьших привилегий (Least Privilege):

* Описание: Предоставление пользователям минимально необходимого уровня доступа для выполнения своих задач, чтобы ограничить потенциальные угрозы.
* Применение: Минимизация рисков путем ограничения прав доступа.

1. Ролевая модель управления доступом:

* Описание: Назначение прав доступа на основе ролей пользователей в организации. Каждая роль имеет определенные привилегии, соответствующие обязанностям пользователя.
* Применение: Эффективное управление доступом к ресурсам в зависимости от функциональных обязанностей.

1. Централизованное управление доступом:

* Описание: Использование централизованных систем управления доступом для единообразного и удобного контроля прав доступа ко всем ресурсам.
* Применение: Снижение рисков и обеспечение единообразия в управлении доступом.

1. Аудит и мониторинг доступа:

* Описание: Запись и анализ активности пользователей для выявления подозрительных действий или несанкционированного доступа.
* Применение: Быстрое обнаружение и реагирование на угрозы безопасности.

1. Временное управление доступом:

* Описание: Ограничение времени действия определенных прав доступа для пользователей в зависимости от контекста или времени суток.
* Применение: Управление временным доступом для повышения безопасности в критические периоды.

1. Интеграция с единой системой аутентификации (SSO):

* Описание: Использование SSO для обеспечения однократной аутентификации и автоматического предоставления доступа к различным ресурсам без повторной аутентификации.
* Применение: Удобство для пользователей и сокращение рисков связанных с необходимостью многократной аутентификации.

# Организационные меры по обеспечению безопасности.

Разработка политик безопасности для мобильных устройств является критическим шагом в обеспечении безопасности информационных ресурсов организации. Эти политики должны устанавливать стандарты и правила, регулирующие использование мобильных устройств сотрудниками в рамках корпоративного окружения.

## Разработка политик безопасности для мобильных устройств.

Ключевые аспекты при разработке политик безопасности:

1. Цели политики безопасности:

* Защита конфиденциальности: Гарантировать, что конфиденциальная информация не подвергается угрозам утечки или несанкционированного доступа.
* Обеспечение целостности данных: Предотвращение несанкционированных изменений и модификаций данных на мобильных устройствах.
* Гарантирование доступности: Обеспечение надежного и безопасного доступа к корпоративным ресурсам с мобильных устройств.
* Минимизация рисков: Сокращение возможности угроз и атак на корпоративные данные, связанных с использованием мобильных устройств.

1. Управление устройствами:

* Обязательная регистрация устройств: Требование к регистрации всех мобильных устройств, используемых в корпоративной сети.
* Удаленное управление устройствами (MDM): Реализация систем MDM для централизованного управления устройствами, включая возможности блокировки, удаленного стирания и мониторинга.
* Политики BYOD (Bring Your Own Device): Определение правил для использования сотрудниками собственных устройств, включая требования к безопасности и процедуры регистрации.

1. Аутентификация и авторизация:

* Использование многофакторной аутентификации: Введение требования использования двух и более методов аутентификации для повышения безопасности.
* Управление привилегиями: Применение принципов наименьших привилегий и ролевой модели управления доступом для контроля полномочий пользователей.

1. Шифрование и безопасность данных:

* Обязательное шифрование данных: Установка требования шифрования для всех хранимых на мобильных устройствах корпоративных данных.
* Защита от утери данных: Введение механизмов удаленного стирания данных в случае утери или кражи устройства.

1. Обучение и осведомленность:

* Обучение сотрудников: Проведение обучения сотрудников по правилам безопасности при использовании мобильных устройств.
* Регулярные проверки знаний: Проведение регулярных проверок знаний сотрудников в области безопасности мобильных технологий.

1. Аудит и мониторинг:

* Системы аудита и мониторинга: Разработка систем аудита и мониторинга для отслеживания активности пользователей и выявления потенциальных угроз.
* Реагирование на инциденты: Определение процедур и ответственности в случае обнаружения безопасностных инцидентов на мобильных устройствах.

1. Политики использования:

* Ограничение использования несанкционированных приложений: Установка правил по использованию только одобренных и безопасных приложений.
* Определение правил работы в общественных сетях: Установление правил для безопасного использования мобильных устройств в общественных Wi-Fi сетях.

Эти меры представляют собой основные элементы политики безопасности для мобильных устройств. Они должны быть адаптированы к конкретным потребностям и требованиям организации, а также регулярно обновляться в ответ на изменяющуюся угрозовую среду и развитие технологий.

## Обучение персонала и повышение осведомленности о безопасности.

1. Разработка обучающих программ:

* Интерактивные курсы по безопасности мобильных устройств.
* Тренинги для распознавания и предотвращения фишинговых атак.

1. Создание ресурсов:

* Информационные материалы для самостоятельного обучения.
* Доступ к онлайн-ресурсам.

1. Организация сессий:

* Регулярные тренинги и симуляции атак.
* Вовлечение руководства и использование реальных случаев.

1. Проверки и тестирование:

* Регулярные тесты знаний и проверки.
* Обратная связь для улучшения результата тестирования.

1. Активные кампании:

* События по безопасности и использование внутренних коммуникаций.
* Метрики для отслеживания прогресса.

1. Поддержка службы безопасности:

* Консультации и обратная связь.
* Система для сообщений о безопасности от сотрудников.

# Заключение.

В заключение, разработка и внедрение политики безопасности для мобильных устройств, совмещенные с эффективными мерами обучения персонала, представляют собой неотъемлемый комплекс в обеспечении надежной кибербезопасности организации. Обеспечивая защиту конфиденциальности, целостности и доступности данных, такая политика становится стержнем, на котором строится устойчивая кибербезопасная среда.

Обучение персонала, включая регулярные тренинги, тестирование и активные кампании осведомленности, играет ключевую роль в создании культуры безопасности в организации. Это не только укрепляет знания сотрудников по вопросам безопасности мобильных устройств, но также помогает им активно участвовать в поддержании безопасного цифрового пространства.

С учетом динамичной природы киберугроз и постоянного развития технологий, необходимость в постоянном совершенствовании политик безопасности и обучении персонала становится более актуальной. Регулярный мониторинг, анализ инцидентов и адаптация подходов к обучению помогут эффективно реагировать на новые угрозы и поддерживать высокий уровень защиты.

Только внедрение комплексного подхода, охватывающего технологические, организационные и образовательные аспекты, позволяет организациям успешно противостоять современным угрозам в цифровом мире и обеспечивать безопасное использование мобильных устройств в корпоративной среде.

*Список литературы:*

1. Корпоративная мобильная безопасность и управление доступом пользователей – URL: <https://habr.com/ru/companies/gemaltorussia/articles/323338/>
2. Обеспечение ИБ корпоративных мобильных устройств – URL: <https://lib.itsec.ru/articles2/mobile-security/obespechenie-ib-korporativnyh-mobilnyh-ustroystv>
3. 7.6 Безопасность мобильных пользователей корпоративных систем – URL: <https://studfile.net/preview/3015145/page:25/>
4. Безопасность мобильного предприятия – URL: <https://www.osp.ru/os/2013/01/13033833>
5. Мобильные устройства в корпоративной среде: риски и угрозы XXI века – URL: <https://www.itweek.ru/security/article/detail.php?ID=194871>

|  |  |
| --- | --- |
|  | **Российский государственный социальный университет** |

**Итоговое практическое задание № 3.**

**по дисциплине «Информационная безопасность»**

**на тему «Создание блоков в сети Биткоин»**

|  |  |
| --- | --- |
| **ФИО студента** | Салов Артём Владимирович |
| **Направление подготовки** | Программная инженерия |
| **Группа** | ПИН-Б-О-Д-2021-1 |

**Москва 2023**

Оглавление

[Введение. 3](#_Toc153737419)

[1. Основные принципы работы сети Биткоин. 4](#_Toc153737420)

[1.1. Понятие блокчейна и его роль в сети Биткоин. 4](#_Toc153737421)

[1.2. Децентрализованная природа криптовалюты и блокчейна. 4](#_Toc153737422)

[1.3. Концепция децентрализованных транзакций и хранения данных. 4](#_Toc153737423)

[2. Майнинг и майнеры в сети Биткоин. 4](#_Toc153737424)

[2.1. Роль майнинга в создании новых блоков. 4](#_Toc153737425)

[2.2. Как майнеры конкурируют за право добавить блок в блокчейн. 4](#_Toc153737426)

[2.3. Вознаграждение майнеров и стимулы для участия в майнинге. 4](#_Toc153737427)

[3. Структура блока в сети Биткоин. 4](#_Toc153737428)

[3.1. Как формируются транзакции внутри блока. 5](#_Toc153737429)

[3.2. Размер блока и проблемы масштабируемости. 5](#_Toc153737430)

[3.3. Мерклевские деревья и их роль в обеспечении целостности блока. 5](#_Toc153737431)

[4. Криптографические аспекты создания блоков в сети Биткоин. 5](#_Toc153737432)

[4.1. Применение хэш-функций в блокчейне. 5](#_Toc153737433)

[4.2. Роль нулевых битов (Proof-of-Work) в процессе майнинга. 5](#_Toc153737434)

[4.3. Обеспечение безопасности блокчейна через криптографию. 5](#_Toc153737435)

[5. Транзакции в сети Биткоин: 5](#_Toc153737436)

[5.1. Структура транзакции. 6](#_Toc153737437)

[5.2. Входы и выходы транзакции: 6](#_Toc153737438)

[5.3. Подписи и удостоверения подлинности в транзакциях: 6](#_Toc153737439)

[6. Проблемы и вызовы при создании блоков в сети Биткоин: 6](#_Toc153737440)

[6.1. Проблемы масштабируемости и способы их решения: 6](#_Toc153737441)

[6.2. Экологические и энергетические аспекты майнинга: 6](#_Toc153737442)

[6.3. Влияние высоких комиссий на процесс создания блоков: 6](#_Toc153737443)

[7. Будущее создания блоков в сети Биткоин: 6](#_Toc153737444)

[7.1. Тенденции и направления развития технологии: 7](#_Toc153737445)

[7.2. Исследования и предложения по улучшению процесса создания блоков: 7](#_Toc153737446)

[7.3. Возможные изменения и обновления протокола Биткоин: 7](#_Toc153737447)

[Заключение. 8](#_Toc153737448)

# Введение.

В современном мире криптовалюты стали одним из наиболее обсуждаемых и активно развивающихся направлений в финансовой сфере. Среди них особое место занимает биткоин – первая и наиболее известная криптовалюта, которая стала непрерывным объектом внимания исследователей, инвесторов и обычных пользователей.

Одним из фундаментальных аспектов функционирования биткоин-сети является процесс создания блоков, который является неотъемлемой частью механизма децентрализованной криптовалютной системы. Создание блоков в сети биткоин обеспечивает не только осуществление транзакций, но и обеспечивает безопасность и устойчивость всей сети.

В данном докладе мы рассмотрим ключевые аспекты создания блоков в сети биткоин, начиная от базовых принципов и заканчивая более сложными технологическими процессами. Мы рассмотрим, как майнеры соревнуются за право добавить новый блок в блокчейн, как формируются транзакции в блоках, и какие механизмы обеспечивают целостность и надежность всей системы.

Погружение в процесс создания блоков в сети биткоин позволит нам лучше понять не только технические аспекты функционирования криптовалют, но и их влияние на современную финансовую и технологическую парадигму. Давайте вместе пройдем через ключевые шаги и механизмы, сделавшие биткоин настоящим веховым событием в мире децентрализованных финансов.

# Основные принципы работы сети Биткоин.

*Битко́йн* — пиринговая платёжная система, использующая одноимённую единицу для учёта операций.

Сеть Биткоин представляет собой децентрализованный механизм обмена цифровыми активами, основанный на инновационной технологии блокчейн.

## Понятие блокчейна и его роль в сети Биткоин.

*Блокчейн* представляет собой цепочку блоков, каждый из которых содержит информацию о транзакциях. Эта цепочка хранится на распределенной сети компьютеров, что обеспечивает прозрачность и надежность. Блокчейн является основой для регистрации всех транзакций в сети Биткоин.

## Децентрализованная природа криптовалюты и блокчейна.

Биткоин работает без центрального контроля, что отличает его от традиционных финансовых систем. Блокчейн распределен по всей сети узлов, каждый из которых хранит полную историю транзакций. Это исключает необходимость доверия к центральному органу и обеспечивает устойчивость к внешним атакам.

## Концепция децентрализованных транзакций и хранения данных.

Транзакции в сети Биткоин проводятся напрямую между участниками, обходя посредников. Эти транзакции затем собираются в блоки и добавляются к общей цепочке. Этот процесс обеспечивает децентрализованный и открытый характер сети, снижая вероятность мошенничества и обеспечивая непрерывность операций.

# Майнинг и майнеры в сети Биткоин.

Майнинг в сети Биткоин представляет собой ключевой механизм, обеспечивающий безопасность и эффективную работу блокчейна. Майнеры играют решающую роль в создании новых блоков и поддержании устойчивости криптовалютной системы.

## Роль майнинга в создании новых блоков.

*Майнинг* – это процесс решения математически сложных задач, известных как "Proof-of-Work" (доказательство выполнения работы), с целью добавления нового блока в блокчейн. Этот процесс требует вычислительной мощности, и успешное решение проблемы позволяет майнеру создать новый блок и добавить его к цепочке.

## Как майнеры конкурируют за право добавить блок в блокчейн.

Майнеры соревнуются между собой за возможность добавить следующий блок. Это достигается путем решения криптографической задачи, что делает процесс не только конкурентоспособным, но и децентрализованным. Успешный майнер получает право добавить блок и получает вознаграждение в виде новых биткоинов и комиссий от транзакций.

## Вознаграждение майнеров и стимулы для участия в майнинге.

Майнеры получают как новые биткоины, так и комиссии от транзакций в блоке в качестве вознаграждения за свою работу. Это служит стимулом для участия в майнинге и обеспечивает долгосрочную устойчивость сети. Система также предусматривает уменьшение вознаграждения с течением времени, что создает дефицитность биткоинов и повышает их ценность.

# 3. Структура блока в сети Биткоин.

Структура блока в сети Биткоин представляет собой сложный организованный формат, в котором информация о транзакциях и других ключевых элементах сохраняется и обеспечивает ее интегритет. Рассмотрим основные компоненты и принципы формирования блока в блокчейне Биткоин.

## 3.1. Как формируются транзакции внутри блока.

Каждый блок содержит информацию о проведенных транзакциях. Эти транзакции группируются в блок в хронологическом порядке и представляют собой записи об обмене биткоинами между участниками сети. Каждая транзакция содержит входы (inputs) и выходы (outputs), определяя, откуда берутся средства и куда они направляются.

## 3.2. Размер блока и проблемы масштабируемости.

Размер блока влияет на количество транзакций, которые он может содержать. Проблемы масштабируемости в сети Биткоин связаны с ограниченным размером блока, что приводит к задержкам в обработке транзакций и увеличению комиссий. Сообщество активно исследует способы решения этих проблем, такие как внедрение второго уровня (Layer 2) или увеличение размера блока.

## 3.3. Мерклевские деревья и их роль в обеспечении целостности блока.

Мерклевские деревья представляют собой структуру данных, позволяющую эффективно и безопасно хранить хеш-суммы транзакций в блоке. Это обеспечивает быструю проверку целостности блока: изменение любой транзакции потребует изменения соответствующей хеш-суммы, что сразу становится заметным.

# Криптографические аспекты создания блоков в сети Биткоин.

Криптография играет фундаментальную роль в обеспечении безопасности и целостности блокчейна Биткоин. Рассмотрим ключевые криптографические аспекты, которые лежат в основе создания блоков и обеспечивают надежность этой инновационной криптовалютной системы.

## Применение хэш-функций в блокчейне.

Хэш-функции играют центральную роль в создании блоков. Каждый блок содержит уникальный хеш, который зависит от данных в блоке. Эта хеш-функция служит не только для идентификации блока, но и для обеспечения целостности данных: даже небольшие изменения в блоке вызовут существенное изменение его хеша.

## Роль нулевых битов (Proof-of-Work) в процессе майнинга.

Алгоритм Proof-of-Work требует, чтобы майнеры находили хеш для блока, начинающийся с определенного количества нулевых битов. Этот процесс трудоемок и требует значительной вычислительной мощности. Таким образом, майнеры фактически доказывают, что они выполнили определенный объем работы для создания нового блока.

## Обеспечение безопасности блокчейна через криптографию.

Эллиптическая криптография используется для создания криптографических подписей, которые подтверждают подлинность транзакций в блоке. Приватные и публичные ключи используются для безопасной передачи средств, а смарт-контракты предоставляют дополнительные возможности для программных соглашений в блокчейне.

# Транзакции в сети Биткоин:

Транзакции представляют собой основной строительный блок блокчейна Биткоин, определяя перемещение цифровых активов между участниками сети. Рассмотрим ключевые аспекты транзакций в сети Биткоин, начиная от их структуры и заканчивая важными элементами, обеспечивающими безопасность и прозрачность операций.

## Структура транзакции.

Транзакция включает в себя несколько обязательных элементов. Это входы, которые указывают, откуда берутся средства, и выходы, которые определяют, куда направляются эти средства. Также присутствует поле с данными и подписи для обеспечения подлинности.

## Входы и выходы транзакции:

Входы транзакции представляют собой ссылки на выходы предыдущих транзакций, которые становятся входами для новой операции. Выходы определяют, какие адреса и с какими суммами получат средства. Эта структура обеспечивает прозрачность владения и передачи биткоинов.

## Подписи и удостоверения подлинности в транзакциях:

Для подтверждения того, что отправитель имеет право распоряжаться средствами, используется цифровая подпись. Она создается приватным ключом отправителя и проверяется публичным ключом, что обеспечивает надежную аутентификацию и предотвращает манипуляции с транзакциями.

# Проблемы и вызовы при создании блоков в сети Биткоин:

Несмотря на инновационность и успехи сети Биткоин, существуют определенные вызовы и проблемы, которые необходимо решать для дальнейшего развития и улучшения функциональности блокчейна. Рассмотрим некоторые из ключевых проблем и вызовов, с которыми сталкивается сеть Биткоин.

## Проблемы масштабируемости и способы их решения:

С увеличением числа транзакций возникают проблемы масштабируемости. Ограниченный размер блока приводит к задержкам в обработке транзакций и увеличению комиссий. Разработка технологий второго уровня, таких как Lightning Network, и обновлений протокола направлена на решение этих проблем.

## Экологические и энергетические аспекты майнинга:

Майнинг Биткоина требует значительных вычислительных ресурсов, что приводит к высокому энергопотреблению. Эта проблема привлекает внимание из-за своего воздействия на окружающую среду. Исследования направлены на разработку более эффективных и экологически устойчивых методов майнинга.

## Влияние высоких комиссий на процесс создания блоков:

В условиях ограниченной вместимости блоков, конкуренция за включение транзакций становится более яркой, что приводит к увеличению комиссий. Это может сделать мелкие транзакции менее конкурентоспособными и повлиять на пользователей с небольшими суммами.

# Будущее создания блоков в сети Биткоин:

Будущее сети Биткоин предвещает внедрение новых технологий и изменения в протоколе с целью повышения эффективности, безопасности и устойчивости системы. Рассмотрим направления развития, которые могут оказать влияние на процесс создания блоков в блокчейне Биткоин.

## Тенденции и направления развития технологии:

С появлением новых технологий, таких как смарт-контракты и алгоритмы консенсуса, сеть Биткоин может расширить свои возможности. Исследования в области масштабируемости, приватности и интероперабельности также будут влиять на будущую архитектуру создания блоков.

## Исследования и предложения по улучшению процесса создания блоков:

Активное научное исследование направлено на выявление потенциальных улучшений в протоколе Биткоина. Вопросы, связанные с масштабируемостью, снижением энергопотребления и улучшением алгоритмов консенсуса, занимают центральное место в этих исследованиях.

## Возможные изменения и обновления протокола Биткоин:

Сообщество Биткоин активно обсуждает различные предложения по улучшению протокола, такие как BIP (Bitcoin Improvement Proposals). Эти изменения могут включать в себя улучшенные методы масштабирования, новые функциональности и изменения в правилах создания блоков.

# Заключение.

В заключение можно отметить, что блокчейн Биткоин стал неотъемлемой частью современного финансового мира, предоставляя инновационный и эффективный механизм обмена цифровыми активами. Процесс создания блоков в сети Биткоин, основанный на принципах децентрализации, безопасности и прозрачности, стал фундаментом для развития криптовалют и блокчейн-технологии в целом.

Несмотря на свои достижения, сеть Биткоин сталкивается с вызовами, такими как проблемы масштабируемости и вопросы, связанные с энергопотреблением майнинга. Однако активное исследование и обсуждение в сообществе намечают пути решения этих проблем, что говорит о готовности к долгосрочному развитию.

Роль Биткоина как средства хранения стоимости и инструмента для достижения финансовой инклюзивности подчеркивает его значение в глобальной экономике. Будущее блокчейна Биткоин наполнено инновациями, исследованиями и постоянным стремлением к улучшению, что делает его ключевым участником в мировой финансовой революции.

*Список источников:*

1. Bitcoin. Как это работает – URL: <https://habr.com/ru/articles/114642/>
2. Блокчейн изнутри: как устроен биткоин. Разбираемся раз и навсегда человеческим языком. – URL: <https://pikabu.ru/story/blokcheyn_iznutri_kak_ustroen_bitkoin_razbiraemsya_raz_i_navsegda_chelovecheskim_yazyikom_dlinnopost_8857566>
3. Биткойн – URL: <https://ru.wikipedia.org/wiki/Биткойн>
4. Блок Биткоина - что это такое и как он устроен? – URL: <https://tehnoobzor.com/cryptolife/bitcoin/2006-blok-bitkoina-chto-eto-takoe-i-kak-on-ustroen.html>
5. Технология блокчейн и Биткоин: Информация – URL: <https://intuit.ru/studies/courses/3520/762/info>

|  |  |
| --- | --- |
|  | **Российский государственный социальный университет** |

**Глоссарий.**

**по дисциплине «Информационная безопасность»**

|  |  |
| --- | --- |
| **ФИО студента** | Салов Артём Владимирович |
| **Направление подготовки** | Программная инженерия |
| **Группа** | ПИН-Б-О-Д-2021-1 |

**Москва 2023**

1. *Стеганография – на стр. 4* — это междисциплинарная наука и искусство передавать сокрытые данные, внутри других, не сокрытых данных. Скрываемые данные обычно называют стегосообщением, а данные, внутри которых находится стегосообщение называют контейнером. – URL: <https://habr.com/ru/articles/253045/>
2. *Стегоанализ или Стеганоанализ* — раздел стеганографии; наука о выявлении факта передачи скрытой информации в анализируемом сообщении. В некоторых случаях под стегоанализом понимают также извлечение скрытой информации из содержащего её сообщения и (если это необходимо) дальнейшую её дешифровку. – URL: <https://ru.wikipedia.org/wiki/Стегоанализ>
3. *Наименьший значащий бит (Least Significant Bit, LSB*) – на стр. 5 — это техника стеганографии, которая используется в информационной безопасности для скрытой передачи данных. В основе техники LSB лежит замена наименее значимых битов в изображении, звуковом файле или других носителях информации на скрываемые данные. – URL: <https://uralchip.ru/faq/lsb-cto-eto-znacit-i-kak-eto-rabotaet#:~:text=Наименьший%20значащий%20бит%20(Least%20Significant,слухово%20файлы%20остаются%20без%20изменений>
4. *Статистический анализ – на стр. 6* — это процесс сбора и анализа информации, данных о различных аспектах социально-экономической жизнедеятельности, ориентированный на оценку их закономерностей, текущего состояния и перспектив развития, что обеспечивает управленческий учет сведениями, лежащими в основе принимаемых управленческих решений.– URL: <https://spravochnick.ru/statistika/statisticheskiy_analiz/#:~:text=Статистический%20анализ%20—%20это%20процесс,в%20основе%20принимаемых%20управленческих%20решений>
5. *TPM (Trusted Platform Module) – на стр. 15* — это независимый компонент системы, который контролирует ее состояние и обеспечивает защиту данных с помощью шифрования. TPM может быть реализован как отдельный чип в устройстве или как программа, однако аппаратные TPM считаются более надежными. – URL: <https://encyclopedia.kaspersky.ru/glossary/trusted-platform-module-tpm/#:~:text=Trusted%20Platform%20Module%20(TPM%2C%20доверенный,аппаратные%20TPM%20считаются%20более%20надежными>
6. *Блокче́йн* — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих какую-либо информацию.– URL: <https://ru.wikipedia.org/wiki/Блокчейн>
7. *Майнинг – на стр. 24* – это процесс решения математически сложных задач, известных как "Proof-of-Work" (доказательство выполнения работы), с целью добавления нового блока в блокчейн. Этот процесс требует вычислительной мощности, и успешное решение проблемы позволяет майнеру создать новый блок и добавить его к цепочке. – URL: <https://ufchgu.ru/blog/matematicheskie-zadachi-v-majninge-ot>
8. *Битко́йн* — пиринговая платёжная система, использующая одноимённую единицу для учёта операций. – URL: <https://ru.wikipedia.org/wiki/Биткойн>
9. *RSA* (аббревиатура от фамилий Rivest, Shamir и Adleman) – на стр. 15 — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших полупростых чисел. – URL: <https://ru.wikipedia.org/wiki/RSA>
10. SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. – URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-a-ssl-certificate>