Практическое занятие №1

Концепция национальной безопасности Республики Беларусь

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия:** изучение Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, а также ознакомление с правовым обеспечением информационной безопасности в Республике Беларусь.

**Краткие теоретические сведения:**

Концепция национальной безопасности Республики Беларусь определяет основные направления государственной политики в области обеспечения безопасности страны, включая информационную безопасность. С развитием информационных технологий возникла необходимость стандартизации требований в области защиты информации. Основная задача стандартов информационной безопасности — создание основы для взаимодействия между производителями, потребителями и специалистами по сертификации.

Правовое обеспечение информационной безопасности в Республике Беларусь включает:

* Международные договоры, такие как Соглашение о сотрудничестве государств — участников СНГ в области обеспечения информационной безопасности от 20 ноября 2013 г.
* Конституцию Республики Беларусь, которая гарантирует гражданам право на получение, хранение и распространение информации.
* Кодифицированные нормативные правовые акты, такие как Гражданский кодекс, Кодекс об административных правонарушениях, Уголовный кодекс, Трудовой кодекс и Налоговый кодекс.
* Законы Республики Беларусь, регулирующие вопросы защиты информации, такие как Закон «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З.

**Ответы на контрольные вопросы:**

**1. Что такое информационная безопасность?**

Информационная безопасность — это состояние защищенности информационных ресурсов и систем от угроз, которые могут привести к нарушению конфиденциальности, целостности или доступности информации.

**2.** **Перечислите основные национальные интересы в информационной сфере.**

Основные национальные интересы в информационной сфере включают:

* + Защиту государственной тайны и конфиденциальной информации.
  + Обеспечение устойчивости информационных систем.
  + Предотвращение киберугроз и кибератак.
  + Развитие информационных технологий и цифровой экономики.

**3.Какие основные угрозы национальной безопасности, связанные с ИТ-сферой, вы знаете?**

Основные угрозы:

* Кибератаки на критически важные объекты инфраструктуры.
* Утечка конфиденциальной информации.
* Распространение вредоносного программного обеспечения.
* Дезинформация и манипуляция общественным мнением через информационные каналы.

**4. Назовите основные внутренние и внешние источники угроз национальной безопасности в информационной сфере.**

* Внутренние источники:
  + Недостаточный уровень защиты информационных систем.
  + Халатность сотрудников, работающих с конфиденциальной информацией.
  + Недостаточное финансирование мер по обеспечению информационной безопасности.
* Внешние источники:
  + Кибератаки со стороны иностранных государств.
  + Деятельность международных хакерских группировок.
* Распространение вредоносного программного обеспечения через интернет.
  + Использование информационных технологий для вмешательства во внутренние дела государства.
  + Дезинформационные кампании через социальные сети и СМИ

**5. Перечислите основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере.**

1. Совершенствование законодательства в области информационной безопасности.
2. Повышение уровня подготовки специалистов по информационной безопасности.
3. Внедрение современных технологий защиты информации (шифрование, системы обнаружения вторжений).
4. Регулярный аудит и тестирование информационных систем на уязвимости.
5. Обучение сотрудников правилам работы с конфиденциальной информацией.
6. Создание резервных копий данных и систем восстановления после сбоев.
7. Развитие национальных технологий для снижения зависимости от иностранного программного обеспечения.
8. Создание систем мониторинга и предотвращения кибератак.
9. Международное сотрудничество в борьбе с киберпреступностью.
10. Блокирование вредоносных ресурсов и дезинформационных кампаний.
11. Укрепление защиты критически важных объектов (энергетика, транспорт, связь).
12. Разработка стратегий противодействия информационным войнам и пропаганде.
13. Создание резервных систем для обеспечения устойчивости информационной инфраструктуры в случае атак.

**Использованные источники**

1. Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь».
2. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».
3. Гражданский кодекс Республики Беларусь.
4. Уголовный кодекс Республики Беларусь.
5. Трудовой кодекс Республики Беларусь.
6. Налоговый кодекс Республики Беларусь.
7. Материалы лекций и учебные пособия по информационной безопасности.

Практическое занятие №2

Решение задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия:** научиться решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях не санкционированного доступа.

Условие задания:  
Решите задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкциониро ванного доступа в соответствии с вариантом. Варианты выполне ния задания соответствуют номеру студента по журналу группы.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер варианта | E0 | E | K | C |
| 4 | 15000 | 12000 | 2 | 1000 |

Выполнение работы

1. **Расчет потерь эффективности**



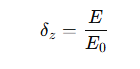
Подставляем значения:



Это означает, что в результате несанкционированного доступа эффективность объекта снизилась на 3 000 единиц.

1. **Расчет относительной эффективности объекта после защиты**

Согласно формуле:



Подставляем значения:

Изображение выглядит как Шрифт, текст, линия, дизайн

Контент, сгенерированный ИИ, может содержать ошибки.

Это означает, что после внедрения защиты объект сохраняет 80% своей исходной эффективности.

1. **Расчет суммарного ущерба объекта**

Согласно формуле:

Изображение выглядит как Шрифт, белый, линия, символ

Контент, сгенерированный ИИ, может содержать ошибки.

Подставляем значения:

Изображение выглядит как Шрифт, текст, белый, типография

Контент, сгенерированный ИИ, может содержать ошибки.

Таким образом, общий ущерб объекта составляет 2 500 единиц, включая стоимость защитных мер.

**Вывод**

В ходе выполнения практической работы были проведены расчёты ущерба от несанкционированного доступа, а также эффективности защитных мер с применением математических моделей. Полученные данные показывают, что внедрение защиты позволяет объекту сохранить 80% своей исходной эффективности. Однако даже при наличии защитных мер суммарный ущерб объекта составляет 2 500 единиц, что важно учитывать при разработке систем безопасности.

Применённые методы расчёта позволяют оценить целесообразность использования защитных средств и их влияние на эффективность функционирования объекта.

Практическое занятие №3

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-КОМПАНИИ(БОЛЬНИЦА)

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Введение**

В современном мире медицинские учреждения сталкиваются с множеством угроз информационной безопасности, что требует комплексного и системного подхода к обеспечению защиты данных. Особенно важно учитывать, что медицинская информация является одной из наиболее конфиденциальных категорий данных, поскольку она включает в себя персональные сведения о пациентах, историю их лечения, медицинские заключения и иные сведения, которые не подлежат разглашению.

Любая утечка данных может привести к серьезным последствиям, включая нарушение врачебной тайны, потерю доверия пациентов и даже юридическую ответственность медицинского учреждения. В связи с этим разработка и внедрение политики информационной безопасности является необходимым шагом для предотвращения угроз, а также для эффективного реагирования на возможные инциденты.

Цель данной работы – разработка политики информационной безопасности для больницы, включающей основные угрозы, оценку рисков и меры защиты. В рамках данной политики рассматриваются механизмы обеспечения безопасности данных, такие как управление доступом, контроль сетевого трафика, резервное копирование, использование антивирусных средств и проведение обучающих мероприятий для персонала.

Данный документ представляет собой структурированный анализ всех аспектов информационной безопасности в медицинском учреждении и дает рекомендации по внедрению эффективных мер защиты. Политика информационной безопасности должна быть ориентирована на долгосрочную перспективу и учитывать возможные изменения в законодательстве, развитие технологий и появление новых угроз. Только системный подход позволит обеспечить надёжную защиту данных и создать безопасную цифровую среду в медицинском учреждении.

**2. Описание структуры больницы**

Современные медицинские учреждения представляют собой сложные организационные структуры, в которых осуществляется постоянный обмен данными между различными подразделениями. Больница включает в себя следующие подразделения:

* **Приёмное отделение** – занимается первичным осмотром и регистрацией пациентов, оформлением медицинской документации и направлением пациентов в соответствующие отделения.
* **Терапевтическое отделение** – обеспечивает амбулаторное лечение пациентов, диагностику заболеваний, ведение истории болезни и медицинских карт.
* **Хирургическое отделение** – проводит хирургические вмешательства и послеоперационный уход, требующий особой точности в обработке и хранении данных пациентов.
* **Реанимация** – специализированное отделение интенсивной терапии, где ведётся круглосуточный мониторинг пациентов, использующий медицинские приборы с интегрированными цифровыми системами.
* **Лаборатория** – выполняет диагностику заболеваний на основе лабораторных исследований, результаты которых должны храниться в защищённой базе данных.
* **Аптека** – отвечает за хранение и выдачу лекарственных препаратов, ведение электронных записей о движении медикаментов и интеграцию с другими системами больницы.
* **Администрация** – управляет финансовыми, кадровыми и юридическими вопросами учреждения, осуществляет бухгалтерский учет и формирует отчёты.
* **IT-отдел** – обеспечивает техническую поддержку всех информационных систем больницы, внедряет новые технологии защиты данных и контролирует сетевую безопасность.

Эффективное взаимодействие этих подразделений возможно только при надёжной системе информационной безопасности, минимизирующей риски несанкционированного доступа, утечек и сбоев в работе системы.

**3. Оценка рисков**

Классификация угроз информационной безопасности в больнице включает широкий спектр потенциальных рисков, с которыми может столкнуться медицинское учреждение:

* 1. **Несанкционированный доступ**
  + Проникновение злоумышленников в сеть больницы с целью кражи данных.
  + Использование слабых паролей сотрудниками.
  + Нарушение регламентов хранения информации.
  + Перехват сетевого трафика при недостаточной защите соединений.
  + Доступ к системам через уязвимости в устаревшем ПО.
  1. **Программные угрозы**
  + Вирусные атаки и вредоносные программы.
  + Использование устаревшего и уязвимого программного обеспечения.
  + Отсутствие регулярных обновлений и патчей безопасности.
  + Эксплуатация уязвимостей в операционных системах и сервисах.
  + Атаки типа «отказ в обслуживании» (DDoS) на критически важные сервисы больницы.
  1. **Аппаратные угрозы**
  + Выход из строя серверного оборудования.
  + Кража физических носителей информации.
  + Поломка рабочих станций и медицинского оборудования.
  + Неконтролируемый доступ к аппаратным средствам хранения данных.
  + Недостаточная резервная мощность серверов при пиковых нагрузках.
  1. **Человеческий фактор**
  + Ошибки сотрудников при работе с медицинской информацией.
  + Несоблюдение правил конфиденциальности.
  + Незнание основ информационной безопасности.
  + Использование личных устройств для работы с конфиденциальными данными.
  + Непреднамеренное удаление или изменение критически важных данных.
  1. **Социальная инженерия**
  + Фишинговые атаки.
  + Манипуляции, направленные на получение паролей.
  + Введение персонала в заблуждение для передачи критически важных данных.
  + Ложные звонки или письма от лиц, выдающих себя за руководство.
  + Использование соцсетей для сбора информации о персонале и организации атак.
  1. **Физическая безопасность**
  + Несанкционированный доступ к серверным комнатам.
  + Кража или подмена носителей информации.
  + Разрушение данных вследствие пожара, затопления или других чрезвычайных ситуаций.
  + Недостаточная защита от электромагнитных помех и внешних воздействий.
  1. **Внутренние угрозы**
  + Намеренные действия сотрудников, направленные на повреждение или утечку данных.
  + Конфликты внутри коллектива, приводящие к нарушению информационной безопасности.
  + Неконтролируемое копирование и распространение конфиденциальной информации.
  + Неавторизованное подключение сторонних устройств к внутренней сети больницы.
  1. **Правовые и регуляторные угрозы**
  + Нарушение требований законодательства о защите персональных данных.
  + Несоответствие внутренней политики безопасности требованиям государственных регуляторов.
  + Ненадлежащее ведение документации и журналов безопасности.
  + Недостаточный уровень подготовки сотрудников в области соблюдения правовых норм.

**4. Разработка мер защиты**

**4.1. Несанкционированный доступ**

* Внедрение многофакторной аутентификации (MFA) для всех сотрудников.
* Регулярное обновление паролей и использование сложных комбинаций.
* Шифрование сетевого трафика с использованием VPN и TLS.

**4.2. Программные угрозы**

* Использование актуального антивирусного ПО и систем обнаружения вторжений (IDS/IPS).
* Регулярное обновление операционных систем и установленного ПО.
* Разделение сетевого доступа для критически важных сервисов.

**4.3. Аппаратные угрозы**

* Создание резервных копий данных и настройка их автоматического обновления.
* Ограничение физического доступа к серверам и рабочим станциям (карточная система, видеонаблюдение).
* Использование ИБП (источников бесперебойного питания) для защиты от сбоев электропитания.

**4.4. Человеческий фактор**

* Проведение регулярного обучения персонала по вопросам информационной безопасности.
* Ограничение доступа сотрудников к данным на основе их должностных обязанностей (принцип минимально необходимого доступа).
* Разработка четких инструкций по работе с конфиденциальной информацией.

**4.5. Социальная инженерия**

* Фильтрация электронной почты для выявления фишинговых сообщений.
* Организация тренингов для сотрудников по выявлению попыток манипуляций.
* Введение политики запрета на передачу конфиденциальных данных по телефону или электронной почте без подтверждения личности.

**4.6. Физическая безопасность**

* Использование замков, биометрической аутентификации и систем видеонаблюдения в серверных помещениях.
* Хранение резервных носителей информации в защищенных сейфах.
* Разработка плана действий на случай пожара, наводнения и других чрезвычайных ситуаций.

**4.7. Внутренние угрозы**

* Мониторинг действий сотрудников в критически важных системах.
* Ограничение копирования и передачи конфиденциальных данных (DLP-системы).
* Запрет на использование личных устройств в корпоративной сети без разрешения.

**4.8. Правовые и регуляторные угрозы**

* Регулярные внутренние аудиты на соответствие законодательным требованиям.
* Разработка и внедрение политики информационной безопасности в соответствии с нормативными актами.
* Проведение обязательного обучения сотрудников по соблюдению норм защиты персональных данных.

**5. Выводы**

Таким образом, информационная безопасность в медицинском учреждении – это не просто отдельный аспект управления, а фундаментальная составляющая эффективного функционирования больницы. Современные угрозы, включая кибератаки, утечку данных и человеческий фактор, требуют тщательного подхода к защите информации, что достигается за счет комплексной политики безопасности, внедрения современных технологий защиты и регулярного обучения персонала.

В ходе исследования были определены основные угрозы, которым подвержена больница, и разработаны меры их предотвращения. Несанкционированный доступ, вредоносные программы, аппаратные сбои и социальная инженерия представляют серьезную угрозу не только для данных пациентов, но и для всей системы здравоохранения. В связи с этим важную роль играет не только внедрение защитных инструментов, но и разработка внутренних регламентов, направленных на минимизацию рисков.

Реализация предложенных мер, таких как многофакторная аутентификация, мониторинг сетевого трафика, резервное копирование, строгая политика управления доступом, применение антивирусных решений и повышение осведомленности персонала, позволит снизить вероятность инцидентов и создать безопасную среду для работы с медицинскими данными.

Кроме того, информационная безопасность не является статичной системой – она должна регулярно пересматриваться и адаптироваться к изменяющимся условиям, новым видам угроз и технологическим достижениям. Это требует постоянного взаимодействия между IT-специалистами, администрацией и медицинским персоналом.

Таким образом, разработка и внедрение политики информационной безопасности является ключевым фактором успешного функционирования медицинского учреждения. Обеспечение надежной защиты данных способствует не только выполнению нормативных требований, но и укреплению доверия пациентов, повышению эффективности работы больницы и улучшению качества оказываемых медицинских услуг. Долговременная стратегия защиты информации является важным условием для стабильного функционирования больницы в условиях цифровой трансформации медицины.

Также необходимо учитывать, что безопасность данных – это процесс, требующий постоянного совершенствования. Современные технологии быстро развиваются, появляются новые типы атак, поэтому больница должна быть готова оперативно реагировать на возникающие угрозы. Внедрение политики информационной безопасности способствует снижению рисков, повышению уровня защищённости данных и созданию эффективной инфраструктуры для хранения и обработки медицинской информации.

В конечном итоге надёжная защита данных – это не просто формальная необходимость, а залог качественного медицинского обслуживания, безопасности пациентов и успешной работы всего медицинского учреждения. Эффективная политика информационной безопасности позволяет не только предотвращать потенциальные угрозы, но и формировать культуру безопасного обращения с данными среди сотрудников, что в свою очередь делает больницу более устойчивой к вызовам цифровой эпохи.

**Использованные источники**

1. Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (с изменениями и дополнениями).
2. Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».
3. Постановление Оперативно-Аналитического центра при Президенте Республики Беларусь от 14.12.2018 № 66 «Об утверждении требований по обеспечению защиты информации».
4. ТКП 17.03-04-2019 (33150) «Информационные технологии и безопасность. Защита информации. Порядок проведения оценки соответствия».
5. ISO/IEC 27001:2022 — международный стандарт информационной безопасности.
6. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations.
7. OWASP Foundation. "Top Ten Security Risks" (https://owasp.org/www-project-top-ten/).
8. Герасимов А.В., Сидорова Е.П. «Информационная безопасность организаций: угрозы, методы защиты, правовое регулирование» — Минск: БГУИР, 2021.
9. Кузнецов М.А., Соловьев Д.А. «Информационная безопасность: угрозы, защита, правовые аспекты» — М.: Бином, 2021.
10. Васильев А.А., Гаврилов С.П. «Кибербезопасность в здравоохранении» — СПб.: Питер, 2020.
11. Статья в журнале "Компьютерные системы и сети": Иванов И.И. «Современные угрозы информационной безопасности в медицинских учреждениях» // №4, 2023.

Практическое занятие №4

НАСТРОЙКА БРАНДМАУЭРА WINDOWS

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия**

Овладеть навыками настройки и использования брандмауэра Windows для обеспечения безопасности системы.

**Краткие теоретические сведения**

Брандмауэр (межсетевой экран) — это программное или аппаратное средство, которое контролирует входящий и исходящий трафик на основе заданных правил безопасности. Он позволяет предотвратить несанкционированный доступ к компьютеру и защищает его от различных угроз.

**Принципы работы брандмауэра:**

1. **Фильтрация трафика:** Брандмауэр проверяет пакеты данных и принимает решение о их разрешении или блокировке.
2. **Правила доступа:** Настройки брандмауэра определяют, какие приложения могут получать доступ к сети и какие соединения могут быть установлены.
3. **Мониторинг активности:** Брандмауэр ведет учет сетевой активности, что позволяет выявлять подозрительные действия.

**Условие задания**

1. Включить брандмауэр Windows.
2. Настроить правила для входящих и исходящих подключений.
3. Создать правила для блокировки и разрешения подключения для выбранной программы.

**Исполнительская часть**

**Шаг 1: Включение брандмауэра Windows**

1. Откройте «Панель управления» через меню «Пуск».
2. Перейдите в раздел «Система и безопасность».
3. Выберите «Брандмауэр Windows».
4. В левой части окна выберите «Включение и отключение брандмауэра Windows».
5. Убедитесь, что брандмауэр включен для всех сетевых подключений.

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

**Шаг 2: Настройка правил для входящих и исходящих подключений**

1. В меню «Брандмауэр Windows» выберите «Дополнительные параметры».
2. В разделе «Правила для входящих подключений» создайте новое правило:
   * Нажмите «Создать правило».
   * Выберите «Для программы» и укажите путь к исполняемому файлу.
   * Выберите действие (разрешить или блокировать).
   * Завершите настройку правила

**Блокировка входящего подключения:**

.Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Разрешение входящего подключения:**

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Правила для входящего подключения:**

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

**Блокировка исходящего подключения**

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Разрешение исходящего подключения:**  
Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

**Правила для исходящего подключения:**

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

**Выполнение команды control admintools:**  
Изображение выглядит как текст, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

При выполнении открывается следующее окно:  
Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Контент, сгенерированный ИИ, может содержать ошибки.

**Выполнение команды dxdiag:**

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Открывается следующее окно:  
Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Выполнение команды diskmgmt.msc:**  
Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Открывает следующее окно:  
Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Заключение**

В ходе выполнения практической работы была успешно настроена работа брандмауэра Windows. Были созданы правила для входящих и исходящих подключений, обеспечивающие защиту системы от несанкционированного доступа. Овладение навыками работы с брандмауэром является важным шагом в обеспечении информационной безопасности.

**Использованные источники**

1. Документация Microsoft по настройке брандмауэра Windows.
2. Учебное пособие по основам защиты информации.

Практическое занятие №5

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель работы:**

Овладение основными криптографическими алгоритмами симметричного и асимметричного шифрования, их применение для защиты данных и проверки целостности информации.

**Теоретические сведения**

**Криптография и ее задачи**

Криптография – это наука о методах защиты информации от несанкционированного доступа путем шифрования и хеширования. Основные задачи криптографии:

* **Конфиденциальность** – защита данных от несанкционированного доступа.
* **Целостность** – предотвращение изменения данных без обнаружения.
* **Аутентификация** – подтверждение подлинности отправителя.
* **Неотрекаемость** – невозможность отказа от факта отправки сообщения.

**Алгоритмы шифрования**

Существует два основных типа криптографических систем:

1. **Симметричное шифрование** – один и тот же ключ используется как для шифрования, так и для расшифрования.
   * **Преимущества:** высокая скорость работы.
   * **Недостатки:** сложность безопасного обмена ключами.
   * **Примеры алгоритмов:** AES, DES, Triple DES.
2. **Асимметричное шифрование** – используются два ключа: открытый (для шифрования) и закрытый (для расшифрования).
   * **Преимущества:** безопасный обмен ключами.
   * **Недостатки:** низкая скорость работы.
   * **Примеры алгоритмов:** RSA, Diffie-Hellman, ElGamal.

**Алгоритм RSA (512 бит)**

RSA – один из самых известных алгоритмов асимметричного шифрования. Он основан на сложности факторизации больших чисел.  
**Принцип работы RSA:**

1. Генерируется пара ключей: **открытый ключ (public key)** и **закрытый ключ (private key)**.
2. Сообщение шифруется с помощью открытого ключа.
3. Расшифрование возможно только с использованием закрытого ключа.

Формулы RSA:

* **Шифрование:** C=Memod  NC = M^e \mod NC=MemodN
* **Расшифрование:** M=Cdmod  NM = C^d \mod NM=CdmodN  
  где:
* MMM – исходное сообщение,
* CCC – зашифрованное сообщение,
* eee – открытая экспонента,
* ddd – секретная экспонента,
* NNN – модуль (произведение двух простых чисел).

**Хеширование и алгоритм MD5**

Хеширование – это процесс получения уникального цифрового отпечатка (хеша) данных фиксированной длины.

**Принцип работы MD5:**

1. Сообщение разбивается на блоки по 512 бит.
2. Каждый блок обрабатывается функцией сдвигов и нелинейных преобразований.
3. В результате получается хеш длиной **128 бит (32 шестнадцатеричных символа)**.

**Недостатки MD5:**

* Уязвимость к коллизиям (разные сообщения могут давать одинаковый хеш).
* Не рекомендуется для критически важных приложений.

**Применение криптографии**

* **Безопасная передача данных в интернете (SSL/TLS).**
* **Электронная цифровая подпись (ЭЦП).**
* **Шифрование файлов и сообщений.**
* **Защита паролей в базах данных.**

**Задание для выполнения**

1. Изучите теоретические сведения по данной теме.

2. Зашифруйте сообщение с использованием нижеперечисленных шифров и полученного секретного ключа (по номеру варианта (см. номер студента в журнале группы) и ключевому слову «Защита»):

− шифр Цезаря;

− шифр Трисемуса;

− шифр Плейфейра;

− шифр Виженера.

В качестве сообщения используйте свое полное имя (Фамилия Имя Отчество).

3. Расшифруйте сообщения по индивидуальному заданию.

|  |  |  |
| --- | --- | --- |
| Номер Варианта | Сообщение | Способ |
| 4 | Лжбзеииеизиачзнр | Расшифровать с помощью магического квадрата   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |

**Выполнение задания:**

**2** Васильев Владислав Васильевич

Ключ: 4

**Шифр Цезаря**

Исходный алфавит

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Ж | З | И | Й | К | Л | М |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| Н | О | П | Р | С | Т | У |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| Ф | Ч | Ц | Ч | Ш | Щ | Ъ |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| Ы | Ь | Э | Ю | Я |
| 29 | 30 | 31 | 32 | 33 |

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Исходная позиция | Новая позиция(+4) | Зашифрованная буква |
| В | 3 | 7 | Ж |
| А | 1 | 5 | Д |
| С | 19 | 23 | Х |
| И | 10 | 14 | М |
| Л | 13 | 17 | П |
| Ь | 30 | 34 -> 1 | А |
| Е | 6 | 10 | И |
| В | 3 | 7 | Ж |

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Исходная позиция | Новая позиция(+4) | Зашифрованная буква |
| В | 3 | 7 | Ж |
| Л | 13 | 17 | П |
| А | 1 | 5 | Д |
| Д | 5 | 9 | З |
| И | 10 | 14 | М |
| С | 19 | 23 | Х |
| Л | 13 | 17 | П |
| А | 1 | 5 | Д |
| В | 3 | 7 | Ж |

|  |  |  |  |
| --- | --- | --- | --- |
| Буква | Исходная позиция | Новая позиция(+4) | Зашифрованная буква |
| В | 3 | 7 | Ж |
| А | 1 | 5 | Д |
| С | 19 | 23 | Х |
| И | 10 | 14 | М |
| Л | 13 | 17 | П |
| Ь | 30 | 34 -> 1 | А |
| Е | 6 | 10 | И |
| В | 3 | 7 | Ж |
| И | 10 | 14 | М |
| Ч | 26 | 30 | Ь |

Готовый результат: ВАСИЛЬЕВ ВЛАДИСЛАВ ВАСИЛЬЕВИЧ ––>

* + ЖДХМПАИЖ ЖПДЗМХПДЖ ЖДХМПАИЖМЬ

**Шифр Трисемуса**

Ключевое слово: Защита

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| З | А | Щ | И | Т | Б | В | Г |
| Д | Е | Ж | Й | К | Л | М | Н |
| О | П | Р | С | У | Ф | Х | Ц |
| Ч | Ш | Ъ | Ы | Ь | Э | Ю | Я |

Готовый результат: ВАСИЛЬЕВ ВЛАДИСЛАВ ВАСИЛЬЕВИЧ ––>

МЕЫЙФТПМ МФЕОЙЫФЕМ МЕЫЙФТПМЙЗ

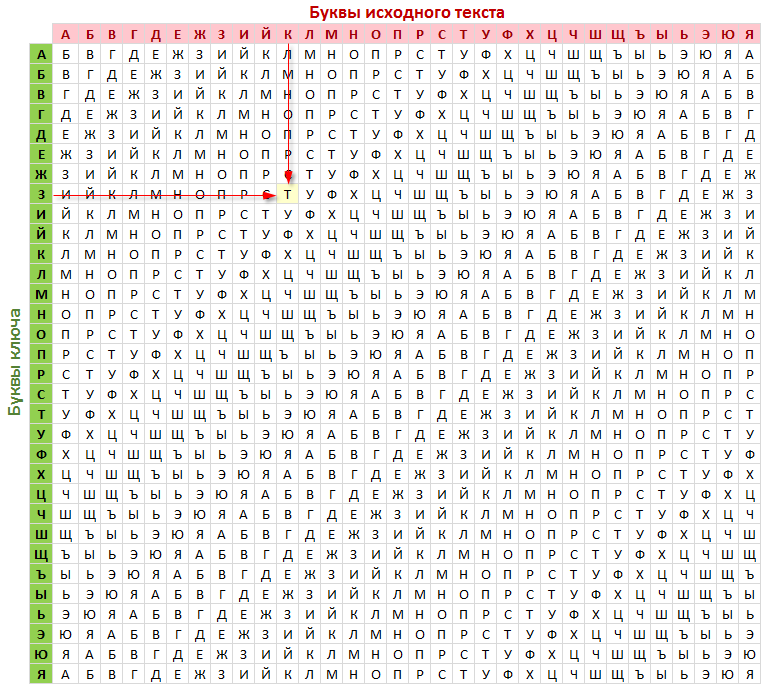
**Шифр Плейфейра**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| З | А | Щ | И | Т | Б | В | Г |
| Д | Е | Ж | Й | К | Л | М | Н |
| О | П | Р | С | У | Ф | Х | Ц |
| Ч | Ш | Ъ | Ы | Ь | Э | Ю | Я |

ВА-СИ-ЛЬ-ЕВ-ВЛ-АД-ИС-ЛА-ВЪ-ВА-СИ-ЛЬ-ЕВ-ИЧ

ГЩ-ЫЙ-КЭ-МА-БМ-ЗЕ-ЙЫ-ЕБ-ЩЮ-ГЩ-ЫЙ-КЭ-МА-ЗЫ

**Шифр Вижинера**



ВАСИЛЬЕВ ВЛАДИСЛАВ ВАСИЛЬЕВИЧ 27 символов

ЗАЩИТАЗА ЩИТАЗАЩИТ АЗАЩИТАЗАЩ

|  |  |  |
| --- | --- | --- |
| В | З | К |
| А | А | Б |
| С | Щ | Л |
| И | И | С |
| Л | Т | Ю |
| Ь | А | Э |
| Е | З | Н |
| В | А | Г |

|  |  |  |
| --- | --- | --- |
| В | Щ | Ь |
| Л | И | Ф |
| А | Т | У |
| Д | А | Е |
| И | З | Р |
| С | А | Т |
| Л | Щ | Е |
| А | И | Й |
| В | Т | Х |

|  |  |  |
| --- | --- | --- |
| В | А | Г |
| А | З | И |
| С | А | Т |
| И | Щ | В |
| Л | И | Ф |
| Ь | Т | П |
| Е | А | Ж |
| В | З | К |
| И | А | Й |
| Ч | Щ | С |

Полученное зашифрованное сообщение:  
КБЛСЮЭНГ ЬФУЕРТЕЙХ ГИТВФПЖКЙС

3. Расшифруйте сообщения по индивидуальному заданию.

|  |  |  |
| --- | --- | --- |
| Номер Варианта | Сообщение | Способ |
| 4 | Лжбзеииеизиачзнр | Расшифровать с помощью магического квадрата   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |

ЛЖБЗ ЕИИЕ ИЗИА ЧЗНР

|  |  |  |  |
| --- | --- | --- | --- |
| 7 Л | 12 Ж | 1 Б | 14 З |
| 2 Е | 13 И | 8 И | 11 Е |
| 16 И | 3 З | 10 И | 5 А |
| 9 Ч | 6 З | 15 Н | 4 Р |

Расшифрованное сообщение:  
БЕЗРАЗЛИЧИЕ ЖИЗНИ

**Использованные источники**

1. Соловьев В. И. Основы криптографии. — М.: Издательство МГТУ, 2020.
2. Шеннон К. Работы по теории информации и кибернетике. — М.: Мир, 1963.
3. Кнут Д. Искусство программирования. Том 2: Получисленные алгоритмы. — М.: Вильямс, 2007.
4. Столбов С. Н. Методы и средства защиты информации. — СПб.: Питер, 2019.
5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая.
6. Официальная документация по криптографическим алгоритмам [Электронный ресурс]. Доступ: <https://cryptography.io>
7. История и принципы работы шифров Цезаря, Вижинера, Плейфера и магических квадратов [Электронный ресурс]. Доступ: <https://crypto-history.com>

Практическое занятие №6

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

С ПОМОЩЬЮ АЛГОРИТМОВ АСИММЕТРИЧНОГО

ШИФРОВАНИЯ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия**

Изучение принципов работы алгоритмов асимметричного шифрования, включая алгоритм RSA, алгоритм Диффи – Хеллмана и алгоритм Эль-Гамаля.

**Теоретические сведения**

Асимметричное шифрование – это метод криптографической защиты, при котором используются два ключа: открытый (публичный) и закрытый (приватный). Открытый ключ применяется для шифрования данных, а закрытый – для их расшифровки. Такие алгоритмы широко применяются в безопасном обмене данными, цифровых подписях и аутентификации пользователей.

**Условие задания**

1. Объяснить процесс работы алгоритма RSA.
2. Объяснить процесс работы алгоритма Диффи – Хеллмана.
3. Объяснить процесс работы алгоритма Эль-Гамаля.

**Исполнительская часть**

**1. Процесс работы алгоритма RSA**

Алгоритм RSA основан на сложности факторизации больших чисел. Он включает следующие этапы:

1. Генерация ключей:
   * Выбираются два больших простых числа ***p*** и ***q*** .
   * Вычисляется их произведение ***n = p \* q***, которое используется в открытом и закрытом ключах.
   * Вычисляется значение функции Эйлера



* + Выбирается открытая экспонента ***e***, которая является взаимно простым числом с  .
  + Вычисляется закрытая экспонента ***d*** как модульное обратное ***e*** по модулю .

1. Шифрование:
   * Сообщение ***M*** преобразуется в числовой формат.
   * Вычисляется зашифрованное сообщение:  .
2. Расшифрование:
   * Вычисляется исходное сообщение: .

**2. Процесс работы алгоритма Диффи – Хеллмана**

Алгоритм Диффи – Хеллмана позволяет двум сторонам создать общий секретный ключ через незащищённый канал связи:

1. Договорённость о параметрах:
   * Выбирается большое простое число ***p*** и первообразный корень ***g*** по модулю ***p***.
2. Генерация закрытых ключей:
   * Сторона A выбирает случайное число ***a*** и вычисляет

.

* + Сторона B выбирает случайное число ***b*** и вычисляет

.

1. Обмен данными:
   * A отправляет ***A*** стороне B.
   * B отправляет ***B*** стороне A.
2. Вычисление общего ключа:
   * A вычисляет

.

* + B вычисляет

.

* + Оба значения совпадают, так как

.

**3. Процесс работы алгоритма Эль-Гамаля**

Алгоритм Эль-Гамаля основан на сложности задачи дискретного логарифмирования:

1. Генерация ключей:
   * Выбирается большое простое число ***p*** и первообразный корень ***g***.
   * Выбирается случайное число ***x*** (закрытый ключ).
   * Вычисляется Изображение выглядит как Шрифт, типография, текст, каллиграфия

     Контент, сгенерированный ИИ, может содержать ошибки. (открытый ключ).
2. Шифрование:
   * Выбирается случайное число ***k***.
   * Вычисляются два значения:
     + 
     + 
   * Пара ***(C1, C2)*** передаётся получателю.
3. Расшифрование:
   * Получатель вычисляет

, используя закрытый ключ .

**Использованные источники**

1. Уильям Ста́ллингс. "Криптография и защита сетей".
2. Ривест Р., Шамир А., Адлеман Л. "Методы шифрования на основе сложности факторизации".
3. Учебные материалы курса.
4. Веб-ресурсы .

Практическое занятие №7

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия**  
Целью данного занятия является получение практических знаний и навыков по использованию методов криптографии для создания и проверки электронной цифровой подписи (ЭЦП). В ходе выполнения задания будет рассмотрен алгоритм RSA, который является основой многих современных криптографических систем. Особое внимание будет уделено теоретическим аспектам и пошаговому объяснению процедур, а также реальной реализации ЭЦП с использованием данного алгоритма.

**Краткие теоретические сведения**

Электронная цифровая подпись (ЭЦП) — это криптографический механизм, который используется для проверки подлинности и целостности данных. ЭЦП основывается на принципах асимметричного шифрования, где используется пара ключей: один — для подписания, второй — для проверки подписи. Асимметричные алгоритмы позволяют обеспечить высокую степень безопасности, поскольку для шифрования данных используется один ключ, а для их расшифровки — другой.

Алгоритм RSA (Ривест, Шамир, Адлеман) является одним из самых популярных асимметричных алгоритмов шифрования. Он основан на сложности факторизации больших чисел. Основной принцип работы алгоритма заключается в генерации пары ключей, которая используется для шифрования и расшифрования данных или для создания и проверки подписи.

Процесс подписания с помощью RSA включает два этапа:

1. Генерация хэш-суммы сообщения.
2. Подписание хэш-суммы с использованием закрытого ключа.

Для проверки подписи отправитель должен использовать свой открытый ключ. Если хэш-сумма, полученная при расшифровке подписи, совпадает с хэш-суммой сообщения, то подпись считается верной.

**Условие задания**

1. Объяснить последовательность выполнения процедур генерации и проверки ЭЦП.
2. Описать последовательность действий участников протокола при отправке и проверке ЭЦП.
3. Описать схему протокола ЭЦП на основе алгоритма RSA.

**Исполнительная часть**

1. **Процесс генерации и проверки ЭЦП**

Процесс создания и проверки ЭЦП состоит из нескольких ключевых этапов:

1. Генерация ключей:
   * На первом этапе генерируются два ключа: закрытый и открытый. Закрытый ключ используется для подписания, а открытый — для проверки подписи. Ключи генерируются с использованием алгоритма RSA, который включает в себя выбор двух больших простых чисел, вычисление их произведения и применение других математических операций.
   * Генерация происходит следующим образом:
     + Выбираются два больших простых числа ***p*** и ***q***.
     + Вычисляется их произведение ***n = p × q***, которое используется в качестве модуля для открытого и закрытого ключей.
     + Вычисляется функция Эйлера ***ϕ(n)=(p−1)(q−1)***
     + Далее выбирается число ***e***, которое должно быть взаимно простым с ***ϕ(n).***
     + Вычисляется ***d***, которое является мультипликативной инверсией ***e*** по модулю ***ϕ(n).***
   * Таким образом, открытый ключ состоит из пары (e, n), а закрытый — из пары (d, n).
2. Генерация подписи:
   * Для того чтобы подписать сообщение, сначала нужно вычислить его хэш-сумму, используя криптографическую хеш-функцию (например, SHA-256). Хэш-сумма — это фиксированная длина строки, которая уникально представляет собой содержимое сообщения.
   * После того как хэш-сумма сообщения вычислена, она подписывается закрытым ключом отправителя. Подпись — это результат шифрования хэш-суммы с использованием закрытого ключа.
   * Подписанное сообщение отправляется получателю вместе с подписью.
3. Проверка подписи:
   * Получатель получает сообщение и подпись. Чтобы проверить подпись, он использует открытый ключ отправителя.
   * Сначала получатель вычисляет хэш-сумму из полученного сообщения.
   * Затем он расшифровывает подпись с помощью открытого ключа отправителя. Полученная при этом хэш-сумма должна совпасть с хэш-суммой сообщения.
   * Если хэш-суммы совпадают, это подтверждает подлинность подписи.
4. **Действия участников протокола**
5. **Отправитель**:
   * Отправитель генерирует пару ключей с использованием алгоритма RSA.
   * Создает хэш-сумму сообщения с помощью криптографической хеш-функции.
   * Подписывает хэш-сумму закрытым ключом.
   * Отправляет сообщение и подпись получателю.
6. **Получатель**:
   * Получает сообщение и подпись.
   * Вычисляет хэш-сумму из полученного сообщения.
   * Расшифровывает подпись с помощью открытого ключа отправителя.
   * Сравнивает полученную хэш-сумму с вычисленной. Если они совпадают, то сообщение и подпись являются подлинными.
7. **Схема протокола ЭЦП на основе алгоритма RSA**

Протокол ЭЦП может быть представлен следующими этапами:

1. **Генерация ключей**:
   * Отправитель генерирует пару ключей: (e, n) — открытый, (d, n) — закрытый.
2. **Создание подписи**:
   * Отправитель вычисляет хэш-сумму сообщения.
   * Отправитель подписывает хэш-сумму с использованием закрытого ключа.
3. **Отправка сообщения**:
   * Отправитель отправляет сообщение и подпись получателю.
4. **Проверка подписи**:
   * Получатель вычисляет хэш-сумму сообщения.
   * Получатель расшифровывает подпись с использованием открытого ключа отправителя.
   * Если хэш-сумма совпадает, сообщение считается подлинным.

**Использованные источники**

1. Криптографический стандарт RSA, <https://www.rsa.com>
2. Учебник "Криптография и безопасность информации",
3. Официальная документация библиотеки PyCryptodome, <https://www.pycryptodome.org>
4. Статья "Как работает RSA и его применение в криптографии".

Практическое занятие №8

ТЕОРИЯ ЧИСЕЛ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель работы:**  
Изучить основные понятия теории чисел, освоить методы вычисления наибольшего общего делителя (НОД) с использованием алгоритма Евклида и его расширенной версии, а также применить понятие сравнений по модулю и малую теорему Ферма для решения задач, связанных с разложением чисел на простые множители и поиском остатков от деления.

**Краткие теоретические сведения:**

1. **Арифметические операции и свойства целых чисел:**
   * Множество целых чисел ℤ содержит 0, положительные и отрицательные числа.
   * На ℤ определены операции сложения и умножения, обладающие свойствами ассоциативности, коммутативности, дистрибутивности, а также наличием нейтральных элементов (0 и 1).
2. **Деление с остатком и позиционные системы счисления:**
   * Теорема о делении с остатком утверждает, что для любых целых чисел a и b (b ≠ 0) существуют единственные числа q и r, такие что a = b⋅q + r, где 0 ≤ r < |b|.
   * Это основание для записи чисел в позиционных системах счисления, где число представляется в виде суммы цифр, умноженных на соответствующие степени основания.
3. **Наибольший общий делитель (НОД) и алгоритм Евклида:**
   * НОД(a, b) – наибольший общий делитель чисел a и b.
   * Алгоритм Евклида позволяет найти НОД посредством последовательного вычисления остатков от деления, а его расширенная версия даёт возможность выразить НОД через линейную комбинацию a и b (соотношение Безу).
4. **Простые числа и каноническое разложение:**
   * Простое число p > 1 делится только на 1 и на себя.
   * Теорема о бесконечности простых чисел (Евклида) утверждает, что простых чисел бесконечно много.
   * Каждое натуральное число n > 1 может быть представлено в виде произведения простых множителей (каноническое разложение).
5. **Сравнения по модулю и малая теорема Ферма:**
   * Два целых числа называются сравнимыми по модулю m, если они дают одинаковый остаток при делении на m (записывается как a ≡ b (mod m)).
   * Малая теорема Ферма утверждает, что если p — простое число и a не делится на p, то a^(p–1) ≡ 1 (mod p). Это свойство позволяет быстро находить остатки от деления больших чисел на простые.

**Условие задания**

1. Найдите канонические разложения чисел а и b.

2. Найдите НОД (а, b) пользуясь:

a) алгоритмом Евклида;

б) разложением чисел на простые множители.

3. С помощью расширенного алгоритма Евклида найдите целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД(а, b).

4. Найдите остаток от деления данного числа на простое.

|  |  |
| --- | --- |
| Номер варианта | Задание |
| 4 | 1–3. а = 9002242397, b = 433817903.  4. Найти остаток от деления 20042998 на 19 |

**Исполнительная часть**

1. a = 9 002 242 397 = 73 \* 123 318 389 = 732 \* 1 689 293 = 733 \* 23 141 =

= 734 \* 317

b = 433 817 903 = 73 \* 5 942 711 = 732 \* 81 407 = 732 \* 127 \* 641

1. а)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | u | v | r |  |
| a | 1 | 0 | 9 002 242 397 | q |
| b | 0 | 1 | 433 817 903 | 20 |
| a - bq |  |  | 325 884 337 | 1 |
|  |  |  | 107 933 566 | 3 |
|  |  |  | 2 083 639 | 51 |
|  |  |  | 1 667 977 | 1 |
|  |  |  | 415 662 | 4 |
|  |  |  | 5 329 | 78 |
|  |  |  | 0 |  |

(9 002 242 397, 433 817 903) = 5329

б) (9 002 242 397, 433 817 903) = 73 \* 73 = 5329

3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | u | v | r |  |
| a | 1 | 0 | 9 002 242 397 | q |
| b | 0 | 1 | 433 817 903 | 20 |
| a - bq | 1 | -20 | 325 884 337 | 1 |
|  | -1 | 21 | 107 933 566 | 3 |
|  | 4 | -83 | 2 083 639 | 51 |
|  | -205 | 4254 | 1 667 977 | 1 |
|  | 209 | -4337 | 415 662 | 4 |
|  | -1041 | 21602 | 5 329 | 78 |
|  |  |  | 0 |  |

a\*u + b\*v = r

9 002 242 397 \* (-1041) + 433 817 903 \* 21602 = 5 329

5 329 = 5 329

u = -1041

v = 21602

4

X ≡ 20042998 (mod 19)

2004 ≡ 9(mod 19)

X ≡ 92998 (mod 19) 9ф(m) ≡ 1 (mod m)

Ф(19) = 18 918 ≡ 1 (mod 19)

2998≡ 1 (mod 19)

X ≡ (918 )166 \* 910(mod 19)

X ≡ 910(mod 19)

X ≡ 81 \* 81 \* 81 \* 81 \* 81(mod 19) 81≡ 5 (mod 19)

X ≡ 5 \* 5 \* 5 \* 5 \* 5(mod 19)

X ≡ 55(mod 19)

X ≡ 252 \* 5(mod 19) 25≡ 6 (mod 19)

X ≡ 62 \* 5(mod 19)

X ≡ 36\* 5(mod 19) 36≡ 17 (mod 19)

X ≡ 17\* 5(mod 19)

X ≡ 85 (mod 19)

X ≡ 9 (mod 19)

Ответ: остаток от деления = 9.

**Используемая литература**

1. Лабораторный практикум «Основы информационной безопасности», Н. В. Ржеутская, О. А. Нистюк, Н. И. Уласевич, 2024.
2. ЭЛЕКТРОННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «Математические основы криптографии» для специальности 1 - 98 01 03 «Программное обеспечение информационной безопасности мобильных систем», И.К. Асмыкович, Е.И. Ловенецкая, БГТУ.

Практическое занятие №9

АВТОРСКОЕ ПРАВО И СМЕЖНЫЕ ПРАВА

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия**: Изучить положения авторского права и смежных прав, определить принципы и особенности правовой охраны произведений науки, литературы и искусства.

**Теоретические сведения:**

Авторское право представляет собой совокупность прав, предоставляемых авторам произведений литературы, искусства и науки, а также другим субъектам, связанным с использованием таких произведений. Оно возникает с момента создания произведения и не требует регистрации.

Основные принципы авторского права включают:

* свободу творчества;
* сочетание личных интересов автора с интересами общества;
* неотчуждаемость личных неимущественных прав;
* свободу авторского договора.

Авторское право охраняет как обнародованные, так и необнародованные произведения в различных формах (письменной, устной, электронной и т.д.).

**Ответы на контрольные вопросы:**

1. ***На какие объекты распространяется авторское право?***

Авторское право распространяется на произведения науки, литературы и искусства, существующие в какой-либо объективной форме.

Объекты авторского права:

− литературные произведения;

− драматические и музыкально-драматические произведения, произведения хореографии и пантомимы и другие сценарные произведения;

− музыкальные произведения с текстом и без текста;

− аудиовизуальные произведения;

− произведения изобразительного искусства;

− произведения прикладного искусства и дизайна;

− произведения архитектуры, градостроительства и садово-паркового искусства;

− фотографические произведения, в том числе произведения, полученные способами, аналогичными фотографии;

− карты, планы, эскизы, иллюстрации и пластические произведения, относящиеся к географии, картографии и другим наукам;

– компьютерные программы (прикладные программы и операционные системы на любом языке и в любой форме, включая исходный текст и объектный код; базы данных или компиляции иных материалов в любой форме, представляющие собой по подбору и расположению материалов результат интеллектуального творчества);

− произведения науки;

− производные произведения (переводы, обработки, инсценировки, музыкальные аранжировки, обзор, аннотации, рефераты; сборники произведений: энциклопедии, антологии, атласы и другие составные произведения как результат творческого труда);

− составные произведения – сборники.

1. ***Что относится к личным неимущественным правам?***

Авторские права делятся на личные неимущественные (моральные права – droit moral) и имущественные (экономические) права.

Личные неимущественные права:

− признаваться автором произведения (право авторства);

− использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т. е. анонимно (право на имя);

− обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;

− право на защиту произведения, включая его название, от всякого рода искажений или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора).

1. ***Что относится к личным имущественным правам?***

Имущественные права – исключительное право осуществлять или разрешать осуществлять следующие действия:

− воспроизведение произведения;

− распространение оригинала или экземпляров произведения посредством продажи или иной передачи права собственности;

− прокат оригиналов или экземпляров компьютерных программ, баз данных, аудиовизуальных произведений, нотных текстов музыкальных произведений и произведений, воплощенных в фонограммах;

− импорт экземпляров произведения;

− публичный показ оригинала или экземпляра произведения;

− публичное исполнение произведения;

− передачу произведения в эфир;

− иное сообщение произведения для всеобщего сведения;

− перевод произведения на другой язык;

− переделку или иную переработку произведения.

1. ***Каковы особенности авторского права на составные произведения?***

**Авторское право на составные произведения:**

− автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленные им подбор и распоряжение материалов как результат творческого труда (составительство);

− составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное;

− авторы произведений, включенных в составное произведение, вправе использовать свои произведения независимо от составного произведения, если иное не предусмотрено авторским договором;

− авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор и расположение тех же материалов для создания своих составных произведений;

− лицу, выпускающему в свет энциклопедии, энциклопедические словари, периодические и продолжающиеся сборники научных трудов, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Это лицо вправе при любом использовании таких изданий указывать свое наименование или требовать такого указания;

− авторы произведений, включенных в такие издания, сохраняют исключительные права на использование своих произведений независимо от издания в целом, если иное не предусмотрено авторским договором.

1. ***Каков срок действия авторского права?***

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

1. ***Кто является субъектом авторского права?***

Субъектом авторского права, как правило, является гражданин, творческим трудом которого создано произведение науки, литературы или искусства. Им может быть и гражданин, не достигший восемнадцатилетнего возраста, и душевнобольной. Так, авторские права детей, представленные на смотры или выставки детской или юношеской  
самодеятельности и т. д., защищаются авторским правом.

**Использованные источники**

1. Лабораторный практикум «ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»,

Н. В. Ржеутская, О. А. Нистюк, Н. И. Уласевич, Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», 2024

Практическое занятие №10

ПАТЕНТНЫЙ ПОИСК

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель работы:** Изучить методы патентного поиска, провести анализ охраноспособности объекта интеллектуальной собственности и осуществить поиск аналогов в патентных базах данных.

**Краткие теоретические сведения**

Патентный поиск — это поиск охраняемых объектов промышленной собственности в национальных и международных патентных базах. Он позволяет выявить уже существующие технические решения и оценить новизну и патентную чистоту разрабатываемого объекта.

Патентный поиск необходим:

* для оценки охраноспособности изобретения;
* чтобы избежать нарушения чужих прав;
* при подготовке к подаче заявки на патент.

Основные базы данных:

* Espacenet (https://worldwide.espacenet.com)
* Google Patents (<https://patents.google.com>)
* База ФИПС (<https://www.fips.ru>)

**Условие задания**

Необходимо выполнить экспертизу патентной чистоты разра-

ботанных конструктивных решений: методов испытания материа-

лов и устройств для их осуществления; устройств и механизмов для

реализации технологических процессов.

Вариант 4 – Устройство для счета банкнот

**Исполнительная часть**

В результате проведения исследовательских работ по обеспечению требований безопасности и повышения эффективности обработки наличных денежных средств было предложено конструктивное выполнение устройства для счёта банкнот, предназначенного для автоматического пересчёта бумажных денежных знаков с возможностью их верификации.

Наличие предполагаемых существенных признаков (компактность конструкции, повышенная точность счёта, возможность обнаружения подделок) и планируемый выпуск продукции являются предпосылками для патентования разработки.

Необходимо выполнить экспертизу патентной чистоты разработанного конструктивного решения объекта промышленной собственности.

В качестве существенного признака при патентовании предполагаемого изобретения выносится признак: выполнение считывающего узла с комбинированной системой оптического и инфракрасного анализа банкнот, обеспечивающей точность при высокой скорости счёта.  
Для выявления патентной чистоты разработанного объекта промышленной собственности использовался следующий регламент поиска:

* Объект: устройство для счёта банкнот, включающее механизмы подачи, сканирования и выброса купюр;
* Страна поиска: Республика Беларусь, а также международные базы (для расширенного поиска);
* Источники информации: патентные базы данных;
* Ретроспективность: 5 лет;
* Информационная база:
  + Афіцыйны бюлетэнь «Вынаходствы, карысныя мадэлі, прамысловыя ўзоры» НЦИС РБ;
  + Google Patents (<https://patents.google.com>);
  + Espacenet (https://worldwide.espacenet.com);
  + Каталог МПК (https://www.wipo.int/classifications/ipc).

Для проведения патентного поиска была определена классификационная рубрика предполагаемого изобретения, которая классифицируется по разделу «ЭЛЕКТРИКА», класс G07D 1/00 — устройства для счёта, сортировки или проверки бумажных денег.

Проведённый патентный поиск по указанному классу выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели. Все данные по обнаруженным патентам-аналогам сведены в таблицу.

**Патентная документация**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвертационный приоритет, дата публикации | Название изобретения (полезной модели, промышленого образца) | Сведения о действи охранного документа или причины его аннулирования |
| Счетчик банкнот | Патент РБ № 4867  МПК G 06M 7/00 | Общество с ограниченной ответственностью "ПРО"  Барсуков С. Д.  Заявка u 20080337  От 22.04.2008,  Опубл. 30.12.2008 | «Счетчик банкнот» | Дата прекращения действия: 23.04.2011 |
| Счетчик банкнот | Патент РБ № 5064  МПК G 06M 7/00  МПК G 07D 7/00 | Общество с ограниченной ответственностью "ПРО"  Барсуков С. Д.  Заявка u 20080606  От 29.07.2008,  Опубл. 28.02.2009 | «Счетчик банкнот» | Дата прекращения действия: 30.07.2015 |
| Устройство для счёта банкнот с функцией проверки подлинности, включающее подающие ролики и оптические сенсоры | США, патент US6908029B2, МПК G07D 1/00 | Glory Ltd. (Япония). Заявка № 10/195,318 от 15.07.2002, приоритет: США, публикация: 14.06.2005 | «Bill counter with counterfeit detection» | Действует |
| Машина для счёта и сортировки банкнот, оснащённая несколькими выходами и ИК-датчиками | Китай, патент CN203133923U, МПК G07D 1/00 | Wenzhou Ruixing Financial Equipment Co., Ltd. Заявка № CN201320187781.X от 27.04.2013, публикация: 07.08.2013 | «Banknote counting machine» | Действует |
| Компактное устройство для счёта банкнот, обеспечивающее устойчивую подачу купюр | Китай, патент CN2548209Y, МПК G07D 1/00 | Baotou Zhengxin Financial Equipment Co., Ltd. Заявка № CN01247385.X от 25.07.2001, публикация: 26.03.2003 | «Bank-note counting and checking machine» | Действует |

Дальнейший анализ содержания обнаруженной патентной информации позволяет сделать следующие выводы:

1. Все найденные устройства схожи по функциональному назначению с предложенной разработкой — они предназначены для автоматического пересчёта банкнот и могут содержать модули для проверки их подлинности.
2. Существенные отличия предполагаемой конструкции (например, оригинальный способ подачи купюр, новая компоновка считывающих модулей, повышенная точность или скорость счёта и др.) позволяют предположить наличие изобретательского уровня.
3. При наличии технических решений, не раскрытых в рассмотренных патентах-аналогах, разработка может быть признана патентоспособной при подаче заявки.

Таким образом, наличие аналогов с похожими функциями не исключает возможность патентования устройства при условии его оригинальности, новизны и промышленной применимости.

**Использованные источники**

1. Google Patents – <https://patents.google.com>
2. Espacenet – https://worldwide.espacenet.com
3. Афіцыйны бюлетэнь «Вынаходствы, карысныя мадэлі, прамысловыя ўзоры» – Нацыянальны цэнтр інтэлектуальнай уласнасці Рэспублікі Беларусь – <https://www.belgospatent.org.by>
4. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации. Лабораторный практикум. – Минск: БГТУ, 2024. – 124 с.

Практическое занятие №11

НАСТРОЙКА АНТИВИРУСОВ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель**: овладеть навыками настройки и использования различных антивирусов.

**Краткие теоретические сведения:**

**Компьютерный вирус** – это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

**Антивирусные программы** – специальные программы для обнаружения, уничтожения компьютерных вирусов и защиты от них. Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как профилактические возможности, так и средства лечения от вирусов и восстановления данных.

**Условие задания:**

1. Установите и настройте антивирусную программу по варианту.

2. Обновите базу данных сигнатур вирусов.

3. Выполните сканирование дисков.

|  |  |
| --- | --- |
| Вариант | Антивирус |
| 4 | Panda Cloud Antivirus |

**Исполнительная часть:**

Переходим на сайт для скачивания(https://www.pandasecurity.com/en/homeusers/free-antivirus)

Изображение выглядит как текст, снимок экрана, человек, Веб-сайт

Контент, сгенерированный ИИ, может содержать ошибки.

Скачиваем бесплатную версию для дома

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Выполняем установку

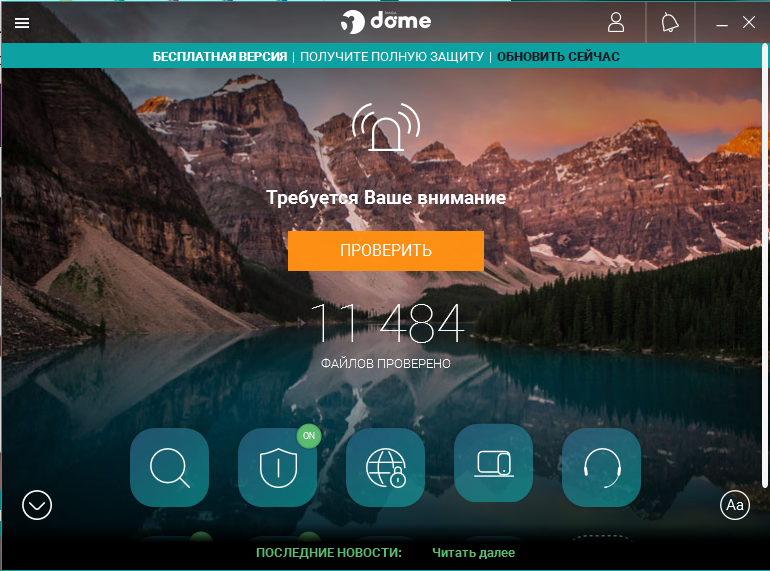
Изображение выглядит как снимок экрана, текст, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Веб-сайт

Контент, сгенерированный ИИ, может содержать ошибки.

Ждем окончания установки и открываем



Выполним проверку диска D

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, Мультимедийное программное обеспечение, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Дожидаемся окончания и смотрим результат

Изображение выглядит как текст, снимок экрана, мультимедиа, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Все отлично, угроз не обнаружено

Использованные источники

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации. Лабораторный практикум. – Минск: БГТУ, 2024. – 124 с.
2. Panda Home Antiviruse – https://www.pandasecurity.com/en/homeusers/free-antivirus

Практическое занятие №12

ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ ДЛЯ РЕАЛИЗАЦИИ

ПРИЛОЖЕНИЙ, ИСПОЛЬЗУЮЩИХ СИММЕТРИЧНОЕ

И АССИМЕТРИЧНОЕ ШИФРОВАНИЕ,

С ПРИМЕНЕНИЕМ БИБЛИОТЕКИ

SYSTEM.SECURITY.CRYPTOGRAPHY

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель:** изучить модель криптографии .NET Framework, основ-

ные классы и структуры данных, разработать приложение для шиф-

рования файлов, использующих симметричные и ассиметричные

алгоритмы шифрования.

**Теоретические сведения**

В .NET Framework присутствует пространство имен для

выполнения криптографических операций под названием

System.Security.Cryptography. Данное пространство имен предостав-

ляет криптографические службы, включающие безопасное кодиро-

вание и декодирование данных, а также другие операции, такие как

хеширование сообщений, генерация случайных чисел и проверка

подлинности сообщений. Данная библиотека предоставляет доступ

для использования различных реализаций алгоритмов, в основном

это программные интерфейсы CryptoApi (CAPI) и Cryptography Next

Generation API (CNG API). Помимо этого, для некоторых алгорит-

мов возможно использование реализаций на основе OpenSSL.

CryptoAPI – интерфейс программирования приложений, кото-

рый обеспечивает разработчиков Windows-приложений стандарт-

ным набором функций для работы с криптопровайдером. Входит в

состав операционных систем Microsoft. Большинство функций

CryptoAPI поддерживается, начиная с Windows 2000.

Cryptography Next Generation API стала долгосрочной заменой

CAPI. Данный набор интерфейсов поддерживает все алгоритмы, пред-

лагаемые CAPI, а также другие алгоритмы, перечисленные в своде пра-

вил Suite B Агентства национальной безопасности США. Данный интер-

фейс поддерживает следующие длины ключей или размерность хеша:

– RSA от 512 до 16 384 бит с шагом 64 бит;

– DH – от 512 до 16 384 бит с шагом 64 бит;

– DSA – от 512 до 1024 бит с шагом 64 бит;

– ECDSA – P-256, P-384, P-521 (NIST Curves);

– ECDH – P-256, P-384, P-521 (NIST Curves);

– MD2 – 128 бит;

– MD4 – 128 бит;

– MD5 – 128 бит;

– SHA1 – 1160 бит;

– SHA256 – 256 бит;

– SHA384 – 384 бит;

– SHA512 – 512 бит.

**Условие задания:**

1. Ознакомиться с созданием криптографического приложения.
2. Выполнить шифрование, дешифрование и хеширование своей фамилии по алгоритмам RSA и MD5.
3. Сохранить ключи, зашифрованные и захешированные данные в файлы.
4. Через Hex-редактор отобразить эти данные.
5. Реализовать проверку целостности сообщения и хеша по примеру ЭЦП, продемонстрировать результат при изменениях.

**Исполнительная часть**

**Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

**Результат выполнения:**

**Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

Использованные источники

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации. Лабораторный практикум. – Минск: БГТУ, 2024. – 124 с.

Практическое занятие №13

ИЗУЧЕНИЕ СТАНДАРТНЫХ СРЕДСТВ

ДЛЯ РЕАЛИЗАЦИИ СИММЕТРИЧНОГО

И АССИМЕТРИЧНОГО ШИФРОВАНИЯ

С ИСПОЛЬЗОВАНИЕМ SUBTLECRYPTO В JS

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель:** изучить интерфейс SubtleCrypto, основные классы и

структуры данных: разработать приложение для шифрования фай-

лов, использующих симметричные и ассиметричные алгоритмы

шифрования.

**Краткие теоретические сведения:**

* **Web Crypto API** — это API, предоставляющее доступ к криптографическим функциям браузера. Оно предоставляет низкоуровневые функции для работы с криптографией, включая создание ключей, шифрование, хеширование и многое другое.
* **AES-GCM** — это алгоритм симметричного шифрования с аутентификацией, который используется для защиты данных. Он использует ключ для шифрования и может быть использован для шифрования данных в сочетании с механизмом аутентификации для предотвращения атак.
* **SHA-512** — это алгоритм хеширования, который генерирует 512-битный хеш. Он используется для защиты данных от модификации и для создания уникальных представлений данных.
* **AES-KW** — алгоритм для упаковки и распаковки симметричных ключей, используемый для безопасного обмена криптографическими ключами.
* **RSA-PSS** — алгоритм подписи, использующий алгоритм RSA и схему подписания с подтверждением (PSS). Он предоставляет высокую степень безопасности для подписанных данных.

**Условие задания**

Выполнить криптографические операции с использованием Web Crypto API в Node.js:

1. Генерация случайных чисел и вывод их в консоль.
2. Шифрование и дешифрование строки (фамилии "Васильев") с использованием алгоритма шифрования **AES-GCM**.
3. Хеширование строки "Васильев" с использованием алгоритма **SHA-512**.
4. Упаковка и распаковка ключа с использованием алгоритма **AES-KW**.
5. Подпись и проверка подлинности сообщения с использованием алгоритма **RSA-PSS**.

**Исполнительная часть**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

Использованные источники

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации. Лабораторный практикум. – Минск: БГТУ, 2024. – 124 с.