**Разработка программно-аппаратного решения для работы с коммерческой тайной**

**Введение**

Коммерческая тайна является ценным активом для бизнеса, поскольку она обеспечивает конкурентное преимущество за счет сохранения конфиденциальной информации в тайне. Однако управление коммерческой тайной может быть непростой задачей, особенно с учетом растущего объема данных, генерируемых и совместно используемых в современном цифровом мире. Таким образом, разработка аппаратно-программного решения для работы с коммерческой тайной становится все более актуальной.

Цель - обеспечить безопасную среду для хранения и обмена конфиденциальной информацией, такой как списки клиентов, ценовые стратегии и др. Это решение поможет защитить коммерческую тайну от несанкционированного доступа, кражи или неправильного использования и обеспечит высокий уровень безопасности для компаний и организаций..

Задачи:

1. Проведите обзор литературы о существующих методах шифрования и дешифрования данных и их пригодности для работы с коммерческой тайной.
2. Разработать набор требований к программно-аппаратному решению на основе обзора литературы и предложений заинтересованных сторон.
3. Разработать аппаратно-программное решение, включая алгоритмы шифрования и дешифрования и пользовательские интерфейсы.
4. Создать прототип программно-аппаратного решения и протестировать его на функциональность и безопасность.
5. Провести исследование удобства использования аппаратно-программного решения для определения простоты его использования и выявления необходимых улучшений.
6. Оценить безопасность аппаратно-программного решения и выявить любые потенциальные уязвимости или слабые места.
7. Разработать документацию, включая руководства пользователя и технические спецификации, для аппаратно-программного решения.
8. Сравнить предлагаемое решение с существующими программами шифрования и дешифрования данных и проанализировать его преимущества и недостатки.

Выполняя эти задачи, предприятия могут гарантировать, что их коммерческая тайна защищена и доступна только уполномоченному персоналу, снижая риск утечки данных и потери конкурентного преимущества.

**Постановка задачи**

Коммерческая тайны - это ценный актив для любой компании или организации. Она может включать конфиденциальную информацию, такую как списки клиентов, стратегии ценообразования и др. Поэтому очень важно защитить коммерческие секреты от несанкционированного доступа, кражи или неправильного использования.

Предлагаемое мной программно-аппаратное решение обеспечит безопасную среду для хранения и обмена коммерческими секретами. Решение будет состоять из аппаратного устройства, которое будет шифровать и расшифровывать данные, и программного обеспечения, которое будет управлять устройством и предоставлять пользовательский интерфейс. Аппаратное устройство будет представлять собой USB-ключ, который можно подключить к USB-порту компьютера. Программное обеспечение будет совместимо с операционной системой Windows.

Предложенное мной решение будет сравниваться с существующими программами для шифрования и дешифрования данных. Мы проанализируем преимущества и недостатки различных методов шифрования и дешифрования данных и их пригодность для работы с коммерческой тайной.

В целом, наше программно-аппаратное решение обеспечит высокий уровень безопасности при хранении и обмене коммерческой тайной. Внедрив это решение, компании и организации смогут защитить свои коммерческие секреты.

* 1. Обзор аналогов
  2. SWOT-анализ

**Сильные стороны**

* Обеспечивает безопасное хранение конфиденциальных данных, предоставляя доступ только уполномоченному персоналу.
* Можно обнаруживать и предотвращать попытки несанкционированного доступа, обеспечивая сохранность хранимой информации.
* Система может быть настроена в соответствии с конкретными потребностями отдельных предприятий, обеспечивая максимальную защиту их коммерческой тайны.

**Слабые стороны**

* Потребность в регулярном обслуживании для обеспечения ее эффективной работы.
* Эффективность системы зависит от персонала, ответственного за ее управление, неэффективное управление может привести к нарушению безопасности.

**Возможности**

* Усовершенствование систем безопасности. С ростом числа кибератак компании должны быть на шаг впереди, чтобы защитить свои коммерческие секреты.
* Это решение может быть представлено на рынке для предприятий различных отраслей, что дает возможность для расширения.

**Угрозы**

* Постоянное развитие хакерских технологий.
* Эффективность системы сильно зависит от персонала, ответственного за ее управление, что может представлять угрозу для компаний с неадекватным управлением.
  1. PEST-анализ

**Политические**

* Уровень государственной поддержки предприятий, стремящихся защитить свои коммерческие тайны, может повлиять на внедрение системы..

**Экономический**

Инвестиции в систему могут быть оправданными, поскольку потенциальные финансовые потери, связанные с нарушением коммерческой тайны, могут быть значительными.

Предприятия должны учитывать долгосрочные экономические выгоды от внедрения программно-аппаратного решения. Например, если система помогает защитить коммерческую тайну, она может предотвратить значительные финансовые потери от судебных исков или потерю конкурентных преимуществ.

**Социокультурный**

Растущая осведомленность о киберугрозах и важности безопасности данных может принести пользу предприятиям, стремящимся внедрить программно-аппаратное решение. Однако некоторые сотрудники могут сопротивляться внедрению системы, поскольку она может показаться навязчивой или ограничивающей.

Предприятия должны решить эти проблемы путем разъяснения сотрудникам преимуществ системы. Кроме того, они могут организовать обучение сотрудников, чтобы помочь им понять, как работает программно-аппаратное решение и как оно может помочь защитить коммерческие секреты компании.

**Технологический**

Проект должен регулярно обновляться, чтобы опережать потенциальные угрозы безопасности в связи с быстрым развитием технологий. Кроме того, технологические достижения могут также предоставлять возможности для расширения возможностей и повышения эффективности системы.

1.4 Формирование требований к программному продукту

1.4.1 Бизнес требования

1. Система должна обеспечивать безопасное хранение конфиденциальных данных, предоставляя доступ только уполномоченному персоналу.

2. Система должна обнаруживать и предотвращать попытки несанкционированного доступа, обеспечивая сохранность хранимой информации.

3. Система должна быть настраиваемой в соответствии со специфическими потребностями отдельных предприятий, обеспечивая максимальную защиту их коммерческой тайны.

4. Система должна регулярно обслуживаться для обеспечения ее эффективной работы.

5. Система должна регулярно обновляться, чтобы опережать потенциальные угрозы безопасности в связи с быстрым развитием технологий.

1.4.2. Пользовательские требования

1.4.3. Функциональные требования

1. Система должна обеспечивать безопасное хранение конфиденциальных данных, предоставляя доступ только уполномоченному персоналу.

2. Система должна обнаруживать и предотвращать попытки несанкционированного доступа, обеспечивая сохранность хранимой информации.

3. Система должна быть настраиваемой в соответствии со специфическими потребностями отдельных предприятий, обеспечивая максимальную защиту их коммерческой тайны.

4. Система должна регулярно обслуживаться для обеспечения ее эффективной работы.

5. Система должна регулярно обновляться, чтобы опережать потенциальные угрозы безопасности в связи с быстрым развитием технологий.

1.4.4. Нефункцональные требования

1. Безопасность: Система должна иметь высокий уровень безопасности для предотвращения несанкционированного доступа и обеспечения сохранности хранимой информации.

2. Надежность: Система должна быть надежной и доступной в любое время, чтобы предприятия могли получить доступ к своим коммерческим секретам, когда это необходимо.

3. Масштабируемость: Система должна быть масштабируемой для удовлетворения растущих потребностей предприятий с течением времени.

4. Удобство использования: Система должна быть простой в использовании и доступной для уполномоченного персонала с минимальной подготовкой.

1.4.5. Ограничения

1.4.6. Требования к интерфейсам

1. Пользовательский интерфейс: Система должна иметь удобный интерфейс, позволяющий авторизованному персоналу легко получать доступ к конфиденциальным данным и управлять ими.

2. Доступность: Система должна быть доступна для авторизованного персонала из любого места с подключением к Интернету.

3. Отчетность: Система должна предоставлять широкие возможности отчетности, позволяющие предприятиям отслеживать и анализировать доступ к конфиденциальным данным.

4. Аудит: Система должна обладать возможностями аудита, позволяющими предприятиям контролировать и отслеживать все действия системы.

5. Шифрование: Система должна использовать шифрование для защиты всех конфиденциальных данных, как при хранении, так и при передаче.

6. Аутентификация: Система должна иметь надежные механизмы аутентификации для обеспечения доступа к конфиденциальным данным только авторизованного персонала.

7. Авторизация: Система должна иметь механизмы авторизации, гарантирующие, что только уполномоченный персонал может выполнять определенные действия с конфиденциальными данными.

8. Бэкап и восстановление: Система должна иметь механизм резервного копирования и восстановления, чтобы гарантировать, что данные не будут потеряны в случае сбоя системы.

1.4.7. Требования к данным

1.5. Программные средства разработки

* MySQL
* Git
* Visual Studio

1.6. Аппаратые средства разработки

USB-накопитель