**Слайд 1.** Здравствуйте, уважаемая государственная аттестационная комиссия. К Вашему вниманию, я хотел бы представить, выпускную квалификационную работу на тему: «Разработка программно-аппаратной системы двухфакторной аутентификации».

**Слайд 2.** Защита от несанкционированного доступа, на сегодняшний день, является одним из актуальных и приоритетных задач в обеспечении безопасности информационных и инфокоммуникационных систем. Несанкционированный доступ представляет с собой множество последствий. Одним из наиболее серьёзных угроз – это захват управления над автоматизированными системами и оборудованием. Такая угроза возможна, вследствие недостаточно надежной системы аутентификации, предназначенного для доступа к автоматизированным системам управления. Для решения данной задачи представлена программно-аппаратная система двухфакторной аутентификации. Техническое задание представлено на слайде номер 2.

**Слайд 3.** Цель работы обеспечение защиты автоматизированной системы управления от несанкционированного доступа и обеспечения безопасности открытого канала связи, путем применения средств криптографической защиты информации.

Для достижения поставленной цели необходимо решить следующие задачи:

* реализовать программную часть системы
* разработать криптографический протокол, на основе российских стандартов, предназначенный для проверки подлинности клиента и обеспечения безопасности пользовательских данных, передаваемых по открытому каналу связи
* разработать приложение для тестирования криптографического протокола
* написать документ, описывающий интерфейс доступа к программной части.

**Слайд 4.** На слайде номер 4 представлена архитектура системы. Основными объектами является клиент и сервер. Сервер предназначен для управления автоматизированной системой. Клиент представляет с собой встраиваемую систему на платформе ОС Linux. Для безопасного доступа администратора к настройкам системы и защиты канала связи, между клиентом и сервером, необходимо внедрить двухфакторную аутентификацию на основе смарт-карты и пароля.

**Слайд 5.** Разрабатываемая программная часть состоит из следующих компонентов:

* криптографический протокол двухфакторной аутентификации (библиотека для клиента и сервера)
* библиотека доступа к считывателю смарт-карты (для клиента)
* приложение тестирования библиотек (для клиента и сервера)
* руководящий документ, описывающий интерфейс доступа к библиотекам.

**Слайд 6.** На слайде номер 6 рассмотрены угрозы, для решения которых предназначена система. Анализ сетевого трафика, направлен в первую очередь на получение пароля и идентификатора пользователя путем "прослушивания сети", помощью специального программного анализатора sniffer. Для противостояния такой угрозы применяется симметричное шифрование. Для предотвращения угроза подмена доверенного объекта в сети и передача по каналу связи сообщения от его имени с присвоением определенных прав применяется процедура проверки подлинности клиента. Для выявления уязвимостей исходных кодах программы, согласно рекомендациям руководящего документа ФСТЭК применяться статистический и динамический анализ кода.

**Слайд 7.** Криптографический протокол двухфакторной аутентификации предназначен для проверки подлинности клиента и защиты открытого канала связи, предназначенного для передачи пользовательских данных. Протокол состоит из трёх этапов:

* аутентификация клиента
* выработка и обмен сессионным ключом шифрования по протоколу Диффи-Хеллмана
* алгоритм аутентификации пользователя