**Слайд 1.** Здравствуйте, уважаемая государственная аттестационная комиссия. Защищается выпускную квалификационную работу на тему: «Разработка программно-аппаратной системы двухфакторной аутентификации». Руководитель работы к. т. н., доцент кафедры «Телекоммуникационные системы» В. П. Батура.

**Слайд 2.** Защита информационных и инфокоммуникационных систем от несанкционированного доступа, является одним из актуальных и приоритетных задач. Интерес к этой тебе, на сегодняшний день, велик, так как получение злоумышленником доступа к информационной системе представляет множество серьёзных угроз. Такие как:

* кража конфиденциальной информации
* изменение критически важных данных автоматизированных систем и дезорганизации работы устройств
* захват управления над системой и т. п.

Одним из причин получения злоумышленником доступа к автоматизированной системе, является недостаточно надежная система аутентификации. Поэтому, для решения данной проблемы было разработано программно-аппаратная система двухфакторной аутентификации, соответствующая требованиям ФСТЭК для информационных систем третьего класса. Техническое задание работы представлено на слайде номер 2.

**Слайд 3.** Целью работы является защита автоматизированной системы и открытого канала связи, предназначенного для аутентификации, от несанкционированного доступа, 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 рассмотрена архитектура. Основными компонентами системы являются клиент, который представляет с собой встраиваемую систему на платформе Linux, согласно техническому заданию, и сервер управления. Для лбеспечения безопасного доступа используется программно-аппаратная система двухфакторной аутентификацию на основе смарт-карты и пароля.

**Слайд 5.** Мною было разработана программной части системы, которая состоит из следующих компонентов:

* крипто провайдер, включающий в себе реализацию стандартов ГОСТ 28147-89, ГОСТ Р11.34-2012 и протокола Диффи-Хеллмана
* криптографический протокол
* приложение тестирования
* библиотека доступа к смарт-карте

**Слайд 6.** На слайде номер 6 рассмотрены угрозы и способы их решения. Перехват и анализ сетевого трафика, направление на получение пароля и идентификатора пользователя, путем "прослушивания сети", помощью специального программного анализатора, предотвращается с применением симметричного шифрования. Нарушение целостности данных, передаваемых по каналу связи, решается применением однонаправленной хеш-функций. Для предотвращения подмены доверенного объекта в сети и передачи сообщения от его имени с присвоением его прав и привилегий применяется процедура проверки подлинности клиента, описанные в международном стандарте. С целью выявления уязвимостей программного обеспечения, относящихся к средствам защиты информации, согласно руководящему документу ФСТЭК, «Защита от несанкционированного доступа к информации часть 1», от 4 июня 1999 г., должны подвергаться к статическому и динамическому анализу.

**Слайд 7.** Далее рассмотрим описание криптографического протокола. Криптографический протокол двухфакторной аутентификации из трёх этапов:

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

**Слайд 8**. При разработке первого этапа протокола, стояла задача выбора алгоритма аутентификации клиента из существующих решений. На слайде 8 представлена таблица сравнения протоколов аутентификации клиента, описанных в международном стандарте. Среди представленных наиболее подходящим является протокол, основанный на применении случайных чисел и имитозащиты. Имитовставка вырабатывается алгоритмом ГОСТ 28147-89 в специальном режиме на заранее известном клиенту ключе.

**Слайд 9.** На слайде номер 9, представлен алгоритм первого этапа протокола, проверка подлинности клиента. Сервер генерирует и отправляет клиенту случайное число, клиент на известном ключе шифрует полученное число, добавляет имитовставку для защиты от фальсификации, передает серверу, сервер зная идентификатор клиента на том же ключе шифрует переданное случайное число и сравнивает результат с полученным сообщение от клиента.

**Слайд 10.** На слайде 10 представлен второй этап протокола. На данном этапе клиент и сервер вырабатывают сессионный ключ шифрования. Для контроля целостности передаваемых данных, использует однонаправленная хеш-функция.

**Слайд 11.** На слайде 11 представлен третий этап протокола. На этом этапе происходит двухфакторная аутентификация пользователей по защищенному каналу связи. Для фактора составляют смарт-карта и пароль. Защита пользовательских данных осуществляется применением симметричного шифрования. Ключ шифрования было выработано во втором этапе протокола.