АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Криптографические протоколы и стандарты»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины:

- изучение принципов построения и алгоритмов протоколов, обеспечивающих конфиденциальность, целостность и аутентичность информации.

Задачи изучения дисциплины:

- обучить студентов принципам работы основных протоколов;
- привить студентам навыки реализации криптографических протоколов с использованием ЭВМ;
- дать студентам представление об анализе стойкости протоколов к атакам.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к базовой части цикла Б1 (Б1.Б.34) образовательной программы и читается в 8-м семестре студентам специальности «Информационная безопасность автоматизированных систем» очной формы обучения. Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Алгебра и геометрия», «Дискретная математика», «Криптографические методы защиты информации», «Информатика». Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Криптографические протоколы и стандарты» является предшествующей для изучения следующих дисциплин: «Методы алгебраической геометрии в криптографии», «Дополнительные главы криптографии».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины «Криптографические протоколы и стандарты» направлен на формирование следующих компетенций:

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);
- способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);
- способностью проводить анализ защищенности автоматизированных систем (ПК-3);
- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);
- способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);
- способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);
- способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
- способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);
- способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);
- способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);

В результате изучения дисциплины студент должен:

знать:

- типовые криптографические протоколы и основные требования к ним;
- методы аутентификации и подтверждения подлинности сообщений и пользователей;
- способы построения хеш-функций и основные требования к ним;
- основные типы электронной подписи;
- базовые протоколы проверки подлинности и обмена ключами;
- протоколы разделения секрета;
- основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности;

уметь:

- формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;
- использовать схемы разделения секрета;
- проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов;
- осуществлять распределение аутентифицированных криптографических ключей в корпоративных сетях;

владеть:

- криптографической терминологией;
- простейшими подходами к анализу безопасности криптографических протоколов;
- навыками использования и администрирования современных средств электронной подписи;
- навыками самостоятельной работы с современными международными стандартами

криптографических протоколов.

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение экзамена.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление;
- выполнение курсовой работы.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: защита лабораторных работ.

Итоговая аттестация проводится в форме: экзамен.