Аннотация рабочей программы дисциплины

«Криптографические протоколы»

Направление подготовки: **10.03.01 - Информационная безопасность**
Профиль подготовки **"Безопасность компьютерных систем" (по отрасли или в сфере профессиональной деятельности)**
Квалификация выпускника: **бакалавр**

Общая трудоемкость дисциплины, изучаемой в 7 семестре, составляет 4 зачетные единицы. По дисциплине предусмотрен экзамен.

Цели и задачи освоения дисциплины

Дисциплина «Криптографические протоколы» имеет целью ознакомление слушателей существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

Задача дисциплины «Криптографические протоколы» – получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

В результате освоения дисциплины обучающийся должен:

Знать:

– формулировать задачу по оцениванию безопасности криптографического протокола применительно к конкретным условиям;
– криптографические стандарты;
– типовые криптографические протоколы и основные требования к ним;
– принципы построения криптографических хеш-функций;
– основные схемы цифровой подписи;
– протоколы идентификации;
– протоколы передачи и распределения ключей;

Уметь:

– использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов;

– формулировать свойства безопасности криптографических протоколов;
– проводить сравнительный анализ криптографических протоколов, решающих сходные задачи;

Владеть:

– криптографической терминологией;
– простейшими подходами к анализу безопасности криптографических протоколов.

Основные разделы дисциплины:

1. Протоколы и их классификация.
2. Протоколы электронной подписи.
3. Протоколы распределения ключей.
4. Протоколы идентификации.
5. Протоколы с нулевым разглашением.
6. Прикладные протоколы.

Разработчик программы:

к.т.н., доцент кафедры ИБ Панков К.Н

Зав. кафедрой ИБ д.т.н., профессор Шелухин О.И