МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Прикладная криптография

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	10	10	часов
3	Лабораторные работы	24	24	часов
4	Всего аудиторных занятий	52	52	часов
5	Самостоятельная работа	56	56	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 7 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

формирование у студентов представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности.

1.2. Задачи дисциплины

- сформировать представление об основных проблемах, связанных с практическим использование криптографических методов защиты информации;
- изучить основные криптографические протоколы;
- изучить инфраструктуру открытого ключа

2. Место дисциплины в структуре ОПОП

Дисциплина «Прикладная криптография» (Б1.В.03.02) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность сетей ЭВМ, Криптографические методы защиты информации, Основы информационной безопасности.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-3 способностью проводить анализ защищенности автоматизированных систем;
- ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
- ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;

В результате изучения дисциплины обучающийся должен:

- **знать** основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.
- **уметь** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.
- **владеть** навыками использования типовых криптографических алгоритмов.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
7 семестр
1 Криптографические протоколы: общие понятия.
2 Протоколы распределения ключей.
3 Инфраструктура открытых ключей.
4 Протоколы идентификации и аутентификации.
5 Безопасный канал обмена сообщениями.
6 Практические аспекты реализации средств криптографической защиты информации.