

Документ подписан электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 29.09.2023 07:35:35
Уникальный программный ключ:
27e516f4c088deb62ba68945f4406e13fd454355

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: **38.05.01 Экономическая безопасность**

Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **5**

Семестр: **9**

Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	8	8	часов
3	Лабораторные работы	16	16	часов
4	Всего аудиторных занятий	42	42	часов
5	Самостоятельная работа	30	30	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Зачёт: 9 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Основная цель дисциплины «Прикладная криптография» — 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 использованием криптографических методов защиты информации; изучить основные криптографические протоколы; изучить инфраструктуру открытого ключа.

2. Место дисциплины в структуре ОПОП

Дисциплина «Прикладная криптография» (ФТД.2) относится к блоку ФТД.2.

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности.

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

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
9 семестр
1 Криптографические протоколы: общие понятия.
2 Протоколы распределения ключей.
3 Инфраструктура открытого ключа.
4 Протоколы идентификации и аутентификации.
5 Безопасный канал обмена сообщениями.
6 Практические аспекты реализации средств криптографической защиты информации.