

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Уровень подготовки: высшее образование – специалитет

Специальность

10.05.05 «Безопасность информационных технологий
в правоохранительной сфере»
(код и наименование специальности)

Специализация

Технологии защиты информации в правоохранительной сфере
(наименование специализации)

Квалификация (степень) выпускника

Специалист

Форма обучения

очная

Год начала подготовки – 2013

Место дисциплины в структуре образовательной программы

Дисциплина «Криптографическая защита информации» является дисциплиной базовой части основной профессиональной образовательной программы (ОПОП).

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по специальности 090915 Безопасность информационных технологий в правоохранительной сфере, утвержденного приказом Министерства образования и науки Российской Федерации от "01" февраля 2011 г. № 132, а также в соответствии с Приказом Министерства образования и науки Российской Федерации от 19 декабря 2013 г. N 1367 г. «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» и актуализирована в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, утвержденного приказом Министерства образования и науки Российской Федерации 19 декабря 2016 г. № 1612. Является неотъемлемой частью основной профессиональной образовательной программы.

Целью освоения дисциплины является ознакомление с основополагающими принципами защиты информации с помощью криптографических методов и примерами реализации этих методов на практике.

Задачи:

Получить общее представление об основах:

1. Системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;
2. Принципов разработки шифров;
3. Математических методов, используемых в криптографии.

Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	ОПК-1	- Основные теоремы, и методы построения систем криптографической защиты информации; - Теоретические основы методов формирования и реализации информационных атак		- Математическим аппаратом, применяемым для построения криптографических алгоритмов
2	Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ПК-1	- Наиболее распространенные стандарты криптографических алгоритмов	- Применять методы противодействия атакам. - Осуществлять выбор криптографических средств защиты информации	
3	Способность применять технические и программно-аппаратные средства обработки и защиты информации	ПК-2	Особенности реализации стандартных криптографических алгоритмов		Навыками работы с программами, реализующими средства криптографической защиты информации

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	<p>Физические основы видеосъемки: Устройство видеокамеры. Объективы. Камера-обскура и pinhole-объективы. Запись изображения с помощью ПЗС и КМОП-матриц. Трехчиповые и одночиповые цветные видеокамеры. Обработка видеоинформации в видеокартах.</p>
2	<p>Технические характеристики устройств и систем видеоконтроля: Различия между системами видеонаблюдения, видеоохраны и видеозащиты. Различия между системами охранного телевидения различных групп и классов. Влияние освещенности объекта контроля на работу камер. Требования и рекомендации к оснащению рабочего места оператора ТВСК. Функциональные характеристики камер: угол обзора, оптический формат, метрическое фокусное расстояние, кружок рассеяния, светосила, зона резкости, чувствительность. Инфракрасная подсветка. Компенсация засветки. Калибровочные параметры камер: размерность пикселей, пиксельное фокусное расстояние, принципиальная точка, угол скоса, радиальная и тангенциальная дисторсия. Калибровка видеокамеры.</p>
3	<p>Системы трехмерного видеоконтроля: Извлечение информации о положении объекта в пространстве из видеоданных. Преобразования пространственных координат. Стереовидение: стереотриангуляция, стереокалибровка, эпиполярная ректификация, построение разностных карт. Системы структурированного света. Времяпролетные системы. Компьютерное представление трехмерных данных.</p>
4	<p>Компьютерная обработка данных видеонаблюдения: Общие представления о компьютерном зрении и распознавании образов. Компьютерное представление черно-белых и цветных изображений. Цветовые пространства. Сегментация изображений. Гистограммы изображений и их применение. Адаптивное пороговое преобразование. Выделение границ на изображениях: фильтры Собеля, Прюитт и Щарра, алгоритм Кенни. Сегментация с помощью кластеризации: алгоритмы k-средних, k-медоид, среднего сдвига; аггломеративная кластеризация. Распознавание простых геометрических объектов: преобразование Хафа, метод RANSAC. Распознавание ключевых точек: детектор углов Харриса, SIFT-дескрипторы. Распознавание людей на изображениях: алгоритм Виолы-Джонса, нейросетевые подходы. Компрессия данных при передаче видеопотока. Обнаружение движения. Трекинг перемещающихся объектов. Применение фильтров Калмана при трекинге.</p>

Подробное содержание дисциплины, структура учебных занятий, трудоемкость изучения дисциплины, входные и исходящие компетенции, уровень освоения, определяемый этапом формирования компетенций, учебно-методическое, информационное, материально-техническое обеспечение учебного процесса изложены в рабочей программе дисциплины.