МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ РЕСПУБЛИКИ ДАГЕСТАН

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН
«ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Генеральный директор
ГАУ РД «ЦИТ»

«29» марта 2024г.

С.М.Сабиров

М.П.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(повышение квалификации)

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Махачкала, 2024

1. Цели освоения образовательной программы.

К **основным целям** освоения образовательной программы «Методы и средства защиты информации» следует отнести:

- формирование у слушателей знаний о методах и средствах защиты информации, о принципах преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею.

К **основным задачам** освоения образовательной программы «Методы и средства защиты информации» следует отнести:

- ознакомление с основными понятиями, относящимися к области защиты информации в технических системах управления;

- овладение современными методами шифрования в криптографии информационных потоков технических систем управления;

- овладение программно-аппаратными комплексами защиты информации;

- овладение основными классификационными признаками компьютерных вирусов и методами защиты от них;

- овладение стандартами и спецификациями в области информационной безопасности систем управления.

2. Перечень планируемых результатов обучения по образовательной программе.

В результате освоения программы у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

В результате освоения образовательной программы обучающийся должен обладать	**Перечень планируемых результатов обучения по образовательной программе**
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	**Знать:** современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. **Уметь**: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. **Владеть:** навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	**Знать:** программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях. **Уметь:** конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности. **Владеть:** принципами формирования политики информационной безопасности объекта информатизации.

ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	**Знать:** основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных; основные виды угроз безопасности персональных данных в информационных системах персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных. **Уметь:** создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных; планировать мероприятия по обеспечению безопасности персональных данных; обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных; проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. **Владеть:** навыками работы с правовыми базами данных; навыки определения уровней защищённости персональных данных; навыки выявления угроз безопасности персональных данных в информационных системах персональных данных; навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных; навыки применения сертифицированных средств защиты информации.
ПК-6. Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных	**Знать:** архитектуру и принцип работы операционных систем. **Уметь:** выполнять работы по установке, настройке, отладке и обслуживанию операционных систем. **Владеть:** навыками эффективного управления серверными операционными системами, конфигурирования корпоративных сервисов.

3. Структура и содержание образовательной программы

Общая продолжительность образовательной программы составляет **36** академических часов.

№ п/п	Названия разделов	Всего (час.)	в том числе (в часах)			Формы контроля
			Лекции	Практические занятия	Лабораторные занятия	
1	2	3	4	5	6	10
1	**Введение.** Основные понятия, положения и определения. Предмет и объект защиты. Понятие угрозы безопасности. Классификация угроз. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации.	2	2			Устный опрос, дискуссия
2	**Правовые и организационные методы защиты информации.** Правовое регулирование в области безопасности информации. Государственная политика РФ в области безопасности информационных технологий. Законодательная база в области информационных технологий. Структура государственных органов, обеспечивающих безопасность информационных технологий. Общая характеристика организационных методов защиты.	2	2			Устный опрос, дискуссия
3	**Стандарты и спецификации в области информационной безопасности.** Общие критерии безопасности. Подготовка и целевая направленность общих критериев. Организация общих критериев. Возможности и применимость, концепции общих критериев. Действующие стандарты и рекомендации в области информационной безопасности. Критерии оценки надежных компьютерных систем. Гармонизированные критерии европейских стран. Руководящие документы по защите от несанкционированного доступа	2	2			Устный опрос, дискуссия

	Гостехкомиссии при Президенте РФ. Особенности информационной безопасности компьютерных сетей. Рекомендации Х.800.					
4	**Административный уровень информационной безопасности в информационно-вычислительной системе.** Понятие политики безопасности. Анализ риска. Угрозы/видимость. Уязвимость/последствия. Учет информационных ценностей. Модели основных типов политик безопасности. Типы политик безопасности. Модель матрицы доступов Харрисон-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла-Лападула. Модель Low-Water-Mark. Модель ролевого разграничения доступа.	4	4			Устный опрос, дискуссия
5	**Криптографическая защита информации.** Основные определения криптологии. Классификация методов криптографического закрытия информации. Основы теории К. Шеннона. Основные криптографические модели. Алгоритмы шифрования. Симметричные методы шифрования. Асимметричные методы шифрования. Сравнение криптографических методов. Методы кодирования. Другие методы.	4	4			Устный опрос, дискуссия
6	**Защита информации в локальных ЭВМ иинформационно-вычислительных сетях.** Модели безопасности основных операционных систем. Механизмы защиты операционных систем.	2	2			Устный опрос, дискуссия
7	**Системы защиты программного обеспечения.** Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы. Системы защиты от несанкционированного копирования. Системы защиты от несанкционированного доступа.	4	4			Устный опрос, дискуссия

	Показатели эффективности систем защиты.					
8	**Защита информации в корпоративных сетях.** Основы и цель политики безопасности в компьютерных сетях. Управление доступом. Идентификация и установление подлинности. Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам. Реагирование на несанкционированные действия. Многоуровневая защита корпоративных сетей. Аутентификация. Анализ возможностей маршрутизации и прокси-серверов. Типы межсетевых экранов.	4	4			Устный опрос, дискуссия
9	**Защита от информационных инфекций. Вирусология.** Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов.	2	2			Устный опрос, дискуссия
10	**Технические средства защиты информации.** Виды технических средств защиты информации. Области применения технических средств защиты информации. Объекты, подлежащие технической защите информации. Организация системы технической защиты информации.	4	4			Устный опрос, дискуссия
11	**Аттестация объектов информатизации по требованиям безопасности информации.** Порядок аттестации объектов информатизации по требованиям безопасности информации. Основные мероприятия по аттестации объектов информатизации по требованиям безопасности информации.	4	4			Устный опрос, дискуссия
12	**Контроль состояния технической защиты конфиденциальной информации.** Задачи контроля состояния технической защиты конфиденциальной информации.	2	2			Устный опрос, дискуссия

	Периодичность и виды контроля. Проверка (оценка) эффективности применяемых мер технической защиты информации.					
13	**Форма аттестации**					Зачет
	Всего часов по образовательной программе	**36**	**36**			

Содержание разделов образовательной программы

Введение

Основные понятия, положения и определения. Предмет и объект защиты. Понятие угрозы безопасности. Классификация угроз. Классификация злоумышленников. Основные методы реализации угроз информационной безопасности. Причины, виды и каналы утечки информации.

Правовые и организационные методы защиты информации

Правовое регулирование в области безопасности информации. Государственная политика РФ в области безопасности информационных технологий. Законодательная база в области информационных технологий. Структура государственных органов, обеспечивающих безопасность информационных технологий. Общая характеристика организационных методов защиты.

Стандарты и спецификации в области информационной безопасности

Общие критерии безопасности. Подготовка и целевая направленность общих критериев. Организация общих критериев. Возможности и применимость, концепции общих критериев. Действующие стандарты и рекомендации в области информационной безопасности. Критерии оценки надежных компьютерных систем. Гармонизированные критерии европейских стран. Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при Президенте РФ. Особенности информационной безопасности компьютерных сетей. Рекомендации X.800.

Административный уровень информационной безопасности в информационно-вычислительной системе

Понятие политики безопасности. Анализ риска. Угрозы/видимость. Уязвимость/последствия. Учет информационных ценностей. Модели основных типов политик безопасности. Типы политик безопасности. Модель матрицы доступов Харрисон-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла- Лападула. Модель Low-Water-Mark. Модель ролевого разграничения доступа.

Криптографическая защита информации

Основные определения криптологии. Классификация методов криптографического

закрытия информации. Основы теории К.Шеннона. Основные криптографические модели. Алгоритмы шифрования. Симметричные методы шифрования. Асимметричные методы шифрования. Сравнение криптографических методов. Методы кодирования. Другие методы.

Защита информации в локальных ЭВМ и информационно-вычислительных сетях

Модели безопасности основных операционных систем. Механизмы защиты операционных систем.

Системы защиты программного обеспечения

Классификация систем защиты программного обеспечения. Достоинства и недостатки основных систем защиты. Упаковщики/шифраторы. Системы защиты от несанкционированного копирования. Системы защиты от несанкционированного доступа. Показатели эффективности систем защиты.

Защита информации в корпоративных сетях

Основы и цель политики безопасности в компьютерных сетях. Управление доступом. Идентификация и установление подлинности. Проверка полномочий субъектов на доступ к ресурсам. Регистрация обращений к защищаемым ресурсам. Реагирование на несанкционированные действия. Многоуровневая защита корпоративных сетей. Аутентификация. Анализ возможностей маршрутизации и прокси-серверов. Типы межсетевых экранов.

Защита от информационных инфекций. Вирусология.

Классификация компьютерных вирусов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов.

Технические средства защиты информации.

Виды технических средств защиты информации. Области применения технических средств защиты информации. Объекты, подлежащие технической защите информации. Организация системы технической защиты информации.

Аттестация объектов информатизации по требованиям безопасности информации.

Порядок аттестации объектов информатизации по требованиям безопасности информации. Основные мероприятия по аттестации объектов информатизации по требованиям безопасности информации.

Контроль состояния технической защиты конфиденциальной информации.

Задачи контроля состояния технической защиты конфиденциальной информации. Периодичность и виды контроля. Проверка (оценка) эффективности применяемых мер технической защиты информации.

4. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по образовательной программе

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения образовательной программы (модуля) формируются следующие компетенции:

- Способностью применять естественно-научные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности;
- Способностью использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности;
- Способностью осваивать методики использования программных средств для решения практических задач;
- Способность применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
- Способность в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
- Способность оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями;
- Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных.

Оценивание результатов освоения образовательной программы.

Итоговая аттестация обучающихся производится в форме завершающего тестирования

Шкала оценивания	Описание
Зачтено	70 и более процентов правильных ответов на вопросы итогового тестирования
Не зачтено	Менее 70 процентов правильных ответов на вопросы итогового тестирования

5. Учебно-методическое и информационное обеспечение образовательной программы

а) основная литература:

1. Щербаков А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учебное пособие: – Книжный мир, 2009 г. – 352 с. (http://www.knigafund.ru/books/181313).

2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие: – Директ-Медиа, 2015 г. – 253 с. http:/www.knigafund.ru/books/181420.

б) дополнительная литература:

1. Скрипник Д. А. Общие вопросы технической защиты информации:– Национальный Открытый Университет «ИНТУИТ», 2016 г.– 425 с.

в) вспомогательная литература

1. Карпов В.А. Методы и средства защиты информации. Курс лекций. М., МИРЭА. 2006.

2. Ярочкин В.И. Информационная безопасность. Учебник для вузов. Академический проект. 2006.

3. Баричев С.Г. Основы современной криптографии /С.Г.Баричев, В.В.Гончаров, Р.Е.Серов. – М.: Горячая линия – Телеком, 2001.- 121с.

4. Безруков Н.Н. Компьютерные вирусы. М., Наука, 1991.

5. Горячев Г.А. Методы и средства защиты информации. Методические указания к лабораторному практикуму. СПб., ЛЭТИ. 2006.

г) перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

1. ФСБ России [Электронный ресурс]. – Режим доступа: http://fsb.ru;
2. ФСТЭК России [Электронный ресурс]. – Режим доступа: http://fstec.ru.

Полезные учебно-методические и информационные материалы представлены на сайтах:

1. Бабаш, А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. – 2-е изд. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 216 с. – Режим доступа: http://znanium.com/bookread.php?book=432654;

2. Дубинин, Е.А. Оценка относительного ущерба безопасности информационной системы: Монография [электронный ресурс] / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 192 с. – Режим доступа: http://znanium.com/bookread.php?book=471787.