АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.О.04.10 Информационная безопасность

Специальность/направление подготовки: **09.03.01 Информатика и вычислительная техника**

Специализация/ направленность(профиль): **Проектирование программного обеспечения**

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели:

Ознакомить обучающихся с правовыми основами защиты информации, организационными методами защиты информации,

1.2. Задачи:

-ознакомления обучающихся с мерами и мероприятиями, обеспечивающими безопасность информации и информационных систем;
-рассмотреть основные подходы к защите информации;
-ознакомить обучающихся с наиболее широко применимыми видами технических и программных средств защиты информации.

2. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

ОПК-3 : Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3.1 : Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2 : Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.3 : Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

3. КРАТКАЯ ХАРАКТЕРИСТИКА СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Код занятия	Темы, планируемые результаты их освоения	Семестр	Часов	Прак. подг.
1.1	**Тема 1. Основные виды и источники атак на информацию Краткое содержание: 1.1 Современная ситуация в области информационной безопасности; 1.2 Категории информационной безопасности 1.3 Абстрактные модели защиты информации 1.4 Обзор наиболее распространенных методов "взлома" знать: современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования. /Лек/**	5	8	0
1.2	**Практическая работа 1. Шифрование и дешифрование файлов при помощи простейших программ Краткое содержание: Шифрование и дешифрование файлов при помощи простейших программ уметь: выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты владеть: методами защиты информации и программного обеспечения от несанкционированного доступа и копирования /Пр/**	5	8	0
1.3	**Тема 1. Основные виды и источники атак на информацию Краткое содержание: изучить современную ситуацию в области информационной безопасности; категории информационной безопасности; абстрактные модели защиты информации, обзор наиболее распространенных методов "взлома" знать: современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования уметь: выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты владеть: методами защиты информации и программного обеспечения от несанкционированного доступа и копирования /Ср/**	5	20	0
1.1	**Тема 2. Сетевая безопасность Краткое содержание: 2.1 Атакуемые сетевые компоненты 2.2 Уровни сетевых атак согласно модели OSI**	5	8	0

	знать: устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей /Лек/			
1.2	**Практическая работа 2. Обжим витой пары. Соединение рабочих станций в ЛВС. Краткое содержание: Обжим витой пары. Соединение рабочих станций в ЛВС уметь: проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи информации владеть: навыками монтажа локальной сети. /Пр/**	5	8	0
1.3	**Тема 2. Сетевая безопасность Краткое содержание: Сервера, рабочие станции, среда передачи информации и узлы коммутации сетей. Эталонная модель взаимодействия открытых систем OSI знать: устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей уметь: проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи информации владеть: навыками монтажа локальной сети. /Ср/**	5	20	0
1.4	**Зачет. Знать принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Владеть методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности /Зачёт/**	5	0	0
1.1	**Тема 3. Криптография Краткое содержание: 3.1 Классификация криптоалгоритмов 3.2 Симметричные криптоалгоритмы 3.3 Симметричные криптосистемы 3.4 Асимметричные криптоалгоритмы знать: классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем. /Лек/**	6	8	0
1.2	**Практическая работа 3. Методы и средства защиты информации в Microsoft Office Краткое содержание: Методы и средства защиты информации в Microsoft Office уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Пр/**	6	6	4
1.3	**Лабораторная работа 1. Криптоалгоритм TEA Краткое содержание: Реализация криптоалгоритма TEA на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/**	6	4	0
1.4	**Лабораторная работа 2. Криптоалгоритм Rijndael Краткое содержание: Реализация криптоалгоритма Rijndael на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/**	6	6	0
1.5	**Лабораторная работа 3. Передача зашифрованного текста криптоалгоритмом Rijndael Краткое содержание: Передача зашифрованного текста криптоалгоритмом Rijndael по локальной сети на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные**	6	4	0

	криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/			
1.6	**Лабораторная работа 4. Прием зашифрованного текста криптоалгоритмом Rijndael Краткое содержание: Прием зашифрованного текста криптоалгоритмом Rijndael по локальной сети и его расшифровка на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/**	6	2	0
1.7	**Тема 3. Криптография Краткое содержание: Тайнопись, криптография с ключом, симметричные криптоалгоритмы, асимметричные криптоалгоритмы, перестановочные, подстановочные, потоковые шифры, блочные шифры знать: классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем. уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Ср/**	6	34	0
1.1	**Тема 4. ПО и информационная безопасность. Комплексная система безопасности Краткое содержание: 4.1 Обзор современного ПО 4.2 Ошибки, приводящие к возможности атак на информацию 4.3 Основные положения по разработке ПО 4.4 Классификация информационных объектов 4.5 Политика ролей 4.6 Создание политики информационной безопасности 4.7 Методы обеспечения безотказности знать: информационная безопасность в операционных системах, прикладных программах, ошибки, приводящие к возможности атак на информацию, основные положения по разработке ПО, классификацию по требуемой степени безотказности, классификация по уровню конфиденциальности, требования по работе с конфиденциальной информацией, уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак. /Лек/**	6	8	0
1.2	**Практическая работа 4. Генерация ключей. Шифрование и расшифровка сообщений в программе PGP. Краткое содержание: Генерация ключей. Шифрование и расшифровка сообщений в программе PGP. уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак. /Пр/**	6	4	0
1.3	**Практическая работа 5. Изменение парольной фразы. PGP диск Краткое содержание: Изменение парольной фразы. PGP диск уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных**	6	4	0

	уровнях: аппаратном, программном, информационном владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак. /Пр/			
1.4	**Практическая работа 6. Зашифровка и расшифровка данных алгоритмом RSA. Краткое содержание: Зашифровка и расшифровка данных алгоритмом RSA уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак. /Пр/**	6	2	0
1.5	**Тема 4. ПО и информационная безопасность. Комплексная система безопасности Краткое содержание: обзор современного ПО, ошибки, приводящие к возможности атак на информацию, основные положения по разработке ПО. Классификация по требуемой степени безотказности, классификация по уровню конфиденциальности, требования по работе с конфиденциальной информацией. Рекомендуемые роли: специалист по информационной безопасности, владелец информации, поставщик аппаратного и программного обеспечения, разработчик системы и/или программного обеспечения, линейный менеджер или менеджер отдела, операторы, аудиторы. знать: информационная безопасность в операционных системах, прикладных программах, ошибки, приводящие к возможности атак на информацию, основные положения по разработке ПО, классификацию по требуемой степени безотказности, классификация по уровню конфиденциальности, требования по работе с конфиденциальной информацией, уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак. /Ср/**	6	35	0
1.6	**Экзамен. Знать принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Владеть методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности /Экзамен/**	6	27	0

4. ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Зачёт: 5 семестр

Экзамен: 6 семестр

Разработчик программы Яшин Д.Д. _____

И.о. зав. кафедрой Одинокова Е.В._____