МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ОБРАЗОВАТЕЛЬНАЯ АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛЖСКИЙ УНИВЕРСИТЕТ имени В.Н. ТАТИЩЕВА» (институт)

УТВЕРЖДАЮ
Проректор по учебной работе
_____Т.Б. Исакова
«10» июня 2019 г.

Рабочая программа дисциплины
«Защита информации»
для направления подготовки
09.03.02 «Информационные системы и технологии»

Квалификация (степень) выпускника - бакалавр

Тольятти 2019

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО, ПООП по направлению подготовки 09.03.02 «Информационные системы и технологии» (уровень высшего образования: бакалавриат) и учебного плана.

Программа обсуждена и рекомендована к использованию и (или) изданию решением кафедры на заседании кафедры «ИиСУ»
протокол № 10 от «24» мая 2019 г.
Зав. кафедрой ИиСУ, д.т.н., профессор С.В. Краснов

Одобрена Учебно-методическим советом вуза
протокол № 5 от «19» июня 2019 г.
Проректор по учебной работе, к.п.н., доцент Т.Б. Исакова

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

В результате освоения дисциплины у обучающихся должны быть сформированы следующие общепрофессиональные компетенции и профессиональные компетенции:

Наименование компетенции	Код компетенции
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
Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Данная учебная дисциплина относится к вариативной части образовательной программы 09.03.02 «Информационные системы и технологии».

В таблице 1 представлен перечень компетенций с указанием перечня дисциплин, формирующих эти компетенции согласно учебному плану ОПОП

Таблица 1

Шифр дисциплины	Наименование дисциплины	Этап формирования компетенции*
1	2	3
Очная форма обучения		
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;		
Б1.О.21	Информатика	1,2
Б1.О.06	Компьютерные технологии поиска информации	2
Б1.В.02	Сети и телекоммуникации	6
Б1.В.04	**Защита информации**	**7**
Б1.В.14	Корпоративные информационные системы	7
Б3.О.01	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8

ПК-1. Управление программно- аппаратными средствами информационных служб инфокоммуникационной системы организации		
Б1.В.13	Пакеты и комплексы прикладных программ	1
Б1.В.07	WEB технологии	1,2
Б1.В.08	Базы данных	3,4
Б2.В.01(У)	Учебная практика. Ознакомительная практика	4
Б1.В.01	Инженерная и компьютерная графика	4,5
Б1.В.05	Моделирование	5
Б1.В.06	Стандартизация	5
Б1.В.11	Системное программное обеспечение	5
Б1.В.10	Базовые технологии и процессы	5,6
Б1.В.02	Сети и телекоммуникации	6
Б1.В.04	Надежность систем	6
Б1.В.ДВ.01.01	Электронный бизнес	6
Б1.В.ДВ.01.02	Разработка интернет приложений	6
Б1.В.ДВ.02.01	Имитационное моделирование	6
Б1.В.ДВ.02.02	Теория автоматов	6
Б1.В.09	Методы и средства проектирование информационных систем и технологий	6,7
Б1.В.03	**Защита информации**	**7**
Б1.В.14	Корпоративные информационные системы	7
Б1.В.ДВ.03.01	Инструментальные средства информационных систем	7
Б1.В.ДВ.03.02	Архитектура информационных систем	7
Б2.В.02(П)	Производственная практика. Технологическая (проектно-технологическая) практика	8
Б3.О.01	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8
Заочная форма обучения		
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;		
Б1.О.21	Информатика	1,2
Б1.О.06	Компьютерные технологии поиска информации	2
Б1.В.02	Сети и телекоммуникации	6
Б1.В.14	Корпоративные информационные системы	7
Б1.В.04	**Защита информации**	**7**
Б3.О.01	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	10
ПК-1. Управление программно- аппаратными средствами информационных служб инфокоммуникационной системы организации		
Б1.В.13	Пакеты и комплексы прикладных программ	1
Б1.В.07	WEB технологии	1,2
Б1.В.08	Базы данных	3,4
Б2.В.01(У)	Учебная практика. Ознакомительная практика	4
Б1.В.01	Инженерная и компьютерная графика	5,6
Б1.В.05	Моделирование	6
Б1.В.06	Стандартизация	6
Б1.В.11	Системное программное обеспечение	6
Б1.В.09	Методы и средства проектирование информационных систем и технологий	6,7
Б1.В.10	Базовые технологии и процессы	6,7
Б1.В.02	Сети и телекоммуникации	8
Б1.В.03	**Защита информации**	**8**
Б1.В.04	Надежность систем	8
Б1.В.ДВ.01.01	Электронный бизнес	8
Б1.В.ДВ.01.02	Разработка интернет приложений	8
Б1.В.ДВ.02.01	Имитационное моделирование	8
Б1.В.ДВ.02.02	Теория автоматов	8

Б1.В.14	Корпоративные информационные системы	9
Б1.В.ДВ.03.01	Инструментальные средства информационных систем	9
Б1.В.ДВ.03.02	Архитектура информационных систем	9
Б2.В.02(П)	Производственная практика. Технологическая (проектно-технологическая) практика	10
Б3.О.01	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	10
Очно-заочной форма обучения		
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;		
Б1.О.21	Информатика	1,2
Б1.О.06	Компьютерные технологии поиска информации	2
Б1.В.02	Сети и телекоммуникации	8
Б1.В.04	**Защита информации**	**8**
Б1.В.14	Корпоративные информационные системы	9
Б3.О.01	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	10
ПК-1. Управление программно- аппаратными средствами информационных служб инфокоммуникационной системы организации		
Б1.В.13	Пакеты и комплексы прикладных программ	1
Б1.В.07	WEB технологии	1,2
Б1.В.08	Базы данных	3,4
Б2.В.01(У)	Учебная практика. Ознакомительная практика	4
Б1.В.01	Инженерная и компьютерная графика	5,6
Б1.В.05	Моделирование	6
Б1.В.06	Стандартизация	6
Б1.В.11	Системное программное обеспечение	6
Б1.В.09	Методы и средства проектирование информационных	6,7

	систем и технологий	
Б1.В.10	Базовые технологии и процессы	6,7
Б1.В.02	Сети и телекоммуникации	8
Б1.В.03	**Защита информации**	**8**
Б1.В.04	Надежность систем	8
Б1.В.ДВ.01.01	Электронный бизнес	8
Б1.В.ДВ.01.02	Разработка интернет приложений	8
Б1.В.ДВ.02.01	Имитационное моделирование	8
Б1.В.ДВ.02.02	Теория автоматов	8
Б1.В.14	Корпоративные информационные системы	9
Б1.В.ДВ.03.01	Инструментальные средства информационных систем	9
Б1.В.ДВ.03.02	Архитектура информационных систем	9
Б2.В.02(П)	Производственная практика. Технологическая (проектно-технологическая) практика	10
Б3.О.01	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	10

* в качестве этапа формирования компетенций используются номера семестров согласно учебного плана ОПОП

В результате изучения дисциплины обучающийся должен:

Знать:
- принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);
- процедуры создания и сопровождения программных модулей и компонент (ПК-1)

Уметь:
- 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);
- разрабатывать и сопровождать программные модули и компоненты (ПК-1)

Владеть:
- навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности (ОПК-3);
- навыками разработки и сопровождения программных модулей; осуществляет интеграцию программных модулей и компонент и верификации выпусков программного продукта (ПК-1)

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

ДНЕВНАЯ ФОРМА ОБУЧЕНИЯ

Вид учебной работы	**Всего**	**Семестр**
		7
Общая трудоёмкость дисциплины	144 час 4 з.е.	144 час 4 з.е.
Контактная работа с преподавателем (всего)	64	64
В том числе:		64
Лекции	32	32
Практические / семинарские занятия	-	-
Лабораторные занятия	32	32
Консультации	-	-
Самостоятельная работа (всего)	44 час	44
В том числе (если есть):		
Курсовой проект / работа	-	-
Расчетно-графическая работа	-	-
Контрольная работа	-	-
Реферат / эссе / доклад	-	-
Иное	*44*	*44*
Вид промежуточной аттестации (зачет, экзамен)	Экзамен (36)	Экзамен (36)

ЗАОЧНАЯ ФОРМА

Вид учебной работы	**Всего**	**Семестр**
		7
Общая трудоёмкость дисциплины	144 час 4 з.е.	144 час 4 з.е.
Контактная работа с преподавателем (всего)	16	16
В том числе:		
Лекции	8	8
Практические / семинарские занятия	-	-
Лабораторные занятия	8	8
Консультации	-	-
Самостоятельная работа (всего)	92	92
В том числе (если есть):		
Курсовой проект / работа	-	-
Расчетно-графическая работа	-	-
Контрольная работа	-	-
Реферат / эссе / доклад	-	-
Иное	*92*	*92*
Вид промежуточной аттестации (зачет, экзамен)	Экзамен (36)	Экзамен (36)

ОЧНО-ЗАОЧНАЯ ФОРМА

Вид учебной работы	**Всего**	**Семестр**
		8
Общая трудоёмкость дисциплины	144 час 4 з.е.	144 час 4 з.е.
Контактная работа с преподавателем (всего)	44	44
В том числе:		
Лекции	26	26
Практические / семинарские занятия	-	-
Лабораторные занятия	26	26
Консультации	-	-
Самостоятельная работа (всего)	58	58
В том числе (если есть):		
Курсовой проект / работа	-	-
Расчетно-графическая работа	-	-
Контрольная работа	-	-
Реферат / эссе / доклад	-	-
Иное	*58*	*58*
Вид промежуточной аттестации (зачет, экзамен)	Экзамен (36)	Экзамен (36)

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

ДНЕВНАЯ ФОРМА ОБУЧЕНИЯ

№ п/п	Тема	Количество часов на				Форма контроля
		лекции	практические /семинарские занятия	лабораторные занятия	самостоятельную работу	
Семестр 7						
1	Тема 1. Основные понятия и определения предмета защиты информации	2			3	тест АСТ
2	Тема 2. Разграничение доступа к ресурсам	2			3	тест АСТ
3	Тема 3. Идентификация и аутентификация субъектов	2			3	тест АСТ
4	Тема 4. Методы и	2			3	тест АСТ

	средства криптографической защиты					
5	Тема 5. Контроль целостности информации. Электронно-цифровая подпись	2			3	тест АСТ
6	Тема 6. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей	2			3	тест АСТ
7	Тема 7. Защита программного обеспечения от несанкционированного использования	4			3	тест АСТ
8	Тема 8. Защита от разрушающих программных воздействий	4			3	тест АСТ
9	Тема 9. Защита информации в компьютерных сетях	4		32	11	тест АСТ, отчет по лабораторной работе
10	Тема 10. Инженерно-техническая защита информации	4			3	тест АСТ
11	Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	4			3	тест АСТ
Итого		32		32	44	Экзамен (36)

ЗАОЧНАЯ ФОРМА

№ п/п	Тема	Количество часов на				Форма контроля
		лекции	практические /семинарские	лабораторные	самостоятельную	

			занятия	занятия	работу	
Семестр 7						
1	Тема 1. Основные понятия и определения предмета защиты информации	0.5			9	тест АСТ
2	Тема 2. Разграничение доступа к ресурсам	0.5			9	тест АСТ
3	Тема 3. Идентификация и аутентификация субъектов	0.5			9	тест АСТ
4	Тема 4. Методы и средства криптографической защиты	0.5			9	тест АСТ
5	Тема 5. Контроль целостности информации. Электронно-цифровая подпись	1			9	тест АСТ
6	Тема 6. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей	1			9	тест АСТ
7	Тема 7. Защита программного обеспечения от несанкционированного использования	1			9	тест АСТ
8	Тема 8. Защита от разрушающих программных воздействий	1			9	тест АСТ
9	Тема 9. Защита информации в компьютерных сетях	1		8	2	тест АСТ, отчет по лабораторной работе
10	Тема 10. Инженерно-техническая защита информации	1			9	тест АСТ

11	Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	1			9	тест АСТ
Итого		8		8	92	Экзамен (36)

ОЧНО-ЗАОЧНАЯ ФОРМА

№ п/п	Тема	Количество часов на				Форма контроля
		лекции	практические /семинарские занятия	лабораторные занятия	самостоятельную работу	
Семестр 8						
1	Тема 1. Основные понятия и определения предмета защиты информации	2			5	тест АСТ
2	Тема 2. Разграничение доступа к ресурсам	2			5	тест АСТ
3	Тема 3. Идентификация и аутентификация субъектов	2			5	тест АСТ
4	Тема 4. Методы и средства криптографической защиты	2			5	тест АСТ
5	Тема 5. Контроль целостности информации. Электронно-цифровая подпись	2			5	тест АСТ
6	Тема 6. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей	2			5	тест АСТ
7	Тема 7. Защита программного	2			5	тест АСТ

	обеспечения от несанкционированного использования					
8	Тема 8. Защита от разрушающих программных воздействий	2			5	тест АСТ
9	Тема 9. Защита информации в компьютерных сетях	6		26	8	тест АСТ, отчет по лабораторной работе
10	Тема 10. Инженерно-техническая защита информации	2			5	тест АСТ
11	Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.	2			5	тест АСТ
Итого		26		26	58	Экзамен (36)

4.2. КРАТКОЕ СОДЕРЖАНИЕ ЛЕКЦИОННОГО КУРСА

Тема 1. Основные понятия и определения предмета защиты информации
Санкционированный и несанкционированный доступ. Базовые свойства безопасности информации. Угрозы безопасности и каналы реализации угроз. Основные принципы обеспечения информационной безопасности. Ценность информации. Меры обеспечения безопасности компьютерных систем. Характеристика способов защиты компьютерной информации с помощью аппаратно-программных мер.

Тема 2. Разграничение доступа к ресурсам
Политики безопасности. Классификация политик безопасности. Политики избирательного разграничения доступа. Мандатные политики безопасности. Контроль доступа, базирующийся на ролях. Политики безопасности контроля целостности информационных ресурсов.

Тема 3. Идентификация и аутентификация субъектов
Классификация подсистем идентификации и аутентификации субъектов. Парольные системы идентификации и аутентификации пользователей. Идентификация и аутентификация пользователей с использованием технических устройств. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.

Тема 4. Методы и средства криптографической защиты

Принципы криптографической защиты информации. Традиционные симметричные криптосистемы: шифрование методом замены, шифрование методами перестановки, шифрование методом гаммирования. Элементы криптоанализа. Современные симметричные системы шифрования: стандарт шифрования DES (США), отечественный стандарт симметричного шифрования. Асимметричные криптосистемы: недостатки симметричных криптосистем и принципы асимметричного шифрования, однонаправленные функции, алгоритм шифрования RSA,

Тема 5. Контроль целостности информации. Электронно-цифровая подпись
Проблема обеспечения целостности информации. Функции хэширования и электронно-цифровая подпись. Инфраструктура открытых ключей PKI.

Тема 6. Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей
Типовые схемы хранения ключевой информации. Защита баз данных аутентификации в ОС Windows и UNIX. Иерархия ключевой информации. Распределение ключей. Протоколы безопасной удаленной аутентификации пользователей.

Тема 7. Защита программного обеспечения от несанкционированного использования
Проблема защиты программного обеспечения от несанкционированного использования. Модульная архитектура технических средств защиты ПО от несанкционированного использования. Функционирование подсистем и модулей системы защиты ПО от несанкционированного использования. Электронные ключи HASP. Защита ПО от изучения: базовые методы нейтрализации систем защиты от несанкционированного использования, понятие и средства обратного проектирования, локализация кода модуля защиты посредством отлова WinAPI функций в режиме отладки, базовые методы противодействия отладчикам, базовые методы противодействия дизассемблированию ПО, защита от отладки, основанная на особенностях конвейеризации процессора, использование недокументированных инструкций и недокументированных возможностей процессора, шифрование кода программы как универсальный метод противодействия отладке и дизассемблированию.

Тема 8. Защита от разрушающих программных воздействий
Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и РПВ. Компьютерные вирусы как класс РПВ. Защита от РПВ. Изолированная программная среда.

Тема 9. Защита информации в компьютерных сетях
Основные угрозы и причины уязвимости сети INTERNET. Классификация типовых удаленных атак на интрасети. Подходы к защите от типовых удаленных атак. Ограничение доступа в сеть. Межсетевые экраны. Виртуальные частные сети (VPN). Доменная архитектура в Windows NT. Служба Active Directory. Централизованный контроль удаленного доступа. Серверы аутентификации.

Тема 10. Инженерно-техническая защита информации
Радиомикрофоны. Устройства перехвата телефонных сообщений. Специализированные устройства. Обнаружение, локализация и подавление закладных подслушивающих устройств. Предотвращение утечки информации через побочные электромагнитные излучения и наводки.

Тема 11. Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму.
Показатели защищенности средств вычислительной техники от НСД. Статья 272 УК РФ.

Статья 273 УК РФ. Статья 274 УК РФ. Статья 146. Нарушение авторских и смежных прав. Статья 147. Нарушение изобретательских и патентных прав. Законодательное противодействие распространению террористических материалов в Интернет. Проблемы экспертизы информационных материалов, содержащих признаки идеологии терроризма.

4.3. ТЕМАТИКА ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа № 1 Базовые механизмы безопасности коммутаторов
Лабораторная работа № 2 Безопасность на основе сегментации трафика
Лабораторная работа № 3 Безопасность на основе протокола IEEE 802.1x
Лабораторная работа № 4 Списки контроля доступа ACL
Лабораторная работа № 5 Утилита iptables
Лабораторная работа № 6 Туннелирование соединений с использованием протокола SSL
Лабораторная работа № 7 Удаленное управление по защищенному протоколу SSH
Лабораторная работа № 8 Протокол PPPoE

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

5.1. Основная литература.

Гашков, С. Б. Криптографические методы защиты информации [Текст] : учеб. пособие доп. УМО . - М. : "Академия", 2010. - 298 с - 4 НТБ ВУиТ.

Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие доп. УМО . - М. : "Академия", 2012. - 331 с- 6 НТБ ВУиТ.

Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт] https://www.biblio-online.ru/bcode/444046

Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт] https://www.biblio-online.ru/bcode/433715

5.2. Дополнительная литература.

Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт] https://www.biblio-online.ru/bcode/437163

Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт] https://www.biblio-online.ru/bcode/434171

5.3. Методические разработки кафедры.

Горбачевская, Е. Н. Методы защиты информации : лаб. практикум / Е. Н. Горбачевская, С. С.. - Тольятти : ВУиТ, 2014. - 60 с -

Аникин В. И., Горбачевская, Е. Н. Методы и средства защиты компьютерной информации : учеб. пособие . - Тольятти : ВУиТ, 2007. - 274 с

5.4. Ресурсы информационно-коммуникационной сети «Интернет».

Адрес Интернет ресурса	Название Интернет ресурса	Режим доступа

http://intuit.ru/	Интернет-университет информационных технологий	Свободный
http://vkit.ru/	Сайт журнала «Вестник компьютерных и информационных технологий»	Свободный
http://ru.wikipedia.org/.	Свободная общедоступная мультиязычная универсальная интернет-энциклопедия	Свободный

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (Приложение 1) включает в себя:

- распределение процесса формирования компетенций по темам (разделам) дисциплины (паспорт фонда оценочных средств);
- закрепление видов оценочных средств за компетенциями (паспорт фонда оценочных средств);
- критерии оценивания уровня сформированности компетенций;
- критерии конкретного оценочного средства;
- оценочные средства.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1 Методические рекомендации для обучающихся

Дисциплина «**Защита информации**» изучается в течение двух семестров. При планировании и организации времени, необходимого на изучение обучающимся дисциплины, необходимо придерживаться следующих рекомендаций.

В период между сессиями студенты должны вести конспект лекций, изучать теоретический материал в соответствии с программой курса, выполнять предложенные преподавателем задания для самостоятельной работы, готовиться к сдаче зачета и экзамена, прорабатывая необходимый материал согласно перечню вопросов для подготовки к зачету и экзамену и списку рекомендованной литературы.

Выполнение лабораторных работ относится к числу обязательных видов работ. Перед выполнением работы необходимо внимательно ознакомиться с теоретическим материалом, представленным в методических указаниях к соответствующей лабораторной работе. При необходимости можно воспользоваться рекомендуемой литературой. В ходе выполнения работы необходимо руководствоваться порядком выполнения лабораторной работы и указаниями преподавателя, при этом должны соблюдаться правила техники безопасности. Результатом выполнения работы является отчёт, который должен быть аккуратно оформлен и выполнен в соответствии с требованиями, приведенными в методических указаниях.

В указанное преподавателем время обучающиеся защищают отчеты. Защита проводится в виде собеседования по контрольным вопросам, приведенным в методических указаниях. Кроме того, преподаватель может задавать дополнительные вопросы, касающиеся результатов эксперимента, выводов по результатам опытов и т.п. К промежуточной аттестации допускаются обучающиеся, выполнившие все лабораторные работы и защитившие отчеты по ним. При наличии задолженности по лабораторным работам, по согласованию с преподавателем, возможна замена работы по выполнению отчета на реферат по теме соответствующего лабораторного занятия с последующей его защитой.

В семестре изучения дисциплины учебным планом предусмотрен курсовой проект. При получении задания, необходимо внимательно с ним ознакомиться и, в случае возникновения вопросов, задать их преподавателю. Регулярное посещение консультаций,

внимательное изучение методических указаний к выполнению курсового проекта, а так же строгое соблюдение графика выполнения проекта позволит избежать ненужных проблем. Оценка за курсовой проект выставляется по результатам его защиты.

В течение семестра и во время сессии основным видом подготовки являются самостоятельные занятия. Они включают в себя изучение вопросов, вынесенных на самостоятельное изучение, оформление отчетов по лабораторным работам, курсовое проектирование, а так же подготовку к промежуточной аттестации

Систематическая работа в соответствии с программой дисциплины – условие успешного освоения материала.

7.2 Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Медиаматериалы также следует использовать и адаптировать с учетом индивидуальных особенностей обучения лиц с ОВЗ.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

8. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

При проведение занятий по дисциплине используются следующие программные продукты:

Linux (свободное ПО)

Windows (для академических организациях, лицензия MicrosoftImagine (ранее MSDNAA, DreamSpark);

FileZillaFTPClient (свободное многоязычный FTP – клиент с открытым исходным кодом);

Google Chrome (свободноеПО);

9. НЕОБХОДИМАЯ МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

ауд.Б-604

офисная мебель на 20 мест, демонстрационное оборудование: экран – 1 шт.; проектор – 1 шт.; 9 ПК с доступом в Интернет и ЭИОС;

Учебно-лабораторный комплекс «Корпоративные компьютерные сети» (ЮУрГУ-НПИ «Учебная техника и технологии», Челябинск, 2011, №5)

Комплект коммутационного оборудования D-Link.

Разработчик:

Кафедра ИиСУ	**профессор кафедры ИиСУ**	**Е.Н. Горбачевская**
(место работы)	*(занимаемая должность)*	*(инициалы, фамилия)*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ, ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Защита информации

Паспорт фонда оценочных средств

№ п/п	Код и наименование формируемой компетенции	Этапы формирования компетенции	Наименование оценочного средства
1	ОПК-3 ПК-2	Тема 1-11	Тест АСТ, собеседование по лабораторным работам, курсовой проект

Критерии оценивания уровня сформированности компетенций

Уровень освоения компетенции*	**Планируемые результаты обучения**** (показатели освоения компетенции)	**Критерии оценивания результатов обучения**				
		1	2	3	4	5
Первый уровень (пороговый) **(ОПК-3) –I** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **З1 (ОПК-3) –I**	Не знает	Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объеме	Демонстрирует высокий уровень знаний
	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **У1 (ОПК-3) –I**	Не умеет	Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания в базовом (стандартном) объеме	Демонстрирует высокий уровень умений
	Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности **В1 (ОПК-3) –I**	Не владеет	Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приемами и культурой работы с техническим и программами	Демонстрирует владения на высоком уровне
	Владеть: навыками принятия решений по администрированию сетевой подсистемы инфокоммуникационной системы организации **В1 (ОПК-3) –I**	Не владеет	Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приемами и культурой работы с техническим и программами	Демонстрирует владения на высоком уровне
Уровень освоения компетенции*	**Планируемые результаты обучения**** (показатели освоения компетенции)	**Критерии оценивания результатов обучения**				

		1	2	3	4	5
Первый уровень (пороговый) **(ПК-1) –I** Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	**Знать:** процедуры создания и сопровождения программных модулей и компонент **З1 (ПК-1) –I**	Не знает	Допускает грубые ошибки	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объеме	Демонстрирует высокий уровень знаний
	Уметь: разрабатывать и сопровождать программные модули и компоненты **У1 (ПК-1) –I**	Не умеет	Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания в базовом (стандартном) объеме	Демонстрирует высокий уровень умений
	Владеть: Владеет: навыками разработки и сопровождения программных модулей; осуществляет интеграцию программных модулей и компонент и верификации выпусков программного продукта **В1 (ПК-1) –I**	Не владеет	Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приемами и культурой работы с техническими программами	Демонстрирует владения на высоком уровне

Критерии конкретного оценочного средства (согласно ПОЛОЖЕНИЮ о промежуточной аттестации обучающихся ВУиТ по программам высшего образования – программам бакалавриата и программам специалитета)

По итогам тестирования оценка знаний обучающегося производится в соответствии со следующими критериями:

правильных ответов 0-39% – «неудовлетворительно»/«не зачтено»;
правильных ответов 40-59% – «удовлетворительно»/«зачтено»;
правильных ответов 60-79% – «хорошо»/«зачтено»;
правильных ответов 80-100% – «отлично»/«зачтено».

Вопросы к экзамену

Основные понятия и определения предмета защиты информации. Санкционированный и несанкционированный доступ. Базовые свойства безопасности информации. Угрозы безопасности и каналы реализации угроз.

Основные понятия и определения предмета защиты информации. Основные принципы обеспечения информационной безопасности. Ценность информации.

Основные понятия и определения предмета защиты информации. Меры обеспечения безопасности компьютерных систем. Характеристика способов защиты компьютерной информации с помощью аппаратно-программных мер.

Разграничение доступа к ресурсам. Политики безопасности. Классификация политик безопасности.

Разграничение доступа к ресурсам. Политики избирательного разграничения доступа. Мандатные политики безопасности. Контроль доступа, базирующийся на ролях. Политики безопасности контроля целостности информационных ресурсов.

Идентификация и аутентификация субъектов. Классификация подсистем идентификации и аутентификации субъектов. Парольные системы идентификации и аутентификации пользователей.

Идентификация и аутентификация субъектов. Идентификация и аутентификация пользователей с использованием технических устройств. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.

Методы и средства криптографической защиты. Принципы криптографической защиты информации.

Методы и средства криптографической защиты. Традиционные симметричные криптосистемы: шифрование методом замены, шифрование методами перестановки, шифрование методом гаммирования. Элементы криптоанализа.

Методы и средства криптографической защиты. Современные симметричные системы шифрования: стандарт шифрования DES (США), отечественный стандарт симметричного шифрования.

Методы и средства криптографической защиты. Асимметричные криптосистемы: недостатки симметричных криптосистем и принципы асимметричного шифрования, однонаправленные функции, алгоритм шифрования RSA.

Контроль целостности информации. Электронно-цифровая подпись. Проблема обеспечения целостности информации.

Контроль целостности информации. Электронно-цифровая подпись. Функции хэширования и электронно-цифровая подпись.

Контроль целостности информации. Электронно-цифровая подпись. Инфраструктура открытых ключей PKI.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Типовые схемы хранения ключевой информации.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Защита баз данных аутентификации в ОС Windows и UNIX.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Иерархия ключевой информации. Распределение ключей.

Хранение и распределение ключевой информации. Протоколы безопасной аутентификации пользователей. Протоколы безопасной удаленной аутентификации пользователей.

Защита программного обеспечения от несанкционированного использования. Проблема защиты программного обеспечения от несанкционированного использования.

Защита программного обеспечения от несанкционированного использования. Модульная архитектура технических средств защиты ПО от несанкционированного использования.

Защита программного обеспечения от несанкционированного использования. Функционирование подсистем и модулей системы защиты ПО от несанкционированного использования.

Защита программного обеспечения от несанкционированного использования. Электронные ключи HASP. Защита ПО от изучения: базовые методы нейтрализации систем защиты от несанкционированного использования, понятие и средства обратного проектирования, локализация кода модуля защиты посредством отлова WinAPI функций в режиме отладки, базовые методы противодействия отладчикам, базовые методы противодействия дизассемблированию ПО, защита от отладки, основанная на особенностях конвейеризации процессора, использование недокументированных инструкций и недокументированных возможностей процессора, шифрование кода программы как универсальный метод противодействия отладке и дизассемблированию.

Защита от разрушающих программных воздействий. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и РПВ.

Защита от разрушающих программных воздействий. Компьютерные вирусы как класс РПВ. Защита от РПВ. Изолированная программная среда.

Защита информации в компьютерных сетях. Основные угрозы и причины уязвимости сети INTERNET.

Защита информации в компьютерных сетях. Классификация типовых удаленных атак на интрасети. Подходы к защите от типовых удаленных атак.

Защита информации в компьютерных сетях. Ограничение доступа в сеть. Межсетевые экраны. Виртуальные частные сети (VPN).

Защита информации в компьютерных сетях. Доменная архитектура в Windows NT. Служба Active Directory.

Защита информации в компьютерных сетях. Централизованный контроль удаленного доступа. Серверы аутентификации.

Инженерно-техническая защита информации. Радиомикрофоны. Устройства перехвата телефонных сообщений.

Инженерно-техническая защита информации. Специализированные устройства. Обнаружение, локализация и подавление закладных подслушивающих устройств.

Инженерно-техническая защита информации. Предотвращение утечки информации через побочные электромагнитные излучения и наводки.

Руководящие документы России. Правовое обеспечение информационной безопасности и противодействию терроризму. Показатели защищенности средств вычислительной техники от НСД.

Правовое обеспечение информационной безопасности и противодействию терроризму. Статья 272 УК РФ. Статья 273 УК РФ. Статья 274 УК РФ. Статья 146. Нарушение авторских и смежных прав. Статья 147. Нарушение изобретательских и патентных прав.

Правовое обеспечение информационной безопасности и противодействию терроризму. Законодательное противодействие распространению террористических материалов в

Интернет.

Правовое обеспечение информационной безопасности и противодействию терроризму. Проблемы экспертизы информационных материалов, содержащих признаки идеологии терроризма.

Тесты

Тесты АСТ установлены в Центре тестирования по адресу Ленинградская 16, ауд 104