Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ряполов Петр Алексеевич
Должность: декан ЕНФ
Дата подписания: 10.11.2026 11:44:28
Уникальный программный ключ:
efd3ecdbd183f7649d0e3a33c230c6662946c7c99039b2b268921fde408c1fb6

Аннотация к рабочей программе дисциплины
«Методы и средства защиты компьютерной информации»

Цель преподавания дисциплины

Целью преподавания дисциплины является изложение основ методики комплексной защиты информационных систем на основе программных и программно-аппаратных средств, а также требований к системам защиты информации.

Задачи изучения дисциплины

– изучение классификации угроз информационной безопасности;
– изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
– изучение структуры политики безопасности организации и основных этапов ее разработки;
– ознакомление с симметричными и ассиметричными криптосистемами, изучение алгоритмов RSA, Виженера, AES, электронно-цифровой подписи;
– изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем идентификации и аутентификации;
– изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
– изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
– изучение основных требований и рекомендаций по защите информации в компьютерных системах;
– изучение средств анализа защищенности и обнаружения сетевых атак;
– изучение основных юридических законов в области защиты информации.

Компетенции, формируемые в результате освоения дисциплины, и индикаторы их достижения

ПК-5. Способен осуществлять контроль качества программного обеспечения (надежности, безопасности, удобства использования) и применять инструменты и технологии обеспечения качества	ПК-5.1. Анализирует требования на реализуемость и пригодность к тестированию, формируя отчёт о корректности документации
	ПК-5.2. Разрабатывает требования к тестированию на основе требований к программно-информационной системе
ПК-8. Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта	ПК-8.3. Контролирует выполнение заданий программистами

Разделы дисциплины

1. Основные понятия и анализ угроз информационной безопасности
2. Проблемы информационной безопасности сетей
3. Политика безопасности
4. Криптографическая защита информации
5. Технологии аутентификации
6. Технологии межсетевых экранов
7. Технологии защиты от вирусов
8. Требования к системам защиты информации
9. Основы правового обеспечения защиты информации

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета
фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____ М.О. Таныгин
(подпись, инициалы, фамилия)

«30» ____08____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты компьютерной информации
(наименование дисциплины)

ОПОП ВО 09.03.04 Программная инженерия,
шифр и наименование направления подготовки

направленность (профиль) «Разработка программно-информационных систем»
наименование направленности (профиля)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины Методы и средства защиты компьютерной информации составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 09.03.04Программная инженерия на основании учебного плана ОПОП ВО 09.03.04Программная инженерия, направленность Разработка программно-информационных систем, одобренного Ученым советом университета (протокол №9 «25» 06 2021 г.).

Рабочая программа дисциплины Методы и средства защиты компьютерной информации обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 09.03.04 Программная инженерия, направленность Разработка программно-информационных системна заседании кафедры информационной безопасности Протокол №11 28« 06 »2021 г.

Зав. кафедрой Таныгин М.О.

Разработчик программы

к.воен.н., доцент ХанисА.Л.

Согласовано: на заседании кафедры программной инженерии № 12 «01» 07 2021 г.

Зав. кафедрой Малышев А.В.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Методы и средства защиты компьютерной информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность Разработка программно-информационных систем, одобренного Ученым советом университета протокол №2 «18» 06 2022 г., на заседании кафедры ИБ, протокол №11 от 30.06.2022 .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины Методы и средства защиты компьютерной информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность Разработка программно-информационных систем, одобренного Ученым советом университета протокол №_ «__»2021 г., на заседании кафедры _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № 1 от 29.08.2024.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Медуненко А.Л.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № 11 от 24.06.25г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Тюлькин М.О.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол № 9 «27» 03 2024 г.), на заседании кафедры информационной безопасности, протокол № 11 от 30.06.2026 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ М.О. Тюлькин

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № от _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № от _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины является изложение основ методики комплексной защиты информационных систем на основе программных и программно-аппаратных средств, а также требований к системам защиты информации.

1.2 Задачи дисциплины

– изучение классификации угроз информационной безопасности;

– изучение принципов действия основных видов сетевых атак и методов борьбы с ними;

– изучение структуры политики безопасности организации и основных этапов ее разработки;

– ознакомление с симметричными и ассиметричными криптосистемами, изучение алгоритмов RSA, Виженера, AES, электронно-цифровой подписи;

– изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем идентификации и аутентификации;

– изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;

– изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;

– изучение основных требований и рекомендаций по защите информации в компьютерных системах;

– изучение средств анализа защищенности и обнаружения сетевых атак;

– изучение основных юридических законов в области защиты информации.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-5	Способен осуществлять контроль качества программного обеспечения (надежности, безопасности, удобства использования) и применять инструменты и технологии обеспечения качества	ПК-5.1. Анализирует требования на реализуемость и пригодность к тестированию, формируя отчёт о корректности документации	***Знать:*** методы анализа и тестирования ПО, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). ***Уметь:*** анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования ПО, определять конечные данные для эксплуатации на основе разрабатываемых требований. ***Владеть:*** навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации.
		ПК-5.2. Разрабатывает требования к тестированию на основе требований к программно-информационной системе	***Знать:*** методы анализа и тестирования, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. ***Уметь:*** определять цели тестирования, разрабатывать требования к тестированию, оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки). ***Владеть:*** навыками разработки требований к тестированию ПО на основе требований к информационной системе.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-8	Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта	ПК-8.3. Контролирует выполнение заданий программистами	***Знать:*** методы и приемы формализации задач, виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий, осуществлять обучение и наставничество, проводить оценку и обоснование рекомендуемых решений. ***Владеть:*** навыками руководства программным проектом, распределения заданий между программистами в соответствии с техническими спецификациями, контроля выполнения заданий, обучения программистов.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Методы и средства защиты компьютерной информации» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули»)) основной профессиональной образовательной программы – программы бакалавриата 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем». Дисциплина изучается на 3 курсе в 6 семестре.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	28,1
в том числе:	
лекции	14
лабораторные занятия	14
практические занятия	не предусмотрены
Самостоятельная работа обучающихся (всего)	79,9
Контроль (подготовка к экзамену)	не предусмотрен
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Основные понятия и анализ угроз информационной безопасности	Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности. Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы.
2	Проблемы информационной безопасности сетей	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.
3	Политика безопасности	Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети: физическая безопасность, логическая безопасность, защита ресурсов, определение административных полномочий, аудит и оповещение.
4	Криптографическая защита информации	Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные крипто-системы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП). Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты.
5	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации.

6	Технологии межсетевых экранов	Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
7	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод «белого списка», обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.
8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.
9	Основы правового обеспечения защиты информации	Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и анализ угроз информационной безопасности	1	–	–	У-1-3,6,7 МУ-5	Т-4	ПК-5
2	Проблемы информационной безопасности сетей	2	–	–	У-2,3,6,7 МУ-5	Т-4	ПК-5
3	Политика безопасности	2	–	–	У-1,3,5,7 МУ-5	Т-8	ПК-5
4	Криптографическая защита информации	2	1,2	–	У-1,4,7 МУ-1,2,5	ЛР-4,8, Т-8	ПК-5 ПК-8
5	Технологии аутентификации	1	–	–	У-3,4,6,7 МУ-5	Т-8	ПК-5 ПК-8
6	Технологии межсетевых экранов	1	3	–	У-1,2,4,5 МУ-3,5	ЛР-10, Т-12	ПК-5 ПК-8
7	Технологии защиты от вирусов	2	–	–	У-1,2,4 МУ-5	Т-12	ПК-5 ПК-8
8	Требования к системам защиты информации	2	4	–	У-1-6 МУ-4,5	ЛР-14	ПК-5 ПК-8
9	Основы правового обеспечения защиты информации	1	–	–	У-1,3,4 МУ-5	Т-14	ПК-5 ПК-8

Т – тест, ЛР – защита отчета по лабораторной работе.

4.2 Лабораторные работы и практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	2	3
1	Разработка криптографической программы «Алгоритм RSA»	4
2	Разработка криптографической программы «Шифр Виженера»	4
3	Настройка межсетевого экрана в ОС Windows	2
4	Шифрование с помощью программы TrueCrypt	4
Итого		16

4.2.2 Практические занятия

Не предусмотрены учебным планом

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	2	3	4
1	Основные понятия и анализ угроз информационной безопасности	2 неделя	7,9
2	Проблемы информационной безопасности сетей	4 неделя	9
3	Политика безопасности	6 неделя	9
4	Криптографическая защита информации	8 неделя	9
5	Технологии аутентификации	9 неделя	9
6	Технологии межсетевых экранов	10 неделя	9
7	Технологии защиты от вирусов	11 неделя	9
8	Требования к системам защиты информации	13 неделя	9
9	Основы правового обеспечения защиты информации	14 неделя	9
Итого			79,9

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;
– заданий для самостоятельной работы;
– тем рефератов;
– вопросов к зачету;
– методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся.

Содержание дисциплины обладает воспитательным потенциалом, поскольку в нем аккумулирован исторический и современный научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование профессиональной культуры обучающихся. Содержание дисциплины способствует гражданскому, правовому, экономическому, профессионально-трудовому воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей отрасли защиты информации, высокого профессионализма ученых, их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки, экономики и производства*;*

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися (командная работа, разбор конкретных ситуаций, решение кейсов и др.)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Лекция №1. Основные понятия и анализ угроз информационной безопасности	Анализ конкретных ситуаций	1
2	Лекция №3. Политика безопасности	Анализ конкретных ситуаций	1
3	Лабораторная работа №1. Разработка криптографической программы «Алгоритм RSA»	Анализ конкретных ситуаций	1
4	Лабораторная работа №2. Разработка криптографической программы «Шифр Виженера»	Анализ конкретных ситуаций	1
5	Лабораторная работа №3. Настройка межсетевого экрана в ОС Windows	Анализ конкретных ситуаций	1
6	Лабораторная работа № 4. Шифрование с помощью программы TrueCrypt	Анализ конкретных ситуаций	1
Итого			6

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-5. Способен осуществлять контроль качества программного обеспечения (надежности, безопасности, удобства использования) и применять инструменты и технологии обеспечения качества	Методы и средства защиты компьютерной информации Производственная практика (научно-исследовательская работа)		Тестирование программного обеспечения Разработка и анализ требований Проектирование человеко-машинного интерфейса
ПК-8. Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта	Конструирование программного обеспечения	Методы и средства защиты компьютерной информации Цифровая обработка сигналов / Обработка экспериментальных данных на ЭВМ	Разработка и анализ требований Управление программными проектами Тестирование программного обеспечения Сети ЭВМ и телекоммуникации / Администрирование информационно-вычислительных систем Производственная преддипломная практика

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-5/ начальный, основной	ПК-5.1. Анализирует требования на реализуемость и пригодность к тестированию, формируя отчёт о корректности документации	***Знать:*** общие принципы методов анализа и тестирования ПО, базовые положения теории тестирования (основные модели и этапы планирования), типовые подходы к тест-дизайну и проектированию тестов. ***Уметь:*** прослеживать основные взаимосвязи в требованиях, обнаруживать явно пропущенную или противоречивую информацию при проверке, определять стандартные затратные области в процессе тестирования ПО, перечислять конечные данные для эксплуатации на основе предоставленных требований. ***Владеть:*** базовыми навыками анализа требований на предмет их принципиальной реализуемости и пригодности к тестированию по за-	***Знать:*** современные методы анализа и тестирования ПО, теорию тестирования (модели тестирования, планирование, вариативные техники тест-дизайна и проектирования тестов). ***Уметь:*** системно анализировать сложные взаимосвязи между разделами требований, выявлять скрытую пропущенную или неоднозначную информацию, обоснованно определять и классифицировать наиболее затратные места в процессе тестирования ПО, формулировать конечные данные для эксплуатации на основе анализа разрабатываемых требований с учетом специфики системы. ***Владеть:*** навыками анализа требований на реализуемость и пригодность к тестированию, основными навыками составления структурированных и доказательных отчетов о	***Знать:*** методы анализа и тестирования ПО, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). ***Уметь:*** анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования ПО, определять конечные данные для эксплуатации на основе разрабатываемых требований. ***Владеть:*** навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации.

		данному алгоритму, формирования отчетов о корректности документации по установленному шаблону.	корректности документации с указанием зон риска.	
	ПК-5.2. Разрабатывает требования к тестированию на основе требований к программно-информационной системе	***Знать:*** основные методы анализа и тестирования ПО, базовые положения теории тестирования (типовые модели, этапы планирования, стандартные подходы к тест-дизайну и проектированию тестов), базовые техники тестирования. ***Уметь:*** формулировать цели тестирования в общем виде, разрабатывать требования к тестированию по заданному шаблону, оценивать важность тестов на основе явно указанных критериев (например, заданных приоритетов пользователя или проектных задач) без углублённого анализа рисков. ***Владеть:*** базовыми навыками разработки требований к тестированию ПО на основе требований к информационной системе по установленной методике (инструкции).	***Знать:*** методы анализа и тестирования ПО, теорию тестирования (различные модели тестирования, гибкое планирование, вариативные техники тест-дизайна и проектирования тестов), основные техники тестирования. ***Уметь:*** чётко и обоснованно определять цели тестирования, разрабатывать требования к тестированию с учётом специфики системы и контекста, комплексно оценивать важность различных тестов на основе анализа приоритетов пользователя, проектных задач и вероятных рисков возникновения ошибок. ***Владеть:*** устойчивыми навыками самостоятельной разработки требований к тестированию ПО на основе требований к информационной системе.	***Знать:*** методы анализа и тестирования, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. ***Уметь:*** определять цели тестирования, разрабатывать требования к тестированию, оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки). ***Владеть:*** навыками разработки требований к тестированию ПО на основе требований к информационной системе.
ПК-8/ основной	ПК-8.3. Контролирует выполнение заданий программистами	***Знать:*** базовые методы и приёмы формализации задач, типовые виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий по утверждённому плану (графику) с использованием стандартных средств отслеживания, проводить базовое инструктирование (ознакомление) програм-	***Знать:*** основные методы и приемы формализации задач для различных типов проектов, виды технических спецификаций на программные компоненты с учётом их назначения и уровня детализации. ***Уметь:*** осуществлять контроль выполнения заданий, своевременно выявляя отклонения и корректируя ход работ; осуществлять обучение и	***Знать:*** методы и приемы формализации задач, виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий, осуществлять обучение и наставничество, проводить оценку и обоснование реко-

		мистов с задачами. ***Владеть:*** базовыми навыками руководства небольшим программным проектом, распределения заданий между программистами в соответствии с готовыми техническими спецификациями по шаблону, навыками проведения первичного инструктажа для новых сотрудников.	наставничество программистов; проводить оценку и обоснование рекомендуемых решений. ***Владеть:*** устойчивыми навыками руководства распределённой командой, навыками гибкого распределения заданий между программистами на основе технических спецификаций, организации обучения и наставничества с оценкой эффективности.	мендуемых решений. ***Владеть:*** навыками руководства программным проектом, распределения заданий между программистами в соответствии с техническими спецификациями, контроля выполнения заданий, обучения программистов.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и анализ угроз информационной безопасности	ПК-5	Лекции, СРС	БТЗ	1.1-1.10	Согласно табл.7.2
2	Проблемы информационной безопасности сетей	ПК-5	Лекции, СРС	БТЗ	2.1-2.10	Согласно табл.7.2
3	Политика безопасности	ПК-5	Лекции, СРС	БТЗ	3.1-3.10	Согласно табл.7.2
4	Криптографическая защита информации	ПК-5 ПК-8	Лекции, лабораторные работы, СРС	ЛР№1	1.1-1.10	Согласно табл.7.2
				ЛР№2	2.1-2.10	
				БТЗ	4.1-4.10	
5	Технологии аутентификации	ПК-5 ПК-8	Лекции, СРС	БТЗ	5.1-5.10	Согласно табл.7.2
6	Технологии межсетевых экранов	ПК-5 ПК-8	Лекции, лабораторные работы, СРС	БТЗ	6.1-6.10	Согласно табл.7.2
				ЛР№3	3.1-3.10	
7	Технологии защиты от вирусов	ПК-5 ПК-8	Лекции, СРС	БТЗ	7.1-7.10	Согласно табл.7.2
8	Требования к системам защиты информации	ПК-5 ПК-8	Лекции, лабораторные работы, СРС	ЛР№4	4.1-4.10	Согласно табл.7.2
				БТЗ	8.1-8.10	
9	Основы правового обеспечения защиты информации	ПК-5 ПК-8	Лекции, СРС	БТЗ	9.1-9.10	Согласно табл.7.2

БТЗ – банк тестовых заданий, ЛР – вопросы и задания для защиты лабораторной работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Примерные вопросы тестирования по разделу 1 «Основные понятия и анализ угроз информационной безопасности» в закрытой форме:

Какое свойство информации нарушается при несанкционированном изменении, искажении или уничтожении данных? Выберите один ответ:

а) Конфиденциальность

б) Доступность
в) Целостность
г) Достоверность

Какое из перечисленных воздействий на вычислительную сеть является примером пассивной угрозы? Выберите один ответ:
а) Изменение конфигурации сети
б) Нарушение работоспособности узла сети
в) Прослушивание канала связи в сети
г) Передача сообщений от имени другого объекта

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:
- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Какая угроза информационной безопасности является пассивной:

А) Копирование секретных данных.
Б) Внедрение вредоносного программного обеспечения.
В) Кража носителей информации.
Г) Удаление файла.

Задание в открытой форме:
Заполните пропуск:
В компьютерной сети перехват данных, передаваемых по каналам связи относится к уровню _____.

Задание на установление последовательности:
Установите в порядке увеличения единицы измерения количества информации:
1. 1 ТБ
2. 30 Гбайт
3. 50 Килобайт
4. 100 Мегабайт

Задание на установление соответствия:
Установите соответствие между способов и видов информации.

1. По способу кодирования	а) Цифровая, аналоговая
2. По способу представления	б) Визуальная, звуковая, документ
3. По способу обработки	в) Текстовая, графическая, числовая
4. По способу восприятия	г) Непрерывная, дискретная

Компетентностно-ориентированная задача:
Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей

в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Лабораторная работа №1	3	Выполнил и «защитил». Доля правильных ответов на «защите» составила 50%	8	Выполнил и «защитил». Доля правильных ответов на «защите» составила более 85%
Лабораторная работа №2	2	Выполнил и «защитил». Доля правильных ответов на «защите» составила 50%	8	Выполнил и «защитил». Доля правильных ответов на «защите» составила более 85%
Лабораторная работа №3	3	Выполнил и «защитил». Доля правильных ответов на «защите» составила 50%	8	Выполнил и «защитил». Доля правильных ответов на «защите» составила более 85%
Лабораторная работа №4	1	Выполнил и «защитил». Доля правильных ответов на «защите» составила 50%	8	Выполнил и «защитил». Доля правильных ответов на «защите» составила более 75%
Тестирование в контрольной точке №1	2	Доля правильных ответов составила 50%	4	Доля правильных ответов составила более 85%
Тестирование в контрольной точке №2	2	Доля правильных ответов составила 50%	4	Доля правильных ответов составила более 85%
Тестирование в контрольной точке №3	2	Доля правильных ответов составила 50%	4	Доля правильных ответов составила более 85%
Тестирование в контрольной точке №4	2	Доля правильных ответов составила 50%	4	Доля правильных ответов составила более 85%
Итого	24		48	
Посещаемость	0		16	
Зачет	0		36	
Итого	24		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме – 1 балл,

– задание в открытой форме – 2 балла,

– задание на установление правильной последовательности – 2 балла,

– задание на установление соответствия – 2 балла,

– решение компетентностно-ориентированной задачи – 10 баллов.

Максимальное количество баллов за тестирование – 36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2017. – 196 с. – Текст : электронный.

2. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – 202 с. – URL: http://biblioclub.ru/index.php?page=book&id=561238 (дата обращения 09.09.2022). – Режим доступа : по подписке. – Текст : электронный.

3. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва, Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения 12.09.2022). – Режим доступа : по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

4. Грибунин, Вадим Геннадьевич. Комплексная система защиты информации на предприятии : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М. : Академия, 2009. – 416 с. – (Высшее профессиональное образование). – Текст : непосредственный.

5. Лопин, В. Н. Защита информации в компьютерных системах : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. – Курск : КГТУ, 2006. – 159 с. – Текст : непосредственный.

6. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун. – Курск : ЮЗГУ, 2013. – Ч. 1. – 150 с. – Текст : электронный.

7. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун . – Курск : ЮЗГУ, 2013. – Ч. 2. – 303 с. – Текст : электронный.

8.3 Перечень методических указаний

1. Алгоритм шифрования RSA : методические указания к выполнению практических и лабораторных работ / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. – Курск : ЮЗГУ, 2022. – 11 с. – Текст : электронный.

2. Шифрование с помощью таблицы Виженера : методические указания к выполнению лабораторных работ / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. – Курск : ЮЗГУ, 2022. – 9 с. – Текст : электронный.

3. Настройка межсетевого экрана в операционной системе Windows : методи-

ческие указания по выполнению лабораторных и практических работ / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. – Курск : ЮЗГУ, 2022. – Текст : электронный.

4. Шифрование с помощью программы TrueCrypt : методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. – Курск : ЮЗГУ, 2022. – 20 с. – Текст : электронный.

5. Методы и средства защиты компьютерной информации : методические указания для самостоятельной работы по изучению дисциплины для студентов направления подготовки (специальности) 09.03.04 «Программная инженерия» / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. – Электрон. текстовые дан. (271 КБ). – Курск : ЮЗГУ, 2021. – 14 с. – Загл. с титул. экрана. – Б. ц. – Текст : электронный.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
2. http://school-collection.edu.ru/ - федеральное хранилище Единая коллекция цифровых образовательных ресурсов.
3. http://www.edu.ru/ - федеральный портал Российское образование.
4. http://www.igumo.ru/ - интернет-портал Института гуманитарного образования и информационных технологий.
5. http://elibrary.ru/defaultx.asp - научная электронная библиотека «Elibrary».
6. http://www.eduhmao.ru/info/1/4382/ - информационно-просветительский портал «Электронные журналы».
7. www.diss.rsl.ru – электронная библиотека диссертаций.
8. http://fictionbook.ru – электронная библиотека.
9. http://svitk.ru – электронная библиотека.
10. http://www.iqlib.ru – электронная библиотека образовательных и просветительных изданий.
11. http://www.lib.msu.su/index.html - Научная библиотека Московского государственного университета им. М.В.Ломоносова.
12. http://www.rsl.ru/ - Российская Государственная Библиотека.
13. http://e.lanbook.com/ - Электронно-библиотечная система «Лань».
14. http://window.edu.ru/ - Электронная библиотека «Единое окно доступа к образовательным ресурсам».

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Методы и средства защиты компьютерной информации» являются лекции и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспекти-

ровать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Методы и средства защиты компьютерной информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, отработку студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Методы и средства защиты компьютерной информации» с целью освоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Методы и средства защиты компьютерной информации» – закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программный продукт LibreOffice (свободно распространяемое ПО для некоммерческих целей) (ссылка на скачивание: ru.libreoffice.org/download/).

Программа анализа и управления информационными рисками «Гриф» (свободно распространяемое ПО для некоммерческих целей).

Программа хранения паролей PasswordCommander (свободно распространяемое ПО для некоммерческих целей).

Фаервол ComodoFirewall (свободно распространяемое ПО для некоммерческих целей).

Программа анализа защищенности операционной системы GFILANguardNetworkSecurityScanner.

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Криптографическая программа TrueCrypt.

Операционная система Windows.

Антивирус Касперского *(или ESETNOD)*.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения лекционных занятий требуется учебная аудитория для проведения занятий лекционного типа оснащенная:

– учебной мебелью: столы (в количестве не менее 1 на 2 обучающихся) и стулья для обучающихся (в количестве не менее списочного состава группы);

– столом и стулом для преподавателя;

– доской;

– видеопроектором и ноутбуком (для показа презентаций и учебных фильмов).

Проведение лабораторных занятий предполагается в учебной лаборатории кафедры информационной безопасности, оснащенной:

– учебной мебелью: столы (в количестве не менее 1 на 2 обучающихся) и стулья для обучающихся (в количестве не менее списочного состава группы);

– доской;

– столом и стулом для преподавателя;

– учебными компьютерами (в количестве не менее 1 устройство на 2 студентов), с предустановленными программными продуктами, перечисленными в п.11 настоящей программы.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
И.о. декана факультета
фундаментальной и прикладной информатики
(наименование ф-та полностью)

_____ М.О. Таныгин
(подпись, инициалы, фамилия)

«30» ____08____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты компьютерной информации
(наименование дисциплины)

ОПОП ВО 09.03.04 Программная инженерия,
шифр и наименование направления подготовки

направленность (профиль) «Разработка программно-информационных систем»
наименование направленности (профиля)

форма обучения заочная
(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины Методы и средства защиты компьютерной информации составлена в соответствии с ФГОС ВО – бакалавриат по направлению подготовки (специальности) 09.03.04Программная инженерия на основании учебного плана ОПОП ВО 09.03.04Программная инженерия, направленность Разработка программно-информационных систем, одобренного Ученым советом университета (протокол №9 «25» 06 2021 г.).

Рабочая программа дисциплины Методы и средства защиты компьютерной информации обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 09.03.04 Программная инженерия, направленность Разработка программно-информационных системна заседании кафедры информационной безопасности Протокол №11 28« 06 »2021 г.

Зав. кафедрой Таныгин М.О.

Разработчик программы

к.воен.н., доцент ХанисА.Л.

Согласовано: на заседании кафедры программной инженерии № 12 «01» 07 2021 г.

Зав. кафедрой Малышев А.В.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа дисциплины Методы и средства защиты компьютерной информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность Разработка программно-информационных систем, одобренного Ученым советом университета протокол №2 «18» 06 2022 г., на заседании кафедры ИБ, протокол №11 от 30.06.2022 .

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины Методы и средства защиты компьютерной информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность Разработка программно-информационных систем, одобренного Ученым советом университета протокол №_ «__»2021 г., на заседании кафедры _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № 1 от 29.08.2024.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Медуненко А.Л.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № 11 от 24.06.25г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Тюлькин М.О.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол № 9 «27» 03 2024 г.), на заседании кафедры информационной безопасности, протокол № 11 от 30.06.2026 г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ М.О. Тюлькин

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № от _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем», одобренного Ученым советом университета (протокол №__ «___» _____ 202__ г.), на заседании кафедры информационной безопасности, протокол № от _____.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Целью преподавания дисциплины является изложение основ методики комплексной защиты информационных систем на основе программных и программно-аппаратных средств, а также требований к системам защиты информации.

1.2 Задачи дисциплины

– изучение классификации угроз информационной безопасности;

– изучение принципов действия основных видов сетевых атак и методов борьбы с ними;

– изучение структуры политики безопасности организации и основных этапов ее разработки;

– ознакомление с симметричными и ассиметричными криптосистемами, изучение алгоритмов RSA, Виженера, AES, электронно-цифровой подписи;

– изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем идентификации и аутентификации;

– изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;

– изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;

– изучение основных требований и рекомендаций по защите информации в компьютерных системах;

– изучение средств анализа защищенности и обнаружения сетевых атак;

– изучение основных юридических законов в области защиты информации.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-5	Способен осуществлять контроль качества программного обеспечения (надежности, безопасности, удобства использования) и применять инструменты и технологии обеспечения качества	ПК-5.1. Анализирует требования на реализуемость и пригодность к тестированию, формируя отчёт о корректности документации	***Знать:*** методы анализа и тестирования ПО, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). ***Уметь:*** анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования ПО, определять конечные данные для эксплуатации на основе разрабатываемых требований. ***Владеть:*** навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации.
		ПК-5.2. Разрабатывает требования к тестированию на основе требований к программно-информационной системе	***Знать:*** методы анализа и тестирования, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. ***Уметь:*** определять цели тестирования, разрабатывать требования к тестированию, оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки). ***Владеть:*** навыками разработки требований к тестированию ПО на основе требований к информационной системе.

Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)		*Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной*	*Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций*
код компетенции	*наименование компетенции*		
ПК-8	Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта	ПК-8.3. Контролирует выполнение заданий программистами	***Знать:*** методы и приемы формализации задач, виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий, осуществлять обучение и наставничество, проводить оценку и обоснование рекомендуемых решений. ***Владеть:*** навыками руководства программным проектом, распределения заданий между программистами в соответствии с техническими спецификациями, контроля выполнения заданий, обучения программистов.

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Методы и средства защиты компьютерной информации» входит в часть, формируемую участниками образовательных отношений блока 1 «Дисциплины (модули»)) основной профессиональной образовательной программы – программы бакалавриата 09.03.04 Программная инженерия, направленность (профиль) «Разработка программно-информационных систем». Дисциплина изучается на 3 курсе.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 академических часов.

Таблица 3 – Объем дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	8,1
в том числе:	
лекции	4
лабораторные занятия	4
практические занятия	не предусмотрены
Самостоятельная работа обучающихся (всего)	95,9
Контроль (подготовка к зачету)	4
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрен
экзамен (включая консультацию перед экзаменом)	не предусмотрен

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Основные понятия и анализ угроз информационной безопасности	Основные понятия защиты информации и информационной безопасности. Понятие угрозы информационной безопасности. Анализ и классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности информации, целостности информации, доступности информации. Угроза раскрытия параметров автоматизированной системы.
2	Проблемы информационной безопасности сетей	Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP- сетей. Основные виды сетевых атак. Спам. Фишинг и фарминг. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Фрагментарный и комплексный подходы к проблеме обеспечения безопасности компьютерных сетей. Пути решения проблем защиты информации в сетях.
3	Политика безопасности	Основные понятия политики безопасности. Верхний, средний и нижний уровни политики безопасности. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Основные этапы разработки политики безопасности организации. Компоненты архитектуры безопасности сети: физическая безопасность, логическая безопасность, защита ресурсов, определение административных полномочий, аудит и оповещение.
4	Криптографическая защита информации	Основные понятия криптографической защиты информации. Требования к криптографическим системам. Симметричные и ассиметричные крипто-системы шифрования. Блочные и потоковые шифры. Шифры простой замены. Шифры Виженера. Стандарт шифрования AES. Алгоритм шифрования RSA. Функция хэширования. Электронная цифровая подпись (ЭЦП). Защита электронного документооборота с использованием ЭЦП. Обзор программных и программно-аппаратных средств криптографической защиты.
5	Технологии аутентификации	Аутентификация, авторизация и администрирование действий пользователей. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация, основанная на симметричных алгоритмах. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации.

6	Технологии межсетевых экранов	Классификация межсетевых экранов. Функции межсетевых экранов: фильтрация трафика, выполнение функций посредничества. Дополнительные возможности межсетевых экранов: идентификация и аутентификация пользователей, трансляция сетевых адресов, регистрация и анализ событий. Варианты исполнения межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.
7	Технологии защиты от вирусов	Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Вирусы-сценарии. Макровирусы. Троянские программы. Черви. Жизненный цикл вирусов. Основные каналы распространения вредоносных программ. Методы обнаружения компьютерных вирусов: обнаружение, основанное на сигнатурах, обнаружение программ подозрительного поведения, метод «белого списка», обнаружение вирусов при помощи эмуляции работы программы, эвристический анализ. Обзор современных антивирусных программ. Построение системы антивирусной защиты корпоративной сети.
8	Требования к системам защиты информации	Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Основные требования и рекомендации по защите информации, составляющей служебную или коммерческую тайну, а также персональных данных. Требования к защите информации в автоматизированных системах, локальных вычислительных сетях, на рабочих местах пользователей ПК. Требования к защите информации при работе с системами управления базами данных. Требования к защите информации при взаимодействии абонентов с сетями общего пользования.
9	Основы правового обеспечения защиты информации	Правовое обеспечение информационной собственности и его место в системе информационного права. Информация как объект юридической защиты. Формирование государственной системы правового обеспечения информационной безопасности. Правовое обеспечение защиты государственной тайны. Законодательство Российской Федерации в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Правовая защита интеллектуальной собственности. Правовое регулирование деятельности организаций в области информационной безопасности.

Таблица 4.1.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Основные понятия и анализ угроз информационной безопасности	1	–	–	У-1-3,6,7 МУ-3	Т	ПК-5
2	Проблемы информационной безопасности сетей	1	–	–	У-2,3,6,7 МУ-3	Т	ПК-5
3	Политика безопасности	–	–	–	У-1,3,5,7 МУ-3	Т	ПК-5
4	Криптографическая защита информации	1	1	–	У-1,4,7 МУ-1,3	ЛР, Т	ПК-5 ПК-8
5	Технологии аутентификации	–	–	–	У-3,4,6,7 МУ-3	Т	ПК-5 ПК-8
6	Технологии межсетевых экранов	–	–	–	У-1,2,4,5 МУ-3	Т	ПК-5 ПК-8
7	Технологии защиты от вирусов	–	–	–	У-1,2,4 МУ-	Т	ПК-5 ПК-8
8	Требования к системам защиты информации	1	2	–	У-1-6 МУ-2,3	ЛР	ПК-5 ПК-8
9	Основы правового обеспечения защиты информации	–	–	–	У-1,3,4 МУ-3	Т	ПК-5 ПК-8

Т – тест, ЛР – защита отчета по лабораторной работе.

4.2 Лабораторные работы и практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1	2	3
1	Разработка криптографической программы «Алгоритм RSA»	2
2	Шифрование с помощью программы TrueCrypt	2
Итого		4

4.2.2 Практические занятия

Не предусмотрены учебным планом

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час
1	2	3	4
1	Основные понятия и анализ угроз информационной безопасности	В течении семестра	8,9
2	Проблемы информационной безопасности сетей		9
3	Политика безопасности		10
4	Криптографическая защита информации		14
5	Технологии аутентификации		10
6	Технологии межсетевых экранов		10
7	Технологии защиты от вирусов		10
8	Требования к системам защиты информации		14
9	Основы правового обеспечения защиты информации		10
Итого			95,9

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;
– заданий для самостоятельной работы;
– тем рефератов;
– вопросов к зачету;
– методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся.

Содержание дисциплины обладает воспитательным потенциалом, поскольку в нем аккумулирован исторический и современный научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование профессиональной культуры обучающихся. Содержание дисциплины способствует гражданскому, правовому, экономическому, профессионально-трудовому воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей отрасли защиты информации, высокого профессионализма ученых, их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки, экономики и производства*;*

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися (командная работа, разбор конкретных ситуаций, решение кейсов и др.)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем в часах
1	2	3	4
1	Лабораторная работа №1. Разработка криптографической программы «Алгоритм RSA»	Анализ конкретных ситуаций	1
2	Лабораторная работа № 2. Шифрование с помощью программы TrueCrypt	Анализ конкретных ситуаций	1
Итого			2

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

Таблица 7.1 – Этапы формирования компетенций

Код и наименование компетенции	Этапы формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-5. Способен осуществлять контроль качества программного обеспечения (надежности, безопасности, удобства использования) и применять инструменты и технологии обеспечения качества	Методы и средства защиты компьютерной информации Производственная практика (научно-исследовательская работа)		Тестирование программного обеспечения Разработка и анализ требований Проектирование человеко-машинного интерфейса
ПК-8. Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта	Конструирование программного обеспечения	Методы и средства защиты компьютерной информации Цифровая обработка сигналов / Обработка экспериментальных данных на ЭВМ	Разработка и анализ требований Управление программными проектами Тестирование программного обеспечения Сети ЭВМ и телекоммуникации / Администрирование информационно-вычислительных систем Производственная преддипломная практика

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-5/ начальный, основной	ПК-5.1. Анализирует требования на реализуемость и пригодность к тестированию, формируя отчёт о корректности документации	***Знать:*** общие принципы методов анализа и тестирования ПО, базовые положения теории тестирования (основные модели и этапы планирования), типовые подходы к тест-дизайну и проектированию тестов. ***Уметь:*** прослеживать основные взаимосвязи в требованиях, обнаруживать явно пропущенную или противоречивую информацию при проверке, определять стандартные затратные области в процессе тестирования ПО, перечислять конечные данные для эксплуатации на основе предоставленных требований. ***Владеть:*** базовыми навыками анализа требований на предмет их принципиальной реализуемости и пригодности к тестированию по за-	***Знать:*** современные методы анализа и тестирования ПО, теорию тестирования (модели тестирования, планирование, вариативные техники тест-дизайна и проектирования тестов). ***Уметь:*** системно анализировать сложные взаимосвязи между разделами требований, выявлять скрытую пропущенную или неоднозначную информацию, обоснованно определять и классифицировать наиболее затратные места в процессе тестирования ПО, формулировать конечные данные для эксплуатации на основе анализа разрабатываемых требований с учетом специфики системы. ***Владеть:*** навыками анализа требований на реализуемость и пригодность к тестированию, основными навыками составления структурированных и доказательных отчетов о	***Знать:*** методы анализа и тестирования ПО, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). ***Уметь:*** анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования ПО, определять конечные данные для эксплуатации на основе разрабатываемых требований. ***Владеть:*** навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации.

		данному алгоритму, формирования отчетов о корректности документации по установленному шаблону.	корректности документации с указанием зон риска.	
	ПК-5.2. Разрабатывает требования к тестированию на основе требований к программно-информационной системе	***Знать:*** основные методы анализа и тестирования ПО, базовые положения теории тестирования (типовые модели, этапы планирования, стандартные подходы к тест-дизайну и проектированию тестов), базовые техники тестирования. ***Уметь:*** формулировать цели тестирования в общем виде, разрабатывать требования к тестированию по заданному шаблону, оценивать важность тестов на основе явно указанных критериев (например, заданных приоритетов пользователя или проектных задач) без углублённого анализа рисков. ***Владеть:*** базовыми навыками разработки требований к тестированию ПО на основе требований к информационной системе по установленной методике (инструкции).	***Знать:*** методы анализа и тестирования ПО, теорию тестирования (различные модели тестирования, гибкое планирование, вариативные техники тест-дизайна и проектирования тестов), основные техники тестирования. ***Уметь:*** чётко и обоснованно определять цели тестирования, разрабатывать требования к тестированию с учётом специфики системы и контекста, комплексно оценивать важность различных тестов на основе анализа приоритетов пользователя, проектных задач и вероятных рисков возникновения ошибок. ***Владеть:*** устойчивыми навыками самостоятельной разработки требований к тестированию ПО на основе требований к информационной системе.	***Знать:*** методы анализа и тестирования, теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. ***Уметь:*** определять цели тестирования, разрабатывать требования к тестированию, оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки). ***Владеть:*** навыками разработки требований к тестированию ПО на основе требований к информационной системе.
ПК-8/ основной	ПК-8.3. Контролирует выполнение заданий программистами	***Знать:*** базовые методы и приёмы формализации задач, типовые виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий по утверждённому плану (графику) с использованием стандартных средств отслеживания, проводить базовое инструктирование (ознакомление) програм-	***Знать:*** основные методы и приемы формализации задач для различных типов проектов, виды технических спецификаций на программные компоненты с учётом их назначения и уровня детализации. ***Уметь:*** осуществлять контроль выполнения заданий, своевременно выявляя отклонения и корректируя ход работ; осуществлять обучение и	***Знать:*** методы и приемы формализации задач, виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий, осуществлять обучение и наставничество, проводить оценку и обоснование реко-

		мистов с задачами. ***Владеть:*** базовыми навыками руководства небольшим программным проектом, распределения заданий между программистами в соответствии с готовыми техническими спецификациями по шаблону, навыками проведения первичного инструктажа для новых сотрудников.	наставничество программистов; проводить оценку и обоснование рекомендуемых решений. ***Владеть:*** устойчивыми навыками руководства распределённой командой, навыками гибкого распределения заданий между программистами на основе технических спецификаций, организации обучения и наставничества с оценкой эффективности.	мендуемых решений. ***Владеть:*** навыками руководства программным проектом, распределения заданий между программистами в соответствии с техническими спецификациями, контроля выполнения заданий, обучения программистов.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или ее части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Основные понятия и анализ угроз информационной безопасности	ПК-5	Лекции, СРС	БТЗ	1.1-1.10	Согласно табл.7.2
2	Проблемы информационной безопасности сетей	ПК-5	Лекции, СРС	БТЗ	2.1-2.10	Согласно табл.7.2
3	Политика безопасности	ПК-5	Лекции, СРС	БТЗ	3.1-3.10	Согласно табл.7.2
4	Криптографическая защита информации	ПК-5 ПК-8	Лекции, лабораторные работы, СРС	ЛР№1	1.1-1.10	Согласно табл.7.2
				БТЗ	4.1-4.10	
5	Технологии аутентификации	ПК-5 ПК-8	Лекции, СРС	БТЗ	5.1-5.10	Согласно табл.7.2
6	Технологии межсетевых экранов	ПК-5 ПК-8	Лекции, СРС	БТЗ	6.1-6.10	Согласно табл.7.2
7	Технологии защиты от вирусов	ПК-5 ПК-8	Лекции, СРС	БТЗ	7.1-7.10	Согласно табл.7.2
8	Требования к системам защиты информации	ПК-5 ПК-8	Лекции, лабораторные работы, СРС	ЛР№2	4.1-4.10	Согласно табл.7.2
				БТЗ	8.1-8.10	
9	Основы правового обеспечения защиты информации	ПК-5 ПК-8	Лекции, СРС	БТЗ	9.1-9.10	Согласно табл.7.2

БТЗ – банк тестовых заданий, ЛР – вопросы и задания для защиты лабораторной работы

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Примерные вопросы тестирования по разделу 1 «Основные понятия и анализ угроз информационной безопасности» в закрытой форме:

Какое свойство информации нарушается при несанкционированном изменении, искажении или уничтожении данных? Выберите один ответ:

а) Конфиденциальность

б) Доступность

в) Целостность
г) Достоверность

Какое из перечисленных воздействий на вычислительную сеть является примером пассивной угрозы? Выберите один ответ:
а) Изменение конфигурации сети
б) Нарушение работоспособности узла сети
в) Прослушивание канала связи в сети
г) Передача сообщений от имени другого объекта

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:
- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:
Какая угроза информационной безопасности является пассивной:
А) Копирование секретных данных.

Б) Внедрение вредоносного программного обеспечения.
В) Кража носителей информации.
Г) Удаление файла.

Задание в открытой форме:
Заполните пропуск:
В компьютерной сети перехват данных, передаваемых по каналам связи относится к уровню _____.

Задание на установление последовательности:
Установите в порядке увеличения единицы измерения количества информации:
1. 1 ТБ
2. 30 Гбайт
3. 50 Килобайт
4. 100 Мегабайт

Задание на установление соответствия:
Установите соответствие между способов и видов информации.

1. По способу кодирования	а) Цифровая, аналоговая
2. По способу представления	б) Визуальная, звуковая, документ
3. По способу обработки	в) Текстовая, графическая, числовая
4. По способу восприятия	г) Непрерывная, дискретная

Компетентностно-ориентированная задача:
Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8 бит.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок

начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Лабораторная работа №1	0	Работа не выполнена	10	Выполнил и «защитил». Доля правильных ответов на «защите» составила более 85%
Лабораторная работа №2	0	Работа не выполнена	10	Выполнил и «защитил». Доля правильных ответов на «защите» составила более 85%
Тестирование №1	0	Тест не пройден	8	Доля правильных ответов составила более 85%
Тестирование №2	0	Тест не пройден	8	Доля правильных ответов составила более 85%
Итого	0		36	
Посещаемость	0		14	
Зачет	0		60	
Итого	0		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

– задание в закрытой форме – 3 балл,
– задание в открытой форме – 3 балла,
– задание на установление правильной последовательности – 3 балла,
– задание на установление соответствия – 3 балла,
– решение компетентностно-ориентированной задачи – 15 баллов.

Максимальное количество баллов за тестирование – 60 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 «Информационная безопасность», 400301 «Юриспруденция», 380301 «Экономика»] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2017. – 196 с. – Текст : электронный.

2. Проскуряков, А. В. Компьютерные сети: основы построения компьютерных сетей и телекоммуникаций : учебное пособие / А. В. Проскуряков. – Ростов-на-Дону

; Таганрог : Издательство Южного федерального университета, 2018. – 202 с. – URL: http://biblioclub.ru/index.php?page=book&id=561238 (дата обращения 09.09.2022). – Режим доступа : по подписке. – Текст : электронный.

3. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва, Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения 12.09.2022). – Режим доступа : по подписке. – Текст : электронный.

8.2 Дополнительная учебная литература

4. Грибунин, Вадим Геннадьевич. Комплексная система защиты информации на предприятии : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М. : Академия, 2009. – 416 с. – (Высшее профессиональное образование). – Текст : непосредственный.

5. Лопин, В. Н. Защита информации в компьютерных системах : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. – Курск : КГТУ, 2006. – 159 с. – Текст : непосредственный.

6. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун. – Курск : ЮЗГУ, 2013. – Ч. 1. – 150 с. – Текст : электронный.

7. Спеваков, А. Г. Основы правового обеспечения информационной безопасности : учебное пособие / А. Г. Спеваков, А. П. Фисун . – Курск : ЮЗГУ, 2013. – Ч. 2. – 303 с. – Текст : электронный.

8.3 Перечень методических указаний

1. Алгоритм шифрования RSA : методические указания к выполнению практических и лабораторных работ / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. – Курск : ЮЗГУ, 2022. – 11 с. – Текст : электронный.

2. Шифрование с помощью программы TrueCrypt : методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. – Курск : ЮЗГУ, 2022. – 20 с. – Текст : электронный.

3. Методы и средства защиты компьютерной информации : методические указания для самостоятельной работы по изучению дисциплины для студентов направления подготовки (специальности) 09.03.04 «Программная инженерия» / Юго-Зап. гос. ун-т ; сост. А. Л. Ханис. – Электрон. текстовые дан. (271 КБ). – Курск : ЮЗГУ, 2021. – 14 с. – Загл. с титул. экрана. – Б. ц. – Текст : электронный.

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».

2. http://school-collection.edu.ru/ - федеральное хранилище Единая коллекция цифровых образовательных ресурсов.

3. http://www.edu.ru/ - федеральный портал Российское образование.

4. http://www.igumo.ru/ - интернет-портал Института гуманитарного образования и информационных технологий.

5. http://elibrary.ru/defaultx.asp - научная электронная библиотека «Elibrary».

6. http://www.eduhmao.ru/info/1/4382/ - информационно-просветительский портал «Электронные журналы».

7. www.diss.rsl.ru – электронная библиотека диссертаций.

8. http://fictionbook.ru – электронная библиотека.

9. http://svitk.ru – электронная библиотека.

10. http://www.iqlib.ru – электронная библиотека образовательных и просветительных изданий.

11. http://www.lib.msu.su/index.html - Научная библиотека Московского государственного университета им. М.В.Ломоносова.

12. http://www.rsl.ru/ - Российская Государственная Библиотека.

13. http://e.lanbook.com/ - Электронно-библиотечная система «Лань».

14. http://window.edu.ru/ - Электронная библиотека «Единое окно доступа к образовательным ресурсам».

10 Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Методы и средства защиты компьютерной информации» являются лекции и лабораторные занятия.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, защиты отчетов по лабораторным работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Методы и средства защиты компьютерной информации»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со

студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному освоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Методы и средства защиты компьютерной информации» с целью освоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Методы и средства защиты компьютерной информации» – закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Программный продукт LibreOffice (свободно распространяемое ПО для некоммерческих целей) (ссылка на скачивание: ru.libreoffice.org/download/).

Программа анализа и управления информационными рисками «Гриф» (свободно распространяемое ПО для некоммерческих целей).

Программа хранения паролей PasswordCommander (свободно распространяемое ПО для некоммерческих целей).

Фаервол ComodoFirewall (свободно распространяемое ПО для некоммерческих целей).

Программа анализа защищенности операционной системы GFILANguardNetworkSecurityScanner.

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Криптографическая программа TrueCrypt.

Операционная система Windows.

Антивирус Касперского *(или ESETNOD)*.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения лекционных занятий требуется учебная аудитория для проведения занятий лекционного типа оснащенная:

– учебной мебелью: столы (в количестве не менее 1 на 2 обучающихся) и стулья для обучающихся (в количестве не менее списочного состава группы);

– столом и стулом для преподавателя;

– доской;

– видеопроектором и ноутбуком (для показа презентаций и учебных фильмов).

Проведение лабораторных занятий предполагается в учебной лаборатории кафедры информационной безопасности, оснащенной:

– учебной мебелью: столы (в количестве не менее 1 на 2 обучающихся) и стулья для обучающихся (в количестве не менее списочного состава группы);

– доской;

– столом и стулом для преподавателя;

– учебными компьютерами (в количестве не менее 1 устройство на 2 студентов), с предустановленными программными продуктами, перечисленными в п.11 настоящей программы.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента

(помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			