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 09.03.04Программная инженерия
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Разработка программно-
наименование направленности (профиля, специализации)

информационных систем»

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 №7 «30» 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 №6 «06» 02 2021 г., на заседании кафедры ИБ, протокол №1 от 30.08.2023.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины Методы и средства защиты коммерческой информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.03. Прикладная информатика направленность Прикладная информатика в экономике, одобренного Ученым советом университета протокол №_«__»___20_г., на заседании кафедры ИБ, протокол №1 от 29.08.2024.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____ Медведенко А.А.

Рабочая программа дисциплины Методы и средства защиты коммерческой информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.03. Прикладная информатика направленность Прикладная информатика в экономике, одобренного Ученым советом университета протокол №_«__»___20_г., на заседании кафедры_____.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины Методы и средства защиты коммерческой информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.03. Прикладная информатика направленность Прикладная информатика в экономике, одобренного Ученым советом университета протокол №_«__»___20_г., на заседании кафедры_____.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа дисциплины Методы и средства защиты коммерческой информации пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 09.04.03. Прикладная информатика направленность Прикладная информатика в экономике, одобренного Ученым советом университета протокол №_«__»___20_г., на заседании кафедры_____.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

(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 «Методы и средства защиты компьютерной информации» является изложение основметодики 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

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. Теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). ***Уметь:*** Анализировать взаимосвязи, выявлять пропущенную информацию. Определять наиболее затратные места в процессетестирования. 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.

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*		
			Оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки). ***Владеть:*** навыками разработки требований к тестированию.
ПК-8	Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта.	ПК-8.3 Контролирует выполнение заданий программистами.	***Знать:*** виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий, осуществлять обучение и наставничество. ***Владеть:*** навыками: навыками руководства программным проектом, контроля выполнения заданий, обучения программистов.

2. Указание места дисциплины в структуре основной профессиональнойобразовательной 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 (специалитета, магистратуры) 09.03.04Программная инженерия, направленностьРазработка 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 зачетные единицы (з.е.), 108академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	28
в том числе:	
лекции	14
лабораторные занятия	14
практические занятия	0
Самостоятельная работа обучающихся (всего)	79,9
Контроль (подготовка к экзамену)	0
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
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:
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 аутен-тификация 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 распределен-ные 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 собствен-ности 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 ее 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	1	-	-	У-1, У-2, У-3,	УО - 2	ПК-5

	информационной безопасности				У-4, У-5, У-7, МУ-1		
2	Проблемы информационной безопасности сетей	2	-	-	У-2, У-7, У-10, МУ-1	УО - 4	ПК-5
3	Политика безопасности	2	-	-	У-1, У-3, У-5, У-7, МУ-1	УО - 6	ПК-5
4	Криптографическая защита информации	2	1,2	-	У-1, У-4, У-7, МУ-1, МУ-2	УО – 8 ЗЛР – 4,8	ПК-5, ПК-8
5	Технологии аутентификации	1	-	-	У-4, У-6, У-7, У-8, МУ-1, МУ-3	УО - 10	ПК-5, ПК-8
6	Технологии межсетевых экранов	1	3	-	У-1,У-2, У-4,У-6, У-8, МУ-3	УО, ЗЛР - 12	ПК-5, ПК-8
7	Технологии защиты от вирусов	2	-	-	У-2, У-4,У-8, МУ-1, МУ-3	УО - 14	ПК-5, ПК-8
8	Требования к системам защиты информации	2	4	-	У-1-6, МУ-4	УО – 16 ЗЛР – 16	ПК-5, ПК-8
9	Основы правового обеспечения защиты информации	1	-	-	У-1, У-7-8	УО - 18	ПК-5, ПК-8
	Всего	14	14	0			

УО – устный опрос, ЗЛР – лабораторная работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
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		14

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
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	10 неделя	9
6	Технологии межсетевых экранов	12 неделя	9
7	Технологии защиты от вирусов	14 неделя	9
8	Требования к системам защиты информации	16 неделя	9
9	Основы правового обеспечения защиты информации	18 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 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 за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путемразработки:

- методических рекомендаций, пособий по организации

самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

–методических указаний к выполнению лабораторных и практических 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

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. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

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

№	Наименование раздела (лекции, практического 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 №2. Проблемы информационной безопасности сетей.	Анализ конкретных ситуаций	1
3	Лекция №3. Политика безопасности.	Анализ конкретных	1
4	Лабораторная работа №1. Разработка криптографической программы «Алгоритм RSA».	Анализ конкретных ситуаций	1
5	Лабораторная работа №2. Разработка криптографической программы «Шифр Виженера».	Анализ конкретных ситуаций	1
6	Лабораторная работа №3. Настройка межсетевого экрана в ОС Windows.	Анализ конкретных ситуаций	1
Итого			6

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован 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 общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, 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 данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки 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);

– 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.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональнойобразовательной 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		Производственная практика (научно-исследовательская работа).	Тестирование программного обеспечения. Разработка и анализ требований. Выполнение и защита выпускной квалификационной работы.
ПК-8. Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта.	Конструирование программного обеспечения.	Конструирование программного обеспечения.	Управление программными проектами. Тестирование программного обеспечения. Сети ЭВМ и телекоммуникации. Администрирование информационно-вычислительных систем. Производственная преддипломная практика. Выполнение и защита выпускной квалификационной работы.

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций*,	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)

	закрепленные за дисциплиной)			
1	2	3	4	5
ПК-5, завершающий.	ПК-5.1 Анализирует требования на реализуемость и пригодность к тестированию, формируя отчёт о корректности и документации.	Знать: в целом сформированные, но неполные знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять конечные данные для эксплуатации на основе разрабатываемых требованийопределять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками разработки требований к тестированию.	Знать: сформированные, но содержащие отдельные пробелы знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований определять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками анализа требований на реализуемость и пригодность к тестированию,	Знать: сформированные систематические знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований определять цели тестирования, разрабатывать требования к тестированию, оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки).

	ПК-5.2 Разрабатывает требования к тестированию на основе требований к программно-информационной системе.	Знать: в целом сформированные, но неполные знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять конечные данные для эксплуатации на основе разрабатываемых требованийопределять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками разработки требований к тестированию.	формирования отчетов о корректности документации, разработки требований к тестированию. Знать: сформированные, но содержащие отдельные пробелы знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований определять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками анализа требований на	Владеть: навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации Разработки требований к тестированию. Знать: сформированные систематические знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований определять цели тестирования, разрабатывать требования к тестированию,

			реализуемость и пригодность к тестированию, формирования отчетов о корректности документации, разработки требований к тестированию.	оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки) . Владеть: навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации Разработки требований к тестированию.
ПК-8, завершающий.	ПК-8.3 Контролирует выполнение заданий программистами.	Знать: виды технических спецификаций на программные компоненты. Уметь: разрабатывать технические спецификации и согласовывать их с архитектромПО. Владеть: навыками создания технических спецификаций.	Знать: виды технических спецификаций на программные компоненты; методологии конструирования ПО. Уметь: разрабатывать технические спецификации; согласовывать спецификации с архитектором ПО; распределять задания между программистами в соответствии с техническими спецификациями; руководить программным проектом. Владеть: навыками	Знать: виды технических спецификаций на программные компоненты; методологии конструирования ПО; виды технических спецификаций на программные компоненты. Уметь: разрабатывать технические спецификации; согласовывать спецификации с архитектором ПО; распределять задания между программистами в соответствии с техническими спецификациями; руководить программным проектом;

			создания технических спецификаций; создания архитектуры программных проектов; распределения заданий между программистами в соответствии с техническими спецификациями.	осуществлять контроль выполнения заданий; осуществлять обучение и наставничество. Владеть: навыками создания технических спецификаций; создания архитектуры программных проектов; распределения заданий между программистами в соответствии с техническими спецификациями; руководства программным проектом; контроля выполнения заданий; обучения программистов.

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

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её 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	Лекция, СРС	Вопросы для устного опроса	1-3	Согласно таблице 7.2
2	Проблемы информационной безопасности сетей	ПК-5	Лекция, СРС	Вопросы для устного опроса	4-14	Согласно таблице 7.2
3	Политика безопасности	ПК-5	Лекция, СРС	Вопросы для устного опроса	15-17	Согласно таблице 7.2
4	Криптографическая защита информации	ПК-5, ПК-8	Лекция, Лабораторные работы№ 1 №2, СРС	Вопросы для устного опроса КВЗЛР №1 КВЗЛР №2	18-24 1 –3 1 – 3	Согласно таблице 7.2
5	Технологии аутентификации	ПК-5, ПК-8	Лекция, СРС	Вопросы для устного опроса	25-30	Согласно таблице 7.2
6	Технологии межсетевых экранов	ПК-5, ПК-8	Лекция, Лабораторные работы№ 3, СРС	Вопросы для устного опроса КВЗЛР №4	31-33 1 - 4	Согласно таблице 7.2
7	Технологии защиты от вирусов	ПК-5, ПК-8	Лекция, СРС	Вопросы для устного опроса	34-41	Согласно таблице 7.2
8	Требования к системам защиты информации	ПК-5, ПК-8	Лекция, лабораторная работа №4, СРС	Вопросы для устного опроса КВЗЛР №4	42-46 1-4	Согласно таблице 7.2
9	Основы правового обеспечения защиты информации	ПК-5, ПК-8	Лекция, СРС	Вопросы для устного опроса	47-60	Согласно таблице 7.2

СРС – самостоятельная работа студента, КВЗЛР – контрольные вопросы для защиты лабораторных работ

Примеры типовых контрольных заданий для проведения

текущего контроля успеваемости

Вопросы дляустного опроса по разделу (теме) 1. «Основные понятия и анализ угроз информационной безопасности».

1. Основные понятия защиты информации и информационной безопасности.
2. Классификация угроз информационной безопасности компьютерных сетей.
3. Непосредственные виды угроз для компьютерных сетей: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров информационной системы.

Контрольные вопросы для защиты лабораторной работы №2:

Разработка криптографической программы «Шифр Виженера»
1. Квадрат (таблица) Виженера
2. Алфавитный шифр
3. Количество символов в строке для русского алфавита

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

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

Промежуточная аттестация по дисциплине проводится в формезачёта.Зачёт проводится в виде бланкового 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. Все темы дисциплины отражены в КИМ в равных долях (%). 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 (или опыт деятельности) 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 проведенияпромежуточной аттестации обучающихся

Задание в закрытой форме:

1. 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:

1. Угрозы нарушения целостности информации приводят к …….
2. В компьютерной сети перехват данных, передаваемых по каналам связи относится к уровню ……..
3. Пассивной угрозой информационной безопасности является……...

Задание на установление правильной последовательности.

Установить в порядкеувеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

Задание на установление соответствия:

между элементами ПК и функциями элементов

1	Процессор	А	Хранение информации
2	Оперативная память	Б	Обработка информации
3	Жесткий диск	В	Отображение информации
4	Монитор	Г	Ввод информации

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 02.016–2018 Обалльно-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
Устный опрос по темам 1-3	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Устный опрос по темам 4-6	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Устный опрос по темам 7-9	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Лабораторная работа №1 «Разработка криптографической программы «Алгоритм RSA»»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №2 «Разработка криптографической программы «Шифр Виженера»»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №3 «Настройка межсетевого экрана в ОС Windows»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №4 «Шифрование с помощью программы TrueCrypt»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	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 –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 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 по выполнению практических работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.03.01 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с. - Текст : электронный.

2. Шифрование с помощью таблицы Виженера : методические указания по выполнению практических работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.03.01 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с. - Текст : электронный.

3. Настройка межсетевого экрана в операционной системе Windows : методические указания по выполнению лабораторной работы по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для студентов укрупненной группы специальностей 10.00.00 / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 19 с. : ил., табл. - Библиогр.: с. 19. - Текст : электронный.

4. Шифрование с помощью программы TrueCrypt : методические указания по выполнению лабораторных работ по дисциплинам «Методы и средства защиты компьютерной информации», для студентов направления подготовки бакалавров 09.03.04, «Информационная безопасность» для студентов направлений подготовки бакалавров 09.03.02, 09.03.03, 45.03.03. / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2017. - 20 с. - Текст : электронный.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца

2. Журнал «InformationSecurity/Информационная безопасность.»- http://window.edu.ru/

3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- http://window.edu.ru/

4. Журнал «Вестник УрФО. Безопасность в информационной сфере»

5. Журнал «Вопросы защиты информации»

6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

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

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания дляобучающихся поосвоениюдисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность» являются лекции, практические 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 конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические и 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 и работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защита информационных процессов в компьютерных системах»: 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, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации 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 усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность» - 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)

Программа анализа и управления информационными рисками “Гриф”.(свободное ПО).

Программа хранения паролей PasswordCommander(свободное ПО).

ФаерволComodoFirewall (свободное ПО).

Программа анализа защищенности операционной системы GFILAN-guardNetworkSecurityScanner.

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

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

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

Криптографическая программа TrueCrypt.

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

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. 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
	Изме-нённых	Заменённых	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 09.03.04Программная инженерия
(шифр согласно ФГОС и наименование направления подготовки (специальности))

направленность (профиль, специализация) «Разработка программно-
наименование направленности (профиля, специализации)

информационных систем»

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 № 11 «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 №7 «28.02»2022 г., на заседании кафедры КБ, 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 №6 «26.02»2021 г., на заседании кафедры КБ, протокол №1 от 30.08.2023.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

(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 «Методы и средства защиты компьютерной информации» является изложение основметодики 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

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. Теорию тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). ***Уметь:*** Анализировать взаимосвязи, выявлять пропущенную информацию. Определять наиболее затратные места в процессетестирования. 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.

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*		
			Оценивать важность (приоритет выполнения) различных тестов (на основе приоритетов пользователя, проектных задач и рисков возникновения ошибки). ***Владеть:*** навыками разработки требований к тестированию.
ПК-8	Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта.	ПК-8.3 Контролирует выполнение заданий программистами.	***Знать:*** виды технических спецификаций на программные компоненты. ***Уметь:*** осуществлять контроль выполнения заданий, осуществлять обучение и наставничество. ***Владеть:*** навыками: навыками руководства программным проектом, контроля выполнения заданий, обучения программистов.

2. Указание места дисциплины в структуре основной профессиональнойобразовательной 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 (специалитета, магистратуры) 09.03.04Программная инженерия, направленностьРазработка 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 зачетные единицы (з.е.), 108академических часов.

Таблица 3 - Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	8
в том числе:	
лекции	4
лабораторные занятия	4
практические занятия	0
Самостоятельная работа обучающихся (всего)	95,9
Контроль (подготовка к экзамену)	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 предусмотрена
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. Политика безопасности.	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. Пути решения проблем защиты информации в сетях. 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.
3	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.
4	Технологии аутентификации.Технологии межсетевых экранов.	Аутентификация, авторизация и администрирование действий пользователей. Аппаратно-программные системы идентификации и аутентификации. 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. Основные схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Проблемы безопасности межсетевых экранов.

Таблица 4.1.2 - Содержание дисциплины и ее 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	1	-	-	У-1-3, У-4, У-5, У-7	УО - 4	ПК-5

	информационной безопасности						
2	Проблемы информационной безопасности сетей. Политика безопасности.	1	-	-	У-2, У-7, У-8	УО - 8	ПК-5, ПК-8
3	Криптографическая защита информации	1	1,2	-	У-1, У-3, У-5-7, МУ-1, 2	УО – 6 ЗЛР – 10, 12	ПК-5, ПК-8
4	Технологии аутентификации. Технологии межсетевых экранов.	1	3,4	-	У-1, У-4, У-7,8 МУ-3, МУ-4	УО – 8 ЗЛР – 16, 18	ПК-5, ПК-8
	Всего	4	4	0			

УО – устный опрос, ЗЛР – лабораторная работа

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 - Лабораторные работы

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

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 - Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	Основные понятия и анализ угроз информационной безопасности	4 неделя	23,9
2	Проблемы информационной безопасности сетей. Политика безопасности	8 неделя	24
3	Криптографическая защита информации	12 неделя	24
4	Технологии аутентификации. Технологии межсетевых экранов	18 неделя	24
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 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 за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_tele/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

путемразработки:

- методических рекомендаций, пособий по организации самостоятельной работы студентов;

– заданий для самостоятельной работы;

– вопросов и задач к зачёту;

–методических указаний к выполнению лабораторных и практических 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

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. В рамках дисциплины предусмотрены встречи с экспертами и специалистами Комитета цифрового развития и связи Курской области.

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

№	Наименование раздела (лекции, практического 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	Лабораторная работа №3. Настройка межсетевого экрана в ОС Windows.	Анализ конкретных ситуаций	1
Итого			2

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован 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 общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, 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 данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки 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);

– 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.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональнойобразовательной 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		Производственная практика (научно-исследовательская работа).	Тестирование программного обеспечения. Разработка и анализ требований. Выполнение и защита выпускной квалификационной работы.

ПК-8. Способен формализовать предметную область программного обеспечения и разрабатывать спецификации для компонентов программного продукта.	Конструирование программного обеспечения.	Конструирование программного обеспечения.	Управление программными проектами. Тестирование программного обеспечения. Сети ЭВМ и телекоммуникации. Администрирование информационно-вычислительных систем. Производственная преддипломная практика. Выполнение и защита выпускной квалификационной работы.

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

Таблица 7.2 Показатели, критерии и шкала оценивания компетенций

Код компетенции/ этап (указывается название этапа изп.7.1)	Показатели оценивания компетенций *(индикаторы достижения компетенций, закрепленные за дисциплиной)*	Критерии и шкала оценивания компетенций		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
ПК-5, завершающий.	ПК-5.1 Анализирует требования на реализуемость и пригодность к тестированию, формируя отчёт о корректности документации.	Знать: в целом сформированные, но неполные знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов). Уметь: анализировать взаимосвязи, выявлять пропущенную	Знать: сформированные, но содержащие отдельные пробелы знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. Уметь: анализировать	Знать: сформированные систематические знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. Уметь: анализировать взаимосвязи, выявлять

		информацию, определять конечные данные для эксплуатации на основе разрабатываемых требованийопределять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками разработки требований к тестированию.	взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований определять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации, разработки требований к тестированию. Знать: сформированные, но содержащие отдельные пробелы знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники	пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований 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 анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации Разработки требований к тестированию. Знать: сформированные систематические знания методов анализа и тестирования требований, теории тестирования (модели
	ПК-5.2 Разрабатывает требования к тестированию на основе требований к программно-информационной системе.	Знать: в целом сформированные, но неполные знания методов анализа и тестирования требований, теории тестирования (модели тестирования, планирование тестирования, тест-		

		дизайн, проектирование тестов). Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять конечные данные для эксплуатации на основе разрабатываемых требованийопределять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками разработки требований к тестированию.	тестирования. Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований определять цели тестирования, разрабатывать требования к тестированию. Владеть: навыками анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации, разработки требований к тестированию.	тестирования, планирование тестирования, тест-дизайн, проектирование тестов), техники тестирования. Уметь: анализировать взаимосвязи, выявлять пропущенную информацию, определять наиболее затратные места в процессе тестирования, определять конечные данные для эксплуатации на основе разрабатываемых требований 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 анализа требований на реализуемость и пригодность к тестированию, формирования отчетов о корректности документации Разработки требований к тестированию.

ПК-8, завершающий.	ПК-8.3 Контролирует выполнение заданий программистами.	Знать: виды технических спецификаций на программные компоненты. Уметь: разрабатывать технические спецификации и согласовывать их с архитектромПО. Владеть: навыками создания технических спецификаций.	Знать: виды технических спецификаций на программные компоненты; методологии конструирования ПО. Уметь: разрабатывать технические спецификации; согласовывать спецификации с архитектором ПО; распределять задания между программистами в соответствии с техническими спецификациями; руководить программным проектом. Владеть: навыками создания технических спецификаций; создания архитектуры программных проектов; распределения заданий между программистами в соответствии с техническими спецификациями.	Знать: виды технических спецификаций на программные компоненты; методологии конструирования ПО; виды технических спецификаций на программные компоненты. Уметь: разрабатывать технические спецификации; согласовывать спецификации с архитектором ПО; распределять задания между программистами в соответствии с техническими спецификациями; руководить программным проектом; осуществлять контроль выполнения заданий; осуществлять обучение и наставничество. Владеть: навыками создания технических спецификаций; создания архитектуры программных проектов; распределения заданий между программистами в соответствии с техническими спецификациями; руководства программным проектом; контроля

				выполнения заданий; обучения программистов.

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

Таблица 7.3 Паспорт комплекта оценочных средств для текущего контроля успеваемости

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её 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	Лекция, СРС	Вопросы для устного опроса	1-11	Согласно таблице 7.2
2	Проблемы информационной безопасности сетей. Политика безопасности	ПК-5, ПК-8	Лекция, СРС	Вопросы для устного опроса	12-28	Согласно таблице 7.2
3	Криптографи-ческая защита информации	ПК-5, ПК-8	Лекция, Лабораторные работы№ 1 №2, СРС	Вопросы для устного опроса КВЗЛР №1 КВЗЛР №2	29 - 46 1 - 4 1 - 3	Согласно таблице 7.2
4	Технологии аутентификации.Технологии межсетевых экранов.	ПК-5, ПК-8	Лекция, Лабораторные работы№ 3 №4, СРС	Вопросы для устного опроса КВЗЛР №3 КВЗЛР №4	47 - 60 1 - 3 1 - 4	Согласно таблице 7.2

СРС – самостоятельная работа студента, КВЗЛР – контрольные вопросы для защиты лабораторных работ

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы дляустного опроса по разделу (теме) 1. «Основные понятия и анализ угроз информационной безопасности».

1. Основные понятия защиты информации и информационной безопасности.
2. Классификация угроз информационной безопасности компьютерных сетей.
3. Непосредственные виды угроз для компьютерных сетей: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров информационной системы.

Контрольные вопросы для защиты лабораторной работы №2:

Разработка криптографической программы «Шифр Виженера»
1. Квадрат (таблица) Виженера
2. Алфавитный шифр
3. Количество символов в строке для русского алфавита

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

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачёта.

Промежуточная аттестация по дисциплине проводится в формезачёта.Зачёт проводится в виде бланкового 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. Все темы дисциплины отражены в КИМ в равных долях (%). 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 (или опыт деятельности) 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 проведенияпромежуточной аттестации обучающихся

Задание в закрытой форме:

1. 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:

1. Угрозы нарушения целостности информации приводят к …….
2. В компьютерной сети перехват данных, передаваемых по каналам связи относится к уровню ……..
3. Пассивной угрозой информационной безопасности является……...

Задание на установление правильной последовательности.

Установить в порядкеувеличения единицы измерения количества информации:

1. 1 ТБ

2. 30 Гбайт

3. 50 Килобайт

4. 100 Мегабайт

Задание на установление соответствия:

между элементами ПК и функциями элементов

1	Процессор	А	Хранение информации
2	Оперативная память	Б	Обработка информации
3	Жесткий диск	В	Отображение информации
4	Монитор	Г	Ввод информации

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 02.016–2018 Обалльно-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
Устный опрос по темам 1-3	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Устный опрос по темам 4-6	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Устный опрос по темам 7-9	4	Доля правильных ответов от 50% до 90%	8	Доля правильных ответов более 90%
Лабораторная работа №1 «Разработка криптографической программы «Алгоритм RSA»»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №2 «Разработка криптографической программы «Шифр Виженера»»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №3 «Настройка межсетевого экрана в ОС Windows»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Лабораторная работа №4 «Шифрование с помощью программы TrueCrypt»	3	Выполнил, доля правильных ответов от 50% до 90%	6	Выполнил, доля правильных ответов более 90%
Итого	24		48	
Посещаемость	0		16	
Зачёт	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 –2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 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 по выполнению практических работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.03.01 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с. - Текст : электронный.

2. Шифрование с помощью таблицы Виженера : методические указания по выполнению практических работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.03.01 / Юго-Зап. гос. ун-т ; сост. А. Л. Марухленко. - Курск : ЮЗГУ, 2017. - 10 с. - Текст : электронный.

3. Настройка межсетевого экрана в операционной системе Windows : методические указания по выполнению лабораторной работы по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для студентов укрупненной группы специальностей 10.00.00 / Юго-Зап. гос. ун-т ; сост. М. О. Таныгин. - Курск : ЮЗГУ, 2017. - 19 с. : ил., табл. - Библиогр.: с. 19. - Текст : электронный.

4. Шифрование с помощью программы TrueCrypt : методические указания по выполнению лабораторных работ по дисциплинам «Методы и средства защиты компьютерной информации», для студентов направления подготовки бакалавров 09.03.04, «Информационная безопасность» для студентов направлений подготовки бакалавров 09.03.02, 09.03.03, 45.03.03. / Юго-Зап. гос. ун-т ; сост. К. А. Тезик. - Курск : ЮЗГУ, 2017. - 20 с. - Текст : электронный.

8.4 Другие учебно-методические материалы

Периодические издания:

1. «Защита информации. Инсайд» [Текст] : информ.-метод. журн./ учредитель ООО "Издательский дом "Афина". - Санкт- Петербург : Афина. - Выходит раз в два месяца
2. Журнал «InformationSecurity/Информационная безопасность.»- http://window.edu.ru/
3. Журнал «Проблемы информационной безопасности. Компьютерные системы»- http://window.edu.ru/
4. Журнал «Вестник УрФО. Безопасность в информационной сфере»

5. Журнал «Вопросы защиты информации»
6. Журнал «БДИ (Безопасность. Достоверность. Информация.)»
7. Журнал «Информация и безопасность.»

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

1. http://e.lanbook.com - Электронно-библиотечная система «Лань».
2. http://www.iqlib.ru - Электронно-библиотечная система IQLib.
3. http://window.edu.ru -Электронная библиотека «Единое окно доступа к образовательным ресурсам».
4. http://biblioclub.ru – Электронно-библиотечная система «Университетская библиотека онлайн».
5. http://www.fsb.ru - Федеральная служба безопасности [официальный сайт].
6. http://fstec.ru - Федеральная служба по техническому и экспортному контролю [официальный сайт].
7. http://microsoft.com - Корпорация Microsoft[официальный сайт].
8. http://www.consultant.ruКомпания«Консультант Плюс» [официальный сайт].

10. Методические указания дляобучающихся поосвоениюдисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность» являются лекции, практические 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 конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические и 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 и работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защита информационных процессов в компьютерных системах»: 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, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседованиях). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации 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 усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность» - 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)

Программа анализа и управления информационными рисками “Гриф”.(свободное ПО).

Программа хранения паролей PasswordCommander(свободное ПО).

ФаерволComodoFirewall (свободное ПО).

Программа анализа защищенности операционной системы GFILAN-guardNetworkSecurityScanner.

MicrosoftOffice 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №К0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

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

Windows 7, договор IT000012385

Антивирусная программа Kaspersky Internet Security.

Криптографическая программа TrueCrypt.

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

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут-букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/проекторinFocusIN24+

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. 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	Номера страниц	Всего	Дата	Основание для

изменения	Изме-нённых	Заменённых	Аннулированных	новых	страниц		изменения и подпись лица, проводившего изменения