

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»



УТВЕРЖДАЮ

Декан ФИТКБ

/Гусев П.Ю./

31.08.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Методы и системы защиты информации,
информационная безопасность»

Направление подготовки 10.06.01 ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Профиль 05.13.19 Методы и системы защиты информации,
информационная безопасность

Квалификация выпускника Исследователь. Преподаватель-исследователь

Нормативный период обучения 4 года

Форма обучения очная

Год начала подготовки 2021

Автор программы
Заведующий кафедрой Си-
стем информационной без-
опасности

К.А. Разинкин

Руководитель ОПОП

А.Г. Остапенко

А.Г. Остапенко

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины сформировать у преподавателя-исследователя систему знаний, умений и навыков, связанную с исследованием проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения, а также обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации

1.2. Задачи освоения дисциплины

формирование компетенций по формулировке научных задач в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность;

приобретение навыков, знаний и умений по разработке новых и совершенствованию имеющихся методов и средств защиты информации и обеспечения информационной безопасности;

приобретение навыков, знаний и умений к построению систем обеспечения информационной безопасности объектов защиты, в том числе автоматизированных систем; положения типовых методик оценки рисков нарушения информационной безопасности; основные подходы к проектированию системы менеджмента информационной безопасности;

формирование навыков анализа программных реализаций на предмет наличия уязвимостей

приобретение навыков, знаний и умений по противодействию механизмам информационного воздействия, основными функциями и классификацией результатов информационного управления.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы и системы защиты информации, информационная безопасность» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Методы и системы защиты информации, информационная безопасность» направлен на формирование следующих компетенций:

ОПК-1 - способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять

полученные результаты в практическую деятельность

ОПК-3 - способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности

ПК-2 - способность выявлять угрозы нарушения и владение методами и средствами обеспечения информационно-психологической безопасности

ПК-3 - способность пользоваться мерами риска и владение методами оценки информационных рисков

ПК-6 - способность выявлять угрозы и уязвимости нарушения информационной безопасности, осуществлять выбор адекватных методов и систем защиты информации

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-1	знать особенности исследования проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения
	уметь применять методы защиты информации с целью обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации
ОПК-3	знать обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации
	уметь обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности
ПК-2	знать основные технологии информационно-психологического воздействия
	уметь анализировать информационно-психологическое воздействие в информационных процессах
	владеть методами и средствами обеспечения информационно-психологической безопасности
ПК-3	знать подходы к построению систем обеспечения информационной безопасности объектов

	защиты, в том числе автоматизированных систем; положения типовых методик оценки рисков нарушения информационной безопасности; основные подходы к проектированию системы менеджмента информационной безопасности
	уметь производить анализ рисков информационной безопасности, контролировать эффективность мер комплексной защиты информации объектов, в том числе автоматизированных систем.
	владеть навыками контроля реализации политики информационной безопасности, управления защитой информации в автоматизированных системах
ПК-6	знать методики категорирования объектов и нормативные базы анализа угроз и уязвимостей ИБ
	уметь осуществлять формальное описание угроз и уязвимостей, модели нарушителя
	владеть навыками выявления и устранения уязвимостей

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Методы и системы защиты информации, информационная безопасность» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		5	6
Аудиторные занятия (всего)	32	14	18
В том числе:			
Лекции	32	14	18
в том числе в форме практической подготовки	12	6	6
Самостоятельная работа	157	58	99
Часы на контроль	27	-	27
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость:			
академические часы	216	72	144
зач.ед.	6	2	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	СР С	Всего, час
1	Теория и методология обеспечения информационной безопасности и защиты информации	Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса. Системы документооборота и средства защиты циркулирующей в них информации	6	26	32
		<i>практическая подготовка обучающихся</i>	2	-	2
2	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.	<p>Определение и природа угроз информации в современных системах ее обработки.</p> <p>Классификация и общая характеристика основных угроз. Понятие уязвимости информации. Подходы к определению значений показателей уязвимости. Эмпирические методы определения значений показателей уязвимости. Примеры эмпирических моделей. Способы определения параметров моделей. Особенности использования моделей.</p> <p>Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей. Примеры моделей. Особенности и проблемы практического использования.</p> <p>Теоретико-эмпирические методы определения значений показателей.</p> <p>Подходы к построению теоретико-эмпирических моделей. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения. Методы и модели прогнозирования значений показателей уязвимости. Определение, значение, структура и способы формирования инструментальных средств оценки уязвимости информации.</p>	6	26	32

		<i>практическая подготовка обучающихся</i>	2	-	2
3	Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.	Место анализа рисков в общей схеме управления ИБ. Подходы к оценке рисков ИБ: качественный, количественный. Экономическая модель оценки рисков. Вероятностная модель оценки рисков Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010. Методы оценки риска Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ Методики и ПО для оценки рисков ИБ. Оценка критичных угроз, активов и уязвимостей OCTAVE. Средство качественной оценки vsRisk. Методики и ПО для оценки рисков ИБ. Метод анализа и управления рисками CRAMM. Средство оценки рисков Microsoft Security Assessment Tools. Методики и ПО для оценки рисков ИБ. Средство количественной оценки рисков PracticalThreatAnalysis. Методика Risk Watch Методики и ПО для оценки рисков ИБ. Методика управления рисками Microsoft The Security Risk Management Guide. Средство оценки рисков R-Vision Risk Manager Принятие решений по результатам оценки рисков. Политика обработки рисков.	12	52	64
		<i>практическая подготовка обучающихся</i>	4	-	4
4	Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.	Защита автоматизированных систем от удаленных атак через сеть Internet. Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты. Защита информации от несанкционированного доступа (НСД). Каналы утечки информации. Защита компонентов автоматизированных систем от НСД. Антивирусная защита. Системы анализа за-	4	26	30

		<p>щищённости и обнаружения вторжений. Модель и источники каналов утечки информации. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизасемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; компьютерные вирусы как особый класс разрушающих программных воздействий; защита от разрушающих программных воздействий; понятие изолированной программной среды.</p> <p>Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации.</p> <p>Парольные системы опознавания, их сущность, содержание, достоинства и недостатки. Способы повышения надежности парольных систем. Другие системы опознавания. Средства опознавания аппаратуры, программ, массивов данных.</p> <p>Методы идентификации и проверки подлинности пользователей автоматизированных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных.</p> <p>Биометрическая идентификация и аутентификация пользователей: основные понятия и механизмы. «Fuzzy</p>			
--	--	---	--	--	--

		<p>extractors». Искусственные нейронные сети в преобразователях биометрия-код. Алгоритм быстрого обучения искусственной нейронной сети. Алгоритм ускоренного тестирования нейросетевого преобразователя биометрия-код (НПБК). Алгоритм полного тестирования НПБК. Базы биометрических образов: назначение, виды, требования к формированию. Нейросетевой биометрический контейнер (НБК): назначение, виды. Наиболее вероятные атаки на НБК, защита от них. Программные средства разграничения доступа, их сущность, достоинства и недостатки. Модели разграничения доступа. Разграничение доступа по уровням и кольцам секретности, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения. Примеры систем разграничения доступа. Другие программные средства защиты: регистрации, сигнализации, реагирования и т.п. Программы защиты ЭВМ от электронных вирусов. Способы организации и использования программных средств защиты. Организационно-правовые средства защиты, их сущность, возможности, достоинства и недостатки. Критерии классификации организационно-правовых средств, классификационная структура и общая характеристика. Система законов, регламентирующих защиту информации в РФ. Перечень основных законов, основное их содержание и порядок действия. Руководящие методические материалы (РММ) по защите информации. Назначение и состав необходимых РММ. Перечень и содержание имеющихся РММ. Организационные мероприятия по защите информации, их сущность и назначение. Системная классификация организационных мероприятий. Мероприятия, проводимые на различных этапах жизненного цикла систем</p>			
--	--	---	--	--	--

		обработки данных.			
		<i>практическая подготовка обучающихся</i>	2	-	2
5	Модели и методы управления информационной безопасностью.	<p>Необходимость, сущность и основные понятия управления информационной безопасностью.</p> <p>Служба информационной безопасности на объекте. Назначение и организационно-правовой статус службы. Функции и задачи службы, способы и методы их решения.</p> <p>Создание, поддержка, оценка эффективности, совершенствование системы управления информационной безопасности.</p> <p>Методы и модели управления рисками информационной безопасности.</p> <p>Формирование критериев влияния, оценивания, принятия рисков.</p> <p>Итерационные процедуры управления рисками информационной безопасности.</p> <p>Методы и модели оценки рисков информационной безопасности.</p> <p>Методы идентификации рисков информационной безопасности активов.</p> <p>Методы формирования сценариев инцидентов, модели сценариев инцидентов. Методы идентификации и анализа последствий инцидентов различного вида. Оценка ущерба в результате нарушения безопасности.</p> <p>Методы оценивания рисков информационной безопасности. Методы обработки рисков информационной безопасности. Оценка вариантов обработки рисков.</p> <p>Оценка эффективности выбранных защитных мер. Методы управления изменениями систем.</p> <p>Управление инцидентами информационной безопасности. Обнаружение и анализ инцидентов. Методы реагирования на инциденты информационной безопасности.</p> <p>Управление непрерывностью функционирования систем и объектов</p> <p>Методы и модели мониторинга информационной безопасности.</p> <p>Структура систем мониторинга.</p> <p>Методы аудита информационной без-</p>	4	27	31

		опасности. Оценка соответствия защитных мер, процессов обеспечения информационной безопасности. Методы выявления и анализа свидетельств оценки. Организация обучения и осведомления персонала информационной безопасности.			
		<i>практическая подготовка обучающихся</i>	2	-	2
Итого			32	157	189

Практическая подготовка при освоении дисциплины (модуля) проводится путем непосредственного выполнения обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью, способствующих формированию, закреплению и развитию практических навыков и компетенций по профилю соответствующей образовательной программы на практических занятиях и (или) лабораторных работах:

№ п/п	Перечень выполняемых обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью	Формируемые профессиональные компетенции
1	Формализация моделей и использование инструментов выявления, идентификации и классификации угроз нарушения информационной безопасности	ПК-2, ПК-3, ПК-6
2	Теоретико-вероятностные методы определения значений показателей уязвимости	ПК-2, ПК-3, ПК-6
3	Методики и ПО для оценки рисков ИБ.	ПК-2, ПК-3, ПК-6
4	Методы искусственного интеллекта в обеспечении внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности	ПК-2, ПК-3, ПК-6
5	Теоретико-игровые и имитационные модели информационного влияния в сетевых структурах	ПК-2, ПК-3, ПК-6

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций

на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе: «аттестован»; «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-1	знать особенности исследования проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения	знание особенности исследования проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять методы защиты информации с целью обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации	умение применять методы защиты информации с целью обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-3	знать обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации	знание обеспечения информационной безопасности объектов политической, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	умение обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-2	знать основные технологии информационно-психологического воздействия	знание основные технологии информационно-психологического воздействия	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь анализировать информационно-психологическое воздействие в информационных процессах	умение анализировать информационно-психологическое воздействие в информационных процессах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	владеть методами и средствами обеспечения информационно-психологической безопасности	владение методами и средствами обеспечения информационно-психологической безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-3	знать подходы к построению систем обеспечения информационной безопасности объектов защиты, в том числе автоматизированных систем; положения типовых методик оценки рисков нарушения информационной безопасности; основные подходы к проектированию системы менеджмента информационной безопасности	знание подходов к построению систем обеспечения информационной безопасности объектов защиты, в том числе автоматизированных систем; положения типовых методик оценки рисков нарушения информационной безопасности; основные подходы к проектированию системы менеджмента информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь производить анализ рисков информационной безопасности, контролировать эффективность мер комплексной защиты информации объектов, в том числе автоматизированных систем.	умение производить анализ рисков информационной безопасности, контролировать эффективность мер комплексной защиты информации объектов, в том числе автоматизированных систем.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками контроля реализации политики информационной безопасности, управления защитой информации в автоматизированных системах	владение навыками контроля реализации политики информационной безопасности, управления защитой информации в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-6	знать методики категорирования объектов и нормативные базы анализа угроз и уязвимостей ИБ	знание методики категорирования объектов и нормативные базы анализа угроз и уязвимостей ИБ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлять формальное описание угроз и уязвимостей, модели нарушителя	умение осуществлять формальное описание угроз и уязвимостей, модели нарушителя	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками выявления и устранения уязвимостей	владение навыками выявления и устранения уязвимостей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 5, 6 семестре для очной формы обучения по двухбалльной системе:

«зачтено» «не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
-------------	---	---------------------	---------	------------

ОПК-1	знать особенности исследования проблем разработки, совершенствования и применения методов и средств защиты информации в процессе ее сбора, хранения, обработки, передачи и распространения	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь применять методы защиты информации с целью обеспечения информационной безопасности объектов политической, социальной, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-3	знать обеспечения информационной безопасности объектов политической, социальной, социально-экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз хищения, разрушения и/или модификации информации	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-2	знать основные технологии информационно-психологического воздействия	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь анализировать информационно-психологическое воздействие в информационных процессах	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть методами и средствами обеспечения	Решение прикладных задач в конкретной предметной	Продемонстрирован	Задачи не решены

	информационно-психологической безопасности	области	верный ход решения в большинстве задач	
ПК-3	знать подходы к построению систем обеспечения информационной безопасности объектов защиты, в том числе автоматизированных систем; положения типовых методик оценки рисков нарушения информационной безопасности; основные подходы к проектированию системы менеджмента информационной безопасности	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь производить анализ рисков информационной безопасности, контролировать эффективность мер комплексной защиты информации объектов, в том числе автоматизированных систем.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками контроля реализации политики информационной безопасности, управления защитой информации в автоматизированных системах	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-6	знать методики категорирования объектов и нормативные базы анализа угроз и уязвимостей ИБ	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь осуществлять формальное описание угроз и уязвимостей, модели нарушителя	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками выявления и устранения уязвимостей	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Какой из компонентов подсистемы безопасности Windows предназначен для контроля за доступом к объектам?

Encrypted File System

NT File System

Security Account Manager

Security Reference Monitor

2. К какому типу протоколов относится протокол SSL?

К протоколам прямой аутентификации

К протоколам автономной аутентификации

К протоколам установления защищенной связи на сетевом уровне

К протоколам не прямой аутентификации

3. В чем сущность комплексного подхода к защите информации?

В использовании комплексных систем защиты информации

В привлечении к защите информации коллектива квалифицированных экспертов

В использовании комплекса защитных мер

Защита информации это постоянный процесс, проводимый с использованием всех существующих методов и средств

4. Что не относится к динамическим (поведенческим) биометрическим характеристикам?

Термограмма лица, шеи и верхней части груди

Клавиатурный "почерк"

Тембр голоса

Рукописная подпись

5. Что такое информационная безопасность?

Состояние защищенности информационной среды объекта

Деятельность по созданию безопасных информационных систем

Деятельность по обеспечению защищенности информации

Деятельность по предотвращению утечки информации, непреднамеренного и несанкционированного воздействия на информацию

6. Что понимается под затенением файла с паролями пользователей?

Запрет доступа к файлу для непривилегированных пользователей

Перенос на защищенный от несанкционированного чтения носитель

Замена символов паролей

Запрет доступа к файлу для любых процессов

7. Какая из криптосистем не используется в системах электронной подписи?

Эллиптических кривых

Диффи-Хеллмана

Эль-Гамала

RSA

8. Что относится к локальному уровню правового регулирования информационной безопасности?

Принятие государственных стандартов
Принятие постановлений правительства
Утверждение перечня сведений, составляющих коммерческую

тайну

Принятие федеральных законов

9. Какие виды антивирусных программ принципиально могут обнаруживать только уже известные вредоносные программы?

Эвристические анализаторы

Инспекторы (ревизоры)

Сканеры

Мониторы (сторожа)

Вакцины

7.2.2 Примерный перечень заданий для решения стандартных задач

1. В проекте профиля защиты [PPMOS] предусмотрены максимальные квоты

долговременной памяти

суммарного времени сеансов

суммарного сетевого трафика

2. Служба директорий предоставляет следующие группы операций:

захват

опрос

верификация

3. Формирование контекстов безопасности в IPsec разделено на

две фазы

три фазы

четыре фазы

4. В "Оранжевой книге" фигурируют понятия:

ядро безопасности

периметр безопасности

центр безопасности

5. Если для передачи записей выстроится очередь сообщений разных типов, то приоритет прикладных данных окажется

минимальным

промежуточным

максимальным

6. В обобщенном прикладном программном интерфейсе службы безопасности удостоверения выступают как средство

аутентификации

контроля целостности

обеспечения конфиденциальности

7. В случае нарушения информационной безопасности следует предпочесть стратегию "защититься и продолжить", если

активы организации недостаточно защищены

активы организации надежно защищены

нет достоверных сведений о защищенности активов организации

8. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", в документах группы реагирования должна быть приведена следующая контактная информация:

адрес обычной почты

адрес электронной почты

адрес информационного сервера

9. В стандарте BS 7799 выделены следующие ключевые регуляторы безопасности:

документ о политике информационной безопасности

программа безопасности

регулярное выявление уязвимых мест

10. Согласно стандарту FIPS 140-2, перед криптографическим модулем ставятся следующие высокоуровневые функциональные цели безопасности:

предотвращение несанкционированной и необнаруживаемой модификации модуля и криптографических алгоритмов

предотвращение несанкционированной модификации, подмены, вставки и удаления криптографических ключей

предотвращение несанкционированной модификации ограниченного эксплуатационного окружения

11. Согласно спецификации X.800, ни на сетевом, ни на транспортном уровнях эталонной семиуровневой модели не реализуются следующие функции безопасности:

избирательная конфиденциальность

конфиденциальность трафика

неотказуемость

7.2.3 Примерный перечень заданий для решения прикладных задач

В соответствии с вариантом выполнить следующие действия.

1. Получить у преподавателя описание ИС (Приложение В).

2. Для данной ИС построить модель угроз и уязвимостей: выделить угрозы, применимые к рассматриваемой ИС; выделить уязвимости, через которые могут быть реализованы угрозы; определить угрозы, которые могут воздействовать на каждый из ресурсов в рамках ИС, и обосновать причины наличия этих угроз; определить уязвимости, через которые могут быть реализованы указанные угрозы.

3. Определить вероятности и критичности реализации угроз через уязвимости для каждой пары "угроза-уязвимость".

4. Определить функции для расчета рисков.

5. Рассчитать риски для всех ресурсов в рассматриваемой модели ИС.

6. Провести анализ полученных результатов. Выделить наиболее опасные уязвимости и предложить способы снижения вероятности и критичности. Предложить дальнейший план развития политики информационной безопасности для рассматриваемой ИС.

Вариант 1. Совокупная стоимость активов организации составляет 100 000 у.е. На учредительном собрании руководство приняло решение о реализации перспективного направления в производстве. Для нового отдела были закуплены 10 персональных компьютеров, каждый стоимостью 400 у.е. На каждый компьютер было установлено программное обеспечение стоимостью 300 у.е. на один компьютер. Для обеспечения доступа всего отдела к локальной сети организации дополнительно потрачено 1000 у.е. на закупку сетевого оборудования. Вероятность сетевого вторжения составляет 40 % для данного региона. Среднее количество сетевых вторжений в данном регионе составляет 3 раза в год. На обеспечение защиты компьютерной сети отдела планируется выделить 800 у.е.

Вариант 2. Совокупная стоимость активов организации составляет 35 000 у.е. В организации есть база данных (БД) заказчиков, которая содержит ценную информацию. Стоимость аналогичной БД на рынке составляет 5000 у.е. Но если данная БД будет украдена и произойдет публичная продажа, что весьма вероятно, то в этом случае ее стоимость снизится до 100 у.е. Вероятность кражи БД составляет 30 %. Для обеспечения защиты БД было затрачено 1000 у.е.

Вариант 3. В организации купили новые серверы для того, чтобы обеспечить доступ в Интернет. В организации работают 300 сотрудников, трудозатраты каждого из них в среднем равны 30 у.е./ч. После реализации сетевого вторжения на восстановление системы в среднем необходимо потратить 5 часов. В организации есть БД заказчиков, которая содержит ценную информацию. Стоимость аналогичной БД на рынке составляет 3000 у.е. Но если данная БД будет украдена и произойдет публичная продажа, что весьма вероятно, то в этом случае стоимость снизится до 100 у.е. Вероятность кражи БД составляет 20 %. Среднее количество краж в данном регионе составляет 2 раза в год. Организация решила закупить антивирусное программное обеспечение на общую сумму 2000 у.е. для защиты всех серверов и компьютеров.

Вариант 4. В организации купили беспроводные маршрутизаторы для организации беспроводного доступа к локальной сети. В связи с этим часть организации перешла на беспроводную связь. В организации работают 100 сотрудников, трудозатраты каждого из них в среднем равны 30 у.е./ч. Изменения в ИС приводят к повышению вероятности реализации вирусной угрозы на 20 %, а на полное восстановление ИС в случае заражения в среднем необходимо потратить 3 часа. Организация решила закупить антивирусное программное обеспечение для защиты серверов и компьютеров на сумму 1000 у.е.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса. Системы документооборота и средства защиты циркулирующей в них информации.

Определение и природа угроз информации в современных системах ее обработки.

Классификация и общая характеристика основных угроз. Понятие уязвимости информации. Подходы к определению значений показателей уязвимости. Эмпирические методы определения значений показателей уязвимости. Примеры эмпирических моделей. Способы определения параметров моделей. Особенности использования моделей. Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей. Примеры моделей. Особенности и проблемы практического использования.

Теоретико-эмпирические методы определения значений показателей. Подходы к построению теоретико-эмпирических моделей. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения. Методы и модели прогнозирования значений показателей уязвимости. Определение, значение, структура и способы формирования инструментальных средств оценки уязвимости информации.

Место анализа рисков в общей схеме управления ИБ. Подходы к оценке рисков ИБ: качественный, количественный. Экономическая модель оценки рисков. Вероятностная модель оценки рисков Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. ГОСТ Р ИСО 31010. Методы оценки риска Нормативно-правовые основы оценки рисков. ГОСТ Р ИСО 27005. Менеджмент рисков ИБ. Стандарт банка России по обеспечению ИБ организаций банковской системы РФ Методики и ПО для оценки рисков ИБ. Оценка критичных угроз, активов и уязвимостей OSTATE. Средство качественной оценки vsRisk. Методики и ПО для оценки рисков ИБ. Метод анализа и управления рисками CRAMM. Средство оценки рисков Microsoft Security Assessment Tools. Методики и ПО для оценки рисков ИБ. Средство количественной оценки рисков PracticalThreatAnalysis. Методика Risk Watch Методики и ПО для оценки рисков ИБ. Методика управления рисками Microsoft The Security Risk Management Guide. Средство оценки рисков R-Vision Risk Manager Принятие решений по результатам оценки рисков. Политика обработки рисков.

Защита автоматизированных систем от удаленных атак через сеть Internet. Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты. Защита информации от несанкционированного доступа (НСД). Каналы утечки информации. Защита компонентов автомати-

зированных систем от НСД. Антивирусная защита. Системы анализа защищённости и обнаружения вторжений. Модель и источники каналов утечки информации. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; компьютерные вирусы как особый класс разрушающих программных воздействий; защита от разрушающих программных воздействий; понятие изолированной программной среды.

Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации.

Парольные системы опознавания, их сущность, содержание, достоинства и недостатки. Способы повышения надежности парольных систем. Другие системы опознавания. Средства опознавания аппаратуры, программ, массивов данных.

Методы идентификации и проверки подлинности пользователей автоматизированных систем. Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных. Биометрическая идентификация и аутентификация пользователей: основные понятия и механизмы. «Fuzzy extractors». Искусственные нейронные сети в преобразователях биометрия-код. Алгоритм быстрого обучения искусственной нейронной сети. Алгоритм ускоренного тестирования нейросетевого преобразователя биометрия-код (НПБК).

Алгоритм полного тестирования НПБК. Базы биометрических образов: назначение, виды, требования к формированию. Нейросетевой биометрический контейнер (НБК): назначение, виды. Наиболее вероятные атаки на НБК, защита от них.

Программные средства разграничения доступа, их сущность, достоинства и недостатки. Модели разграничения доступа. Разграничение доступа по уровням и кольцам секретности, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения.

Примеры систем разграничения доступа. Другие программные средства защиты: регистрации, сигнализации, реагирования и т.п. Программы защиты ЭВМ от электронных вирусов.

Способы организации и использования программных средств защиты.

Организационно-правовые средства защиты, их сущность, возможности, достоинства и недостатки. Критерии классификации организационно-правовых средств, классификационная структура и общая характеристика.

Система законов, регламентирующих защиту информации в РФ. Перечень основных законов, основное их содержание и порядок действия. Руководящие методические материалы (РММ) по защите информации. Назначение и состав необходимых РММ. Перечень и содержание имеющихся РММ.

Организационные мероприятия по защите информации, их сущность и назначение. Системная классификация организационных мероприятий.

Мероприятия, проводимые на различных этапах жизненного цикла систем обработки данных.

<i>практическая подготовка обучающихся</i>	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Теория и методология обеспечения информационной безопасности и защиты информации	ОПК-1, ОПК-3, ПК -2, ПК-3, ПК-6	Тест, защита практических работ
2	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.	ОПК-1, ОПК-3, ПК -2, ПК-3, ПК-6	Тест, защита практических работ
3	Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.	ОПК-1, ОПК-3, ПК -2, ПК-3, ПК-6	Тест, защита практических работ
4	Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.	ОПК-1, ОПК-3, ПК -2, ПК-3, ПК-6	Тест, защита практических работ
5	Модели и методы управления информационной безопасностью	ОПК-1, ОПК-3, ПК -2, ПК-3, ПК-6	Тест, защита практических работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496741>

2. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. А. Гатчин, В. В. Сухостат, А. С. Куракин, Ю. В. Донецкая. — 2-е изд., испр. и доп. — Санкт-Петербург : НИУ ИТМО, 2018. — 100 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/136476>

3. Конспект лекций по курсу Математические основы защиты информации и информационной безопасности : учебное пособие / составители Б. Н. Воронков, Ю. А. Крыжановская. — Воронеж : ВГУ, 2017. — 77 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book>

4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/489745>

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/491249>

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профес-

сиональных баз данных и информационных справочных систем:

Шаблоны типовых документов по информационной безопасности

<http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B>

Государственный реестр сертифицированных средств защиты информации

<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>

Банк данных угроз безопасности информации

<https://bdu.fstec.ru/vul>

Международные, национальные (государственные) и отраслевые стандарты в области информационной безопасности (защиты информации), а также информационных технологий и непрерывности бизнеса

<http://www.iso27000.ru/>

Управление рисками ИБ

<https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-1-osnovnye-ponyatiya-i-metodologiya-otsenki-ri/>

Электронная образовательная система ВГТУ

<https://old.education.cchgeu.ru/>

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аудитория для проведения занятий лекционного и практического типа: аудитория, оснащенная набором демонстрационного оборудования (экран, компьютер, проектор) и оборудованная специализированной учебной мебелью

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Методы и системы защиты информации, информационная безопасность» читаются лекции.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Вид учебных занятий	Деятельность студента
Лекция	<p>Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.</p>
Самостоятельная работа	<p>Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:</p> <ul style="list-style-type: none"> - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	<p>Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.</p>

