МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ЭМИТ

_____/С.А. Баркалов/

31 августа 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки 27.03.03 Системный анализ и управление

Профиль Разработка систем интеллектуального управления

Квалификация выпускника бакалавр

Нормативный период обучения 4 года

Форма обучения очная

Год начала подготовки 2022

Автор программы _____ К.В.Славнов

Заведующий кафедрой
Базовая кафедра
кибернетики в системах
организационного
управления _____ В.Е.Белоусов

Руководитель ОПОП _____ Т.Г.Лихачева

Воронеж 2022

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины:

- изучение основ информационной безопасности автоматизированных информационных систем,
- изучение правовых, организационных, технических и инженерных методов обеспечения информационной безопасности.

1.**2. Задачи освоения дисциплины:**

- изучение способов и методов обеспечения информационной безопасности Российской Федерации и её информационной инфраструктуры;
- изучение основ построения, функционирования и настройки программно-аппаратных средств защиты информации от несанкционированного доступа;
- формирование навыков оценки защищенности и обеспечения информационной безопасности компьютерных систем;
- формирование навыков классифицирования автоматизированных информационных систем в соответствии с требованиями обеспечения информационной безопасности;
- формирование навыков выбирать, комплексировать и эксплуатировать программно-аппаратные средства защиты в создаваемых вычислительных и информационных системах и сетевых структурах;
- овладение навыками разработки основных организационно - распорядительных документов и технической документации на систему защиты автоматизированной информационной системы;
- овладение навыками настройки средств защиты информации от несанкционированного доступа.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

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

ОПК-4 - Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-3	Знать: - Методы и средства обеспечения информационной безопасности компьютерных систем
	Уметь: - классифицировать автоматизированные информационные системы в соответствии с требованиями обеспечения информационной безопасности; - выбирать, комплексировать и эксплуатировать программно-аппаратные средства в создаваемых вычислительных и информационных системах и сетевых структурах.
	Владеть: - языками процедурного и объектно-ориентированного программирования, - навыками настройки средств защиты информации от несанкционированного доступа.
ОПК-4	Знать: - требования Федеральных законов, ГОСТ, руководящих документов ФСБ, ФСТЭК по разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью в области информационной безопасности.
	Уметь: - ставить задачу и разрабатывать алгоритм ее решения в области информационной безопасности автоматизированных информационных систем.
	Владеть: - навыками разработки основных организационно - распорядительных документов и технической документации на систему защиты автоматизированной информационной системы.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	108	108
В том числе:		

Лекции	36	36
Практические занятия (ПЗ)	72	72
Самостоятельная работа	45	45
Часы на контроль	27	27
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

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	Прак зан.	СРС	Всего, час
1	Информационная безопасность в системе национальной безопасности Российской Федерации	Основные термины и определения. Классификация защищаемой информации . Основные задачи обеспечения информационной безопасности в Российской Федерации. Основные положения документов «О стратегии национальной безопасности Российской федерации» и «Доктрина информационной безопасности Российской Федерации». Основные составляющие национальных интересов Российской Федерации в информационной сфере. Основные направления федерального законодательства в области защиты информации ограниченного доступа.	6	12	6	24
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	Стандарты по оценке защищенных систем. Критерии безопасности компьютерных систем. Европейские «Критерии безопасности информационных технологий». Федеральные критерии безопасности информационных технологий. Канадские критерии безопасности компьютерных систем. Обзор серии стандартов ISO/IEC 17799. Стандарты ISO/IEC 17799:2002 (BS 7799:2000). Стандарт ISO/IEC 27001. Российский стандарт ГОСТ Р ИСО/МЭК 27001-2006. Стандарты ISO/IEC 15408 и ГОСТ Р ИСО/МЭК 15408. Российская классификация средств вычислительной техники и автоматизированных систем и требования по защите информации согласно РД ФСТЭК	6	12	8	26
3	Основные угрозы информационной безопасности автоматизированных систем	Анализ и классификация угроз информационной безопасности автоматизированных информационных систем. Причины, виды, каналы утечки и искажения информации. Угрозы программно-математических воздействий и нетрадиционных	6	12	8	26

		информационных каналов. Угрозы, основанные на информационных сетевых атаках				
4	Абстрактные модели обеспечения информационной безопасности	Ранние модели управления доступом. Модель матрицы доступов Харрисона – Руззо – Ульмана. Модель Белла и Лападула. Модель систем военных сообщений. Понятие контроля доступа, базирующегося на ролях	6	12	8	26
5	Основы построения систем защиты информации	Основные принципы обеспечения информационной безопасности предприятий. Основные методы и средства защиты информации. Порядок построения защищенной автоматизированной системы Аттестация объектов информатизации о требованиям безопасности информации	6	12	8	26
6	Основы обеспечения информационной безопасности в автоматизированных системах управления	Правовые основы защиты информации. Обеспечение защиты информации в ходе эксплуатации аттестованных информационных систем.. Режимы защиты информации. Классификация и экспертиза компьютерных преступлений.	6	12	7	25
		Итого	**36**	**72**	**45**	**153**

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».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-3	Знать : - Методы и средства обеспечения информационной безопасности компьютерных систем;	Выполнение 100% работ в срок, предусмотренный в рабочих программах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - классифицировать автоматизированные	Выполнение 100% работ в срок, предусмотренный в	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренный в

	информационные системы в соответствии с требованиями обеспечения информационной безопасности; - выбирать, комплексировать и эксплуатировать программно-аппаратные средства в создаваемых вычислительных и информационных системах и сетевых структурах.	рабочих программах	рабочих программах	рабочих программах
	Владеть: - языками процедурного и объектно-ориентированного программирования, - навыками настройки средств защиты информации от несанкционированного доступа.	Выполнение работ в срок, предусмотренный в рабочих программах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-4	Знать: - требования Федеральных законов, ГОСТ, руководящих документов ФСБ, ФСТЭК по разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью в области информационной безопасности.	Выполнение 100% работ в срок, предусмотренный в рабочих программах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: - ставить задачу и разрабатывать алгоритм ее решения в области информационной безопасности автоматизированных информационных систем.	Выполнение 100% работ в срок, предусмотренный в рабочих программах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: - навыками разработки основных организационно - распорядительных документов и технической документации на систему защиты автоматизированной	Выполнение 100% работ в срок, предусмотренный в рабочих программах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	информационной системы.				

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-3	Знать : - Методы и средства обеспечения информационной безопасности компьютерных систем;	Ответы на вопросы	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой,усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании,изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.
	Уметь: - классифици-ровать автоматизированные информационные системы в соответствии с	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	требованиями обеспечения информационной безопасности; - выбирать, комплексировать и эксплуатировать программно-аппаратные средства в создаваемых вычислительных и информационных системах и сетевых структурах.			задачах		
	Владеть: - языками процедурного и объектно-ориентированного программирования, - навыками настройки средств защиты информации от несанкционированного доступа.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-4	Знать: - требования Федеральных законов, ГОСТ, руководящих документов ФСБ, ФСТЭК по разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью в области информационной безопасности.	Ответы на вопросы	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой,усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании,изложении и	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под	Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

			использовании учебно-программного материала.		руководством преподавателя.	
	Уметь: - ставить задачу и разрабатывать алгоритм ее решения в области информационной безопасности автоматизированных информационных систем.	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: - навыками разработки основных организационно - распорядительных документов и технической документации на систему защиты автоматизированной информационной системы.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	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

(минимум 10 вопросов для тестирования с вариантами ответов)

1. Что в сфере информационной безопасности принято считать риском?

а) потенциальную возможность понести убытки из-за нарушения безопасности информационной системы

б) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней

в) характеристику, которая делает возможным возникновение угрозы

2. Что принято считать ресурсом или активом информационной системы?

а) модель информационной системы

б) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет

в) именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите

3. На какие ресурсы может быть направлена угроза?

а) только на информационные

ресурсы б) только на

аппаратные ресурсы

в) на любые виды ресурсов (информационный, аппаратный, программный и т.д.)

4. Какой термин определяет характеристику функции безопасности объекта оценки, выражающую минимальные усилия, которых теоретически может быть достаточно для нарушения работоспособности при прямой атаке на информационную систему?

а) "потенциал падения"

б) "стойкость функции
безопасности (СФБ)" в)
"резистивность системы" (РС)

4. Что определяет ресурсы или активы ИС?

а) модель ИС

б) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет

в) именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите

5. Каковы цели анализа и тестирования прикладных систем в аспектах информационной безопасности?

а) оперативное внесение изменений в операционные
системы б) обеспечение целостности программного
обеспечения
в) обеспечение более эффективного использования готовых пакетов программ

6. Какие из перечисленных рекомендаций уместны в случае, когда для проведения работ по разработке программного обеспечения привлекается сторонняя организация?

а) необходимо предусмотреть антифильтрационные меры
б) необходимо предусмотреть меры по контролю правильности
выполненных работ в) необходимо предусмотреть меры по контролю
качества выполненных работ

7. Какой из перечисленных вариантов последовательности действий предписан стандартом ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью" в аспектах управления непрерывностью бизнеса?

а) идентифицировать события, которые могут быть причиной прерывания бизнес-процессов, провести оценку последствий, после чего разработать планы восстановления

б) произвести экспертную оценку контента информации на сервере на предмет возможных схем утечки критически важной информации, после чего разработать планы восстановления системы

в) произвести контроль плана восстановления и его тестирование на предмет реализуемости, затем идентифицировать события, которые могут быть причиной прерывания бизнес-процессов (отказ оборудования, пожар и т.п.)

8. Чем характеризуются угрозы?

а) нежелательностью их
появления б)
невероятностью их
появления
в) вероятностью их появления

9. Способствуют контрмеры в аспектах достижения информационной безопасности эффективному снижению уязвимостей?

а) да
б) нет
в) лишь отчасти

10. Какова связь анализа рисков с другими компонентами модели информационной безопасности?

а) на базе полученных результатов по оценке рисков осуществляется анализ состояния системы и разрабатывается план построения системы защиты сети

б) анализ рисков увязан с процедурами
анализа рисков

в) анализ не увязывается с другими компонентами

системы

7.2.2 Примерный перечень заданий для решения стандартных задач

Практические Вопросы

I.Определить возможно ли использовать:

1. СВТ 6 класса для построения АС класса 1Д.(Может)
2. СВТ 5 класса для построения АС класса 1Д. (Может)
3. СВТ 4 класса для построения АС класса 1Г. (Не Может)
4. СВТ 5 класса для построения АС класса 3Б. (Может)
5. СВТ 4 класса для построения АС класса 2Б. .(Может)
6. СВТ 3 класса для построения АС класса 1В.(Может)

II.Классифицировать:

АС согласно РД АС. Классификация автоматизированных систем.

1. АС, один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Высший гриф конфиденциальной информации «Для служебного пользования».(3Б)
2. АС, один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Высший гриф конфиденциальной информации «Коммерческая тайна».(3Б)
3. АС, один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Высший гриф конфиденциальной информации «Банковская тайна».(3Б)
4. АРМ, много пользователей, пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Высший гриф конфиденциальной информации «Для служебного пользования».(2Б)
5. АРМ, много пользователей, пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Высший гриф конфиденциальной информации «Коммерческая тайна».(2Б)
6. АРМ, много пользователей, пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Высший гриф конфиденциальной информации «Банковская тайна».(2Б)
7. Многопользовательская АС, в которой одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко

всей информации АС. Высший гриф конфиденциальной информации «Банковская тайна».(1Г)

8. Многопользовательская АС, в которой одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Высший гриф конфиденциальной информации «Для служебного пользования».(1Г)
9. Многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Высший гриф конфиденциальной информации «Коммерческая тайна».(1Д)

7.2.3 Примерный перечень заданий для решения прикладных задач
(минимум 10 вопросов для тестирования с вариантами ответов)

III.Определить класс защищенности ГИС:

1. Информационная система функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях. Степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и является высокой, так как в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) и возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;(К1)
2. Информационная система функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях. Степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и является высокой, так как в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;(К1)
3. Информационная система функционирует на объектах одного федерального органа государственной власти, органа

государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях. Степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и является низкой, так как в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.(К3)

IV. Определить уровень защищенности ИСПДн:

1. В информационной системы установлена несертифицированная ОС Windows 10, сертифицированные прикладные программные продукты для офиса, информационная система обрабатывает специальные категории персональных данных. (1 Уровень защищенности)
2. В информационной системы установлена сертифицированная ОС Астра Linux, несертифицированные прикладные программные продукты для офиса, ИС обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. (1 Уровень защищенности)
3. В информационной системы установлена несертифицированная ОС Windows 10, информационная система обрабатывает общедоступные персональные данные. (2 Уровень защищенности)
4. В информационной системы установлена сертифицированная ОС Астра Linux, несертифицированные прикладные программные продукты для офиса, информационная система обрабатывает специальные категории персональных данных сотрудников оператора. (2 Уровень защищенности)
5. В информационной системы установлена сертифицированная ОС Астра Linux, несертифицированные прикладные программные продукты для офиса, информационная система специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. (2 Уровень защищенности)
6. В информационной системы установлена сертифицированная ОС

Астра Linux, несертифицированные прикладные программные продукты для офиса, информационная система обрабатывает биометрические персональные данные. (2 Уровень защищенности)

7. В информационной системы установлена сертифицированная ОС Астра Linux, несертифицированные прикладные программные продукты для офиса, информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. (2 Уровень защищенности)
8. В информационной системы установлена сертифицированная ОС Астра Linux, несертифицированные прикладные программные продукты для офиса, информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. (2 Уровень защищенности)
9. В информационной системы установлена сертифицированная ОС Астра Linux, сертифицированные прикладные программные продукты для офиса, используется несертифицированное специальное программное обеспечение по учету кадров, информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. (2 Уровень защищенности)
10. В информационной системы установлена сертифицированная ОС Астра Linux, сертифицированные прикладные программные продукты для офиса, используется несертифицированное специальное программное обеспечение по учету кадров, информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. (3 Уровень защищенности)

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1. Каким образом десять неформальных свойств модели СВС реализуются в ее формальном описании?
2. В каком случае система (T, S_0) безопасна?
3. Где в определениях безопасности модели СВС реализовано ss-свойство безопасности классической модели Белла-ЛаПадулы?
4. Где в определениях безопасности модели СВС реализовано *-свойство безопасности классической модели Белла-ЛаПадулы?
5. Где в определениях безопасности модели СВС реализовано ds-свойство безопасности классической модели Белла-ЛаПадулы?

6. Каким стандартам необходимо следовать при построении СУИБ?

7. Что регламентируется в стандарте ISO 27002?

8. Что регламентируется в стандарте ISO 18044?

9. Что должна обеспечивать СУИБ?

10. Какова главная задача СУИБ?

11. Какой вид политики управления доступом используется в качестве основы автоматной модели безопасности информационных потоков?

12. В каких случаях в КС с мандатным управлением доступом нецелесообразно предотвращение возможности реализации всех информационных потоков от устройств ввода пользователей с высоким уровнем доступа к устройствам вывода пользователей с низким уровнем доступа?

13. В чем отличие информационной невыводимости от информационного невлияния?

14. Почему использование определения требований информационного невлияния (с учетом времени) позволяет обеспечить возможность функционирования в КС монитора ссылок?

15. В каких случаях может являться эффективным моделирование безопасности информационных потов с использованием вероятностных подходов?

16. Что понимается под термином информационная безопасность?

17. Что понимается под термином доступность информации?

18. Что понимается под термином целостность информации?

19. Что понимается под термином конфиденциальность информации?

20. Что понимается под термином комплекс средств автоматизации обработки информации?

21. Что понимается под термином информационная безопасность ИС?

22. Что понимается под термином уничтожение информации?

23. Какие способы защиты от вирусов Вы знаете?

24. Какие способы защиты от несанкционированного доступа Вы можете привести?

25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28. Назначение, виды, структура и технология функционирования системы защиты информации.

29. Аналитическая работа по выявлению каналов утечки информации фирмы.

30. Направления и методы защиты профессиональной тайны.

31. Направления и методы защиты служебной тайны.

32. Направления и методы защиты персональных данных о гражданах.

33. Методы защиты личной и семейной тайны.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по билетам, каждый из которых содержит 2 вопроса и задачу.

Каждый правильный ответ на вопрос в оценивается 3 баллом, задача оценивается в 3 балла (3 балла верное решение и 3 баллов за верный ответ, 1 балл за неправильное решение или неправильный ответ). Максимальное количество набранных баллов – 9.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 4 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал 5 баллов.

3. Оценка «Хорошо» ставится в случае, если студент набрал 7 баллов.

4. Оценка «Отлично» ставится, если студент набрал 9 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Информационная безопасность в системе национальной безопасности Российской Федерации	ОПК-3, ОПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем	ОПК-3, ОПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Основные угрозы информационной безопасности автоматизированных систем	ОПК-3, ОПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Абстрактные модели обеспечения информационной безопасности	ОПК-3, ОПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Основы построения систем защиты информации	ОПК-3, ОПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Основы обеспечения информационной безопасности в автоматизированных информационных системах	ОПК-3, ОПК-4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

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

Экзамен осуществляется в классическом варианте. Обучаемый выбирает билет и готовится к ответу в течении 30 мин. Затем осуществляется проверка ответа экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется с использованием выданных задач на бумажном носителе. Время решения задач 10 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется с использованием выданных задач на бумажном носителе. Время решения задач 10 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. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. Пособие для студ. высш. учеб. заведений/ Петр Николаевич Девянин.-М.: Издательский центр «Академия»,2005-144 с. ISBN 5-7695-2053-1.

2. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.:Горячая линия-Телеком, 2006. – 536с.: ил. ISBN 5-93517-291-1.

3. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Том 2 – Средства защиты в сетях. – М.:Горячая линия-Телеком, 2008. – 558с.: ил. ISBN 978-5-9912-0034-9.

4. Белов Е.Б. Основы информационной безопасности: Учеб. Пособие для вузов / Е.Б.Белов, В.П. Лось, Р.В.Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком,, 2006. – 544с.

5. Галатенко В.А. Стандарты информационной безопасности : курс лекций: учебное пособие / Второе издание. –М.:ИНТУИТ.РУ «Интернет-университет Информационных технологий» , 2006. 264 с. ISBN 5-9556-0053-1

6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф.-М.: ДМК Пресс,2008.-544 с.: ил.

7. Торокин А.А. Инженерно-техническая защита информации: учеб.пособие для студентов, обучающихся по специальностям в обл. информ. Безопасности / А.А.Торокин. –М.: Гелиос АРВ, 2005.-960 с.

8. А.В. Волков, Д.В. Игнатов, А.Ю. Кузьмин, С.А. Панов, Е.В.Сидельников, К.В. Славнов, А.В. Шабанов \\ Основы информационной безопасности: Учебное пособие. – Воронеж: издательство РИТМ, 2022. –334 с., ил.

9. Д.В. Игнатов, Р.С. Ковальчук, Н.В. Паршин, К.В. Славнов, А.Н.Темченко. Техническая защита информации ограниченного доступа./Учебное пособие. Воронеж: ООО «Издательство РИТМ», 2021.-418с.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

1. Пакет офисных программ MS Office.
2. Windows media player.
3. Специализированное пргшграммное обеспечечния системного администратора на - Hiren Boot CD.
3. Программа поиска остаточной информации на дисках *Terrier v.3.0.*
4. Средство создания модели системы
разграничения доступа «Ревизор 1 XP»
5. Программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»
6. Программа фиксации и контроля исходного сосотояния программного комплекса «ФИКС» (версия 2.0.2)
7. Сканер безопасности Xspider v 7.5.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Персональные компьютеры.

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

По дисциплине «Информационная безопасность» читаются лекции, проводятся практические занятия.

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

Практические занятия направлены на приобретение практических навыков расчета _____. Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать 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 удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - 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	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 экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП