МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института энергетики, информационных технологий и управляющих систем
_____ Белоусов А.В.
«20» _____ 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: к.т.н. _____ _____ (Гвоздевский И.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

« 14 » 05 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем
(наименование кафедры/кафедр)

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

« 14 » 05 2021 г.

Рабочая программа одобрена методической комиссией института

« 20 » 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____ (Семернин А.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Общепрофессиональные компетенции	ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем.	ОПК-11.1. Анализирует и оценивает исходные данные для создания системы защиты автоматизированных систем.	**Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. **Уметь:** классифицировать и оценивать угрозы безопасности информации для объекта информатизации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей в автоматизированной системе. **Владеть:** навыками проведения анализа и оценки целесообразности создания системы защиты информации автоматизированных систем.
		ОПК-11.2. Проектирует компоненты систем защиты информации автоматизированных систем.	**Знать:** принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем, основные характеристики технических средств защиты информации от утечек по техническим каналам, принципы формирования политики информационной безопасности в автоматизированных системах. **Уметь:** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, выбирать меры защиты информации, подлежащие реализации. **Владеть:** навыками разработки модели угроз и модели нарушителя, проектов нормативных документов, регламентирующих работу по защите информации в автоматизированной системе.
		ОПК-11.3. Реализует и тестирует компоненты систем защиты информации автоматизированных систем	**Знать:** принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения, криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, методы тестирования и отладки программного и аппаратного обеспечения. **Уметь:** анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах, проводить комплексное тестирование аппаратных и программных средств. **Владеть:** навыками разработки программного обеспечения, технических средств, баз

			данных и компьютерных сетей с учетом требований по обеспечению защиты информации.
	ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ОПК-5.2.1. Разрабатывает системы защиты информации открытых информационных систем	**Знать:** эталонную модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей, особенности защиты информации в автоматизированных системах. **Уметь:** анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных система, разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПД. **Владеть:** навыками синтеза структурных и функциональных схем защищенных автоматизированных систем, разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.
		ОПК-5.2.2. Эксплуатирует системы защиты информации открытых информационных систем	**Знать:** базовую конфигурацию системы защиты информации автоматизированной системы, особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах, типовые средства, методы и протоколы идентификации, аутентификации и авторизации, средства и методы защиты информации в локальных и глобальных вычислительных сетях. **Уметь:** обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации, использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи, конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией. **Владеть:** навыками контроля соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации и стабильности характеристик системы защиты информации автоматизированной системы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем.

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Разработка и эксплуатация автоматизированных систем в защищенном исполнении
2.	Разработка веб-приложений.
3.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

2. Компетенция ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Разработка и эксплуатация автоматизированных систем в защищенном исполнении
2.	Методы проектирования защищенных открытых информационных систем
3.	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единиц, 144 часов.

Форма промежуточной аттестации: экзамен.

Вид учебной работы	Всего часов	Семестр № 8
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т. ч.:	73	73
лекции	34	34
лабораторные	17	17
практические	17	17
групповые консультации в период теоретического обучения и промежуточной аттестации	5	5
контроль самостоятельной работы	-	-
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	71	71
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	35	35
Экзамен	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем

Курс 4 Семестр №8

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.	Основы разработки автоматизированных систем в защищенном исполнении.				
	Понятие автоматизированной системы и автоматизированной системы в защищенном исполнении. Требования к АСЗИ. Классификация защищенности АСЗИ. Алгоритм создания АСЗИ.	8	4	4	14
2.	Основы разработки систем защиты информации.				
	Понятие системы защиты информации и ее компонентов. Классификация СЗИ и ее компонентов. Требования к созданию СЗИ. Формирование технического задания на создание СЗИ.	8	4	4	18
3.	Организационные меры защиты информации на основе менеджмента инцидентов.				
	Понятие организационных мер защиты информации и политики ИБ. Понятие конфиденциальности и тайны, их роль и свойства в рамках АСЗИ. Основные виды организационных мер защиты информации. Понятие управления инцидентами ИБ.	8	4	4	18
4.	Эксплуатация автоматизированных систем в защищенном исполнении.				
	Основные этапы эксплуатации АСЗИ. Конфигурирование компонентов системы защиты информации. Процесс управления инцидентами ИБ и основные обязанности группы реагирования на инциденты ИБ.	10	5	5	21
	ВСЕГО	34	17	17	35

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 8				
1	Основы разработки автоматизированных систем в защищенном исполнении.	Понятие автоматизированной системы и автоматизированной системы в защищенном исполнении. Требования к АСЗИ.	4	4
2	Основы разработки систем защиты информации.	Создание программного компонента системы защиты информации.	4	4

3	Организационные меры защиты информации на основе менеджмента инцидентов.	Формирование документации для организации управления инцидентами.	4	4
4	Эксплуатация автоматизированных систем в защищенном исполнении.	Эксплуатация комплексной системы защиты информации Dallas Lock.	5	4
		ИТОГО:	17	16
			ВСЕГО:	33

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр № 8				
1	Основы разработки автоматизированных систем в защищенном исполнении.	Составление требований к системе защиты информации и автоматизированной системе в защищенном исполнении.	4	4
2	Основы разработки систем защиты информации.	Создание программного компонента системы защиты информации.	4	4
3	Организационные меры защиты информации на основе менеджмента инцидентов.	Формирование документации для организации управления инцидентами.	4	4
4	Эксплуатация автоматизированных систем в защищенном исполнении.	Эксплуатация комплексной системы защиты информации Dallas Lock.	5	4
		ИТОГО:	17	16
			ВСЕГО:	33

4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Не предусмотрено учебным планом

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1. Компетенция ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем.

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-11.1. Анализирует и оценивает исходные данные для создания системы защиты автоматизированных систем.	выполнение лабораторной работы, устный опрос, экзамен
ОПК-11.2. Проектирует компоненты систем защиты информации автоматизированных систем.	выполнение лабораторной работы, устный опрос, экзамен
ОПК-11.3. Реализует и тестирует компоненты систем защиты информации автоматизированных систем.	выполнение лабораторной работы, устный опрос, экзамен

2. Компетенция ОПК-5.2. Способность разрабатывать и эксплуатировать системы защиты информации открытых информационных систем

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-5.2.1. Разрабатывает системы защиты информации открытых информационных систем	выполнение лабораторной работы, устный опрос, экзамен
ОПК-5.2.2. Эксплуатирует системы защиты информации открытых информационных систем	выполнение лабораторной работы, экзамен

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Основы разработки автоматизированных систем в защищенном исполнении. ОПК-11.1.	1. Автоматизированные систем, их классификация и назначение. 2. Автоматизированные системы, как предмет защиты. 3. Требования к автоматизированным системам в защищенном исполнении. 4. Алгоритм создания автоматизированной системы в защищенном исполнении. 5. Процесс предварительных испытаний и аттестации автоматизированной системы в защищенном исполнении. 6. Классификация защищенности автоматизированных систем в защищенном исполнении. 7. Требования к автоматизированным системам в защищенном исполнении в рамках информационных систем персональных данных.
2.	Основы разработки систем защиты информации. ОПК-11.1, ОПК-11.2, ОПК-5.2.1.	1. Система защиты информации. Требования к созданию системы защиты информации. 2. Алгоритм разработки системы защиты информации. 3. Классификация систем защиты информации. 4. Критическая информационная инфраструктура. Требования к системам защиты информации, объектов, входящих в КИИ.
3.	Организационные меры защиты информации на основе менеджмента инцидентов. ОПК-11.2.	1. Инцидент и событие ИБ. Процесс управления инцидентами ИБ. Группа реагирования на инциденты ИБ. 2. Меры защиты от атак социальной инженерии в АСЗИ. 3. Организационные меры защиты информации, их виды и специфика применения в рамках автоматизированных систем в защищенном исполнении. 4. Политика безопасности, ее назначение в рамках автоматизированных систем в защищенном исполнении.
4.	Эксплуатация автоматизированных систем в защищенном исполнении. ОПК-11.3, ОПК-5.2.2.	1. Применение политики безопасности в рамках автоматизированных систем в защищенном исполнении. 2. Персональные данные. Процесс обработки персональных данных. 3. Конфиденциальность и тайна, их назначение и свойства в рамках автоматизированных систем в защищенном исполнении. 4. SIEM, DLP и IRP системы, их назначение и применение в рамках автоматизированной системы в защищенном исполнении.

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Текущий контроль осуществляется в течение семестра в форме лабораторных работ.

Лабораторные работы направлены на проверку степени усвоения материала, понимания теоретических сведений и получение практических навыков, используемых в процессе выполнения работы. Примерные перечень вопросов для контроля знаний приведен в таблице:

Тема лабораторной работы	Контрольные вопросы
Составление требований к системе защиты информации и автоматизированной системе в защищенном исполнении.	1. Какие типы требований предъявляются к системам защиты информации и автоматизированным системам в защищенном исполнении? 2. Какую информацию должно содержать описание системы защиты информации и автоматизированной системе в защищенном исполнении? 3. Что является обоснованием для предъявляемых требований к системе защиты информации?
Создание программного компонента системы защиты информации.	1. Какие компоненты может содержать система защиты информации? 2. Защиту от каких типов атак предоставляют программные компоненты системы защиты информации? 3. Каким образом производится сертификация программных компонентов системы защиты информации?
Формирование документации для организации управления инцидентами.	1. В чем заключаются основные положения управления инцидентами информационной безопасности? 2. В чем заключается различие инцидента и события информационной безопасности: 3. Какие задачи выполняет группа реагирования на инциденты информационной безопасности? 4. Из каких этапов состоит процесс управления инцидентами информационной безопасности?
Эксплуатация комплексной системы защиты информации Dallas Lock.	1. Какие этапы содержит эксплуатация системы защиты информации? 2. Какие компоненты содержит система защиты информации Dallas Lock? 3. Каким стандартам удовлетворяет система защиты информации Dallas Lock K? 4. Какие компоненты системы защиты информации Dallas Lock могут быть сконфигурированы на усмотрение администратора? 5. Уязвимостью к каким типам атак обладает система защиты информации Dallas Lock?

Тестовые задания

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Основы разработки автоматизированных систем в защищенном исполнении.	**Задание 1** Автоматизированная система – это *Выберите один из 4 вариантов ответа:* 1) система, выполняющая действия, согласно своему назначению, автоматически; 2) система, состоящая из средств автоматизации ее деятельности; 3) система, состоящая из персонала, комплекса средств автоматизации его деятельности; 4) система, состоящая из персонала, с полной автономией деятельности. **Задание 2** Основными этапами создания АС являются: *Выберите несколько из 4 вариантов ответа:* 1) формирование требований; 2) создание технического задания; 3) создание технического проекта; 4) сопровождение АС. **Задание 3** Требованием к АСЗИ не является: *Выберите один из 4 вариантов ответа:* 1) комплексность; 2) расширяемость; 3) не препятствие нормальному функционированию системы; 4) нормальность. **Задание 4** Аттестацию АСЗИ на соответствие требованиям безопасности информации: *Выберите один из 4 вариантов ответа:* 1) организует и проводит организация, реализующая АСЗИ; 2) организует и проводит заказчик; 3) организует заказчик, а проводит организация, реализующая АСЗИ; 4) организует заказчик, а проводит аттестованная организация. **Задание 5** Следующие типы АСЗИ подлежат аттестации: *Выберите один из 4 вариантов ответа:* 1) автоматизированные системы конфиденциальной информации; 2) государственные информационные системы; 3) информационные системы общего пользования; 4) системы критической информационной инфраструктуры. **Задание 6** Исходными данными, необходимые для классификации конкретной АС являются: *Выберите один из 4 вариантов ответа:* 1) режим обработки данных в АС; 2) перечень лиц, имеющих доступ к штатным средствам, АС, с указанием их уровня полномочий; 3) перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности; 4) модель угроз. **Задание 7** Сколько существует классов защищенности и групп АС?

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		Выберите один из 4 вариантов ответа: 1) 7 классов, 3 группы; 2) 5 классов, 2 группы; 3) 9 классов, 3 группы; 4) 6 классов, 2 группы. **Задание 8** Последним этапом алгоритма построения АСЗИ является: *Выберите один из 4 вариантов ответа:* 1) адаптация, тестирование и сертификация СЗИ АС; 2) Аттестация АСЗИ; 3) Внедрение АСЗИ; 4) Оптимизация параметров качества функционирования СЗИ АС.
2.	Основы разработки систем защиты информации.	**Задание 1** Наименее защищенным типом программной СЗИ является: *Выберите один из 4 вариантов ответа:* 1) СЗИ с полной защитой; 2) СЗИ с единой схемой защиты; 3) СЗИ с программируемой схемой защиты; 4) комплексная система защита. **Задание 2** В системах с полной защитой: *Выберите один из 4 вариантов ответа:* 1) обеспечивается взаимная изоляция пользователей; 2) для каждого файла предусматривается таблица доступа; 3) осуществляется контроль за использованием полученной информации; 4) имеется возможность тонкой настройки всех элементов СЗИ. **Задание 3** Система аудита безопасности подразумевает: *Выберите один из 4 вариантов ответа:* 1) наличие истории действий и возможности работы с ней; 2) наличие возможности наблюдения за персоналом АС; 3) наличие межсетевых экранов в АС; 4) наличие специальных ограничений для персонала АС. **Задание 4** Частью СЗИ не является: *Выберите один из 4 вариантов ответа:* 1) ограничение программной среды; 2) контроль защищенности информации; 3) методические указания пользователю; 4) антивирусная защита. **Задание 5** Документ содержащий полные требования к СЗИ АС, определяемый классом защищенности информации АС, называется: *Выберите один из 4 вариантов ответа:* 1) техническое задание; 2) техническое описание; 3) функциональное описание; 4) полное описание. **Задание 6** К объектам КИИ относят: *Выберите несколько из 4 вариантов ответа:*

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		1) информационные системы; 2) информационно-телекоммуникационные сети; 3) автоматизированные системы управления; 4) сети электросвязи. **Задание 7** Субъектами КИИ являются: *Выберите несколько из 4 вариантов ответа:* 1) владелец объекта КИИ; 2) сопроводитель объекта КИИ; 3) начальник информационной безопасности КИИ; 4) организатор взаимодействия объектов КИИ. **Задание 8** Правом объекта КИИ не является: *Выберите один из 4 вариантов ответа:* 1) право получать от федерального органа исполнительной власти информацию, необходимую для обеспечения ИБ объекта КИИ; 2) право получать от федерального органа исполнительной власти информацию о способах проведения компьютерных атак и методах их предупреждения и обнаружения; 3) право приобретать, устанавливать и обслуживать средства, предназначенные для обнаружения предупреждения и ликвидации компьютерных атак; 4) право сертифицировать и разрабатывать средства, предназначенные для обнаружения предупреждения и ликвидации компьютерных атак. **Задание 9** Главной обязанностью объекта КИИ является: *Выберите один из 4 вариантов ответа:* 1) исполнение нормативных и правовых документов, связанных с КИИ; 2) создание методов и средств обнаружения и предотвращения компьютерных атак; 3) незамедлительное информирование о компьютерных инцидентах ФСБ России; 4) внедрение новейших методов и средств обнаружения и предотвращения компьютерных атак. **Задание 10** SIEM система предназначена для: *Выберите несколько из 4 вариантов ответа:* 1) выявления инцидентов ИБ; 2) логирования остальных средств в СЗИ; 3) уведомления ответственных лиц, в случае инцидента ИБ; 4) предотвращения вторжений и инцидентов ИБ.
3.	Организационные меры защиты информации на основе менеджмента инцидентов.	**Задание 1** По виду информацию можно разделить на следующие группы: *Выберите несколько из 4 вариантов ответа:* 1) общедоступную; 2) конфиденциальную; 3) секретную; 4) запрещенную к распространению. **Задание 2** Основными свойствами информации в АСЗИ являются: *Выберите один из 4 вариантов ответа:* 1) конфиденциальность, целостность и доступность;

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		2) аутентичность, целостность и доступность; 3) подотчетность, надежность, своевременность и целостность; 4) устойчивость, конфиденциальность, своевременность и достоверность. **Задание 3** Персональные данные – это: *Выберите один из 4 вариантов ответа:* 1) любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу; 2) любая информация о человеке; 3) любая информация о человеке или юридическом лице; 4) любая информация, относящаяся к прямо или косвенно определенному, или определяемому юридическому лицу. **Задание 4** В рамках ИС ПДн существует следующее количество категорий и объемов ПДн: *Выберите один из 4 вариантов ответа:* 1) 4 вида категорий и 3 вида объемов; 2) 2 вида категорий и 2 вида объемов; 3) 3 вида категории и 1 вида объемов; 4) 5 вида категории и 3 вида объемов. **Задание 5** Организационные меры обеспечения безопасности ИС – это меры организационного характера: *Выберите один из 4 вариантов ответа:* 1) направленные на то, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации; 2) направленные на снижение рисков; 3) направленные на установление мер наказания для обслуживающего персонала; 4) направленные на совершенствование СЗИ АС. **Задание 6** В задачи организационных мер обеспечения ИБ входит: *Выберите несколько из 4 вариантов ответа:* 1) создание регламента информационных отношений; 2) определение методов и принципов разграничения доступа; 3) создание технической документации; 4) управление персоналом. **Задание 7** Организационные меры обеспечения ИБ в рамках АСЗИ взаимосвязаны с: *Выберите несколько из 4 вариантов ответа:* 1) правовыми мерами обеспечения ИБ; 2) техническими мерами обеспечения ИБ; 3) физическими мерами обеспечения ИБ; 4) технологическими мерами обеспечения ИБ. **Задание 8** Основным документом в рамках организационных мер обеспечения ИБ является: *Выберите один из 4 вариантов ответа:* 1) приказы ФСТЭК России;

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		2) политика ИБ, принятая в АС; 3) федеральный закон №149 «Об информации, информационных технологиях и о защите информации»; 4) письменные распоряжения начальника отдела информационной безопасности.
4.	Эксплуатация автоматизированных систем в защищенном исполнении.	**Задание 1** Ввод в эксплуатацию СЗИ включает следующие этапы: *Выберите несколько из 4 вариантов ответа:* 1) проведение опытной эксплуатации СЗИ; 2) проведение приемно-сдаточных испытаний СЗИ; 3) Проведение оценки защищенности объектов информатизации; 4) Разработка эксплуатационной документации на объекты информатизации и СЗИ. **Задание 2** Типовые политики ИБ или защитные меры ИБ: *Выберите один из 4 вариантов ответа:* 1) обеспечивают полную защиту информации; 2) не позволяют гарантировать полную защиту информации; 3) не обеспечивают достаточную защиту информации; 4) не обеспечивают защиту информации. **Задание 3** Событие ИБ — это: *Выберите один из 4 вариантов ответа:* 1) идентифицированное появление определенного состояния системы, указывающего на возможное нарушение политики ИБ; 2) любое зафиксированное действие в системе; 3) появление определенного состояния системы, указывающего на возможное нарушение политики ИБ; 4) идентифицированное появление определенного состояния системы. **Задание 4** Инцидент ИБ — это: *Выберите один из 4 вариантов ответа:* 1) событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операции и создания угрозы ИБ; 2) событие, полностью соответствующее описанию в модели угроз; 3) событие, не описанное в модели угроз; 4) событие, описанное в стандарте ГОСТ Р ИСО/МЭК 18044. **Задание 5** Целями управления инцидентами ИБ является: *Выберите один из 4 вариантов ответа:* 1) обнаружение и эффективная обработка событий ИБ; 2) идентификация, оценка и урегулирование инцидентов ИБ; 3) минимизация негативных воздействий инцидентов ИБ; 4) извлечение уроков из инцидентов ИБ и их менеджмента. **Задание 6** Определение событий ИБ, относящимся к инцидентам ИБ происходит на следующем этапе управления инцидентами ИБ: *Выберите один из 4 вариантов ответа:* 1) планировании и подготовке; 2) использовании системы управления инцидентами ИБ;

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		3) анализе инцидентов и событий ИБ; 4) улучшении системы управления инцидентами ИБ. **Задание 7** В случае, если инцидент ИБ находится не под контролем, то выполняются: *Выберите один из 4 вариантов ответа:* 1) экстренные действия; 2) особые действия; 3) «антикризисные» действия; 4) специальные действия. **Задание 8** За обнаружение события ИБ отвечает: *Выберите один из 4 вариантов ответа:* 1) специалист по защите информации; 2) специалист по управлению инцидентами ИБ; 3) группа реагирования на инциденты ИБ; 4) лицо, первым заметившее признаки события ИБ. **Задание 9** За вторичную оценку и разрешение инцидента ИБ отвечает: *Выберите один из 4 вариантов ответа:* 1) специалист по защите информации; 2) специалист по управлению инцидентами ИБ; 3) группа реагирования на инциденты ИБ; 4) лицо, первым заметившее признаки события ИБ.

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме зачета используется следующая шкала оценивания: зачтено, не зачтено.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий
	Знание основных закономерностей, принципов, регламентов, методов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний
Умения	Умение анализировать основные положения законодательства в области безопасности информации
	Умение использовать и применять руководящие документы в области информационной безопасности и средства защиты информации
	Умение осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, определять источники, причины и последствия выявленных инцидентов
Навыки	Владение навыками теоретического и экспериментального исследования

	объектов профессиональной деятельности
	Качество выполнения исследований объектов профессиональной деятельности
	Самостоятельность выполнения исследований объектов профессиональной деятельности
	Инструментальный контроль показателей эффективности ЗИ

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5

Умение анализировать основные положения законодательства в области безопасности информации	Не умеет анализировать основные положения законодательства в области безопасности информации	Допускает неточности в анализе основных положений законодательства в области безопасности информации	Умеет анализировать основные положения законодательства в области безопасности информации	Умеет анализировать основные положения законодательства в области безопасности информации и делать обобщающие выводы
Умение использовать руководящие документы регуляторов в области информационной безопасности	Не умеет использовать руководящие документы регуляторов в области информационной безопасности	Использование руководящих документов регуляторов в области информационнй безопасности вызывает затруднения	Умеет использовать руководящие документы регуляторов в области информацион ной безопасности	Умело использует руководящие документы регуляторов в области информационной безопасности
Умение осуществлять контроль обеспечения уровня защищенности в автоматизированн ых системах, определять источники, причины и последствия выявленных инцидентов	Не умеет осуществлять контроль обеспечения уровня защищенности, определять источники, причины и последствия выявленных инцидентов	Определение источников, причин и последствий выявленных инцидентов и осуществление контроля обеспечения уровня защищенности вызывает затруднения	Умеет осуществлять контроль обеспечения уровня защищенности в автоматизирова нных системах, определять источники, причины и последствия выявленных инцидентов	Умеет осуществлять контроль обеспечения уровня защищенности , определять источники, причины и последствия выявленных инцидентов, делать обобщающие выводы

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и экспериментальн ого исследования объектов профессионально й деятельности	Не владеет навыками теоретического и экспериментально го исследования объектов профессионально й деятельности	Не достаточно хорошо владеет навыками теоретического и экспериментальн ого исследования объектов профессиональн ой деятельности	Владеет навыками теоретического и экспериментальн ого исследования объектов профессиональ ной деятельности	Профессионально владеет навыками теоретического и экспериментальног о исследования объектов профессиональной деятельности
Качество выполнения исследований объектов профессионально й деятельности	Не качественно выполняет исследования объектов профессионально й деятельности,	Не достаточно качественно выполняет исследования объектов профессиональн	Не достаточно качественно выполняет исследования объектов профессиональн	Качественно выполняет исследования объектов профессиональной деятельности

	допускает грубые ошибки	ой деятельности, допускает и исправляет ошибки с посторонней помощью	ой деятельности, допускает и исправляет ошибки самостоятельно	
Самостоятельность выполнения исследований объектов профессиональной деятельности	Не может самостоятельно выполнять исследования объектов профессиональной деятельности	Выполняет исследования объектов профессиональной деятельности с посторонней помощью	При выполнении исследования объектов профессиональной деятельности иногда требуется посторонняя помощь	Самостоятельно выполняет исследования объектов профессиональной деятельности
Инструментальный контроль показателей эффективности ЗИ	Не может самостоятельно выполнять инструментальный контроль показателей эффективности ЗИ	Выполняет инструментальный контроль показателей эффективности ЗИ с посторонней помощью	При выполнении инструментального контроля показателей эффективности ЗИ иногда требуется посторонняя помощь	Самостоятельно выполняет инструментальный контроль показателей эффективности ЗИ

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения лабораторных занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду.

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1.	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V6328633 Соглашение действительно с 02.10.2017 по 23.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017.
2.	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V6328633 Соглашение действительно с 02.10.2017 по 23.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017.
3.	Среды программирования Free Pascal, Dev C++, CodeBlocks, VS Code	Свободно распространяемое ПО согласно условиям лицензионного соглашения.

6.3. Перечень учебных изданий и учебно-методических материалов

1. Каданова, Айжана М. et al. АЛГОРИТМ СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 93–100, 2019. ISSN 2074–7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1235>. Дата доступа: 10 jan. 2022. doi:http://dx.doi.org/10.26583/bit.2019.4.07.

2. ГОСТ 34.601–90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания / М.: Стандартинформ, 2009 год.

3. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий (с Поправкой) / М.: Стандартинформ, 2007 год.

4. Бедердинова Оксана Ивановна, Коряковская Наталья Владимировна Алгоритм разработки системы защиты информации // Arctic Environmental Research. 2013. №3. URL: https://cyberleninka.ru/article/n/algoritm-razrabotki-sistemy-zaschity-informatsii (дата обращения: 10.01.2022).

5. Бокова, О. И., Дровникова, И. Г., Етепнев, А. С., Рогозин, Е. А., & Хвостов, В. А. (2019). Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах. Труды СПИИРАН, 18(6), 1301-1332. https://doi.org/10.15622/sp.2019.18.6.1301-1332.

6. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (Переиздание) / Официальное издание. М.: Стандартинформ, 2020.

7. Приказ ФСТЭК России от 31 августа 2010 г. N 489. Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования. Электронный ресурс: fstec.ru (Дата обращения: 14.01.2022).

8. Приказ ФСТЭК России от 11 февраля 2013 г. N 17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Электронный ресурс: fstec.ru (Дата обращения: 14.01.2022).

9. Приказ ФСТЭК России от 14 марта 2014 г. N 31. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных

объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Электронный ресурс: fstec.ru (Дата обращения: 14.01.2022).

10. Приказ ФСТЭК России от 21 декабря 2017 г. N 235. Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования. Электронный ресурс: fstec.ru (Дата обращения: 14.01.2022).
11. Приказ ФСТЭК России от 18 февраля 2013 г. N 21. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Электронный ресурс: fstec.ru (Дата обращения: 14.01.2022).
12. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Электронный ресурс: fstec.ru (Дата обращения: 21.01.2022).
13. Федеральный закон от 26 июля 2017 г. N 187-ФЗ. О безопасности критической информационной инфраструктуры Российской Федерации. Электронный ресурс: fstec.ru (Дата обращения: 21.01.2022).
14. ГОСТ Р 51583–2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения / Официальное издание. М.: Стандартинформ, 2018 год.

6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Электронная библиотека (на базе ЭБС «БиблиоТех») — Режим доступа: http://ntb.bstu.ru
2. Электронно-библиотечная система IPRbooks — Режим доступа: http://www.iprbookshop.ru
3. Электронно-библиотечная система «Университетская библиотека ONLINE» — Режим доступа: http://www.biblioclub.ru/

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 202__/202__ учебный год без изменений / с изменениями, дополнениями

Протокол № _____ заседания кафедры от «____»_____ 202__ г.

Заведующий кафедрой_____
подпись, ФИО

Директор института _____
подпись, ФИО