МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.В.01.01 «Комплексное обеспечение информационной безопасности автоматизированных систем и объектов информатизации»

Направление подготовки:
10.04.01 «Информационная безопасность»

Направленность (профиль) программы магистратуры:
«Информационная безопасность интеллектуальных и информационно-аналитических систем»

Квалификация выпускника: магистр

Тольятти 2022

Рабочая программа дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем и объектов информатизации» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - магистратура по направлению подготовки 10.04.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования РФ от 26 ноября 2020 г. № 1455

Составители:

к. э. н., доцент	О.А. Филиппова
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании высшей школы интеллектуальных систем и кибертехнологий 02.12.2022 г., протокол № 4

Директор высшей школы интеллектуальных систем и кибертехнологий

к. э. н., доцент	/О.А. Филиппова
(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является: формирование у студентов теоретических знаний и практических навыков по разработке и внедрению комплексных систем защиты информации в автоматизированных системах и на предприятиях различных форм собственности.

в области обучения:

- формирование у обучающихся общепрофессиональных и профессиональных компетенций, направленных на решение задач профессиональной деятельности;
- развитие навыков профессиональной деятельности.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**	**Основание (ПС)** *для профессиональных компетенций
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемы	**Знает:** жизненный цикл и принципы организации информационных систем в соответствии с требованиями по защите информации; методы принятия эффективных проектных решений в условиях неопределенности и риска ПО; методы анализа возникающей неопределенности и риска и оценки их негативных последствий. **Умеет:** проектировать системы обеспечения информационной безопасности, ее компоненты и подсистемы, а также управлять подобными проектами и принимать эффективные проектные решения в условиях неопределенности и риска. **Владеет:** навыками разработки технических проектов систем (подсистем либо компонент систем) обеспечения информационной безопасности	
ПК-3 Способен оценить угрозы безопасности информации автоматизированной системы и обосновать необходимость её защиты	ИПК-3.1. Строит модель угроз безопасности информации, обрабатываемой автоматизированной системы; ИПК-3.2. Обосновывает необходимость защиты информации в интеллектуальных и информационно-аналитических системах.	**Знает:** методику построения модели угроз информационной безопасности, а также принципы формирования комплекса мер по обеспечению информационной безопасности предприятия(организации) и организации информационных систем в соответствии с требованиями по защите информации. **Умеет:** проводить мониторинг угроз безопасности информационных систем, а также обосновывать необходимость защиты информации и определять комплекс мер для обеспечения информационной безопасности в интеллектуальных и информационно-аналитических	ПС 06.033 Специалист по защите информации в автоматизированных системах

		системах. **Владеет:** навыками мониторинга и аудита угроз информационной безопасности информационных систем, а также методами обоснования необходимости их защиты	
ПК-4. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных	ИПК-4.3. Разрабатывает архитектуру системы защиты информации автоматизированных систем, а также интеллектуальных и информационно-аналитических систем в частности	**Знает:** принципы, а также современные методологии и технологии построения эффективной и безопасной архитектуры информационно-аналитических систем **Умеет:** разрабатывать единую архитектуру системы всесторонней защиты информации автоматизированных информационно-аналитических и интеллектуальных систем **Владеет:** навыками разработки архитектуры систем защиты информации автоматизированных информационно-аналитических и интеллектуальных систем с учетом специфики деятельности предприятия (организации) и обрабатываемых данных	ПС 06.033 Специалист по защите информации в автоматизированных системах

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы (Б.1.В.01 Профессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **6 з.е. (216 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**216**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**32/14**
занятия лекционного типа (лекции)	12/ 6
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	20/8
Самостоятельная работа всего, в т.ч.:	**157/193**
самоподготовка по темам (разделам) дисциплины	121/157
выполнение курсового проекта /курсовой работы	36/36
Контроль (экзамен)	**27 /9**
Промежуточная аттестация	**Экзамен / защита КП**

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы			Формы текущего контроля (наименование оценочного средства)
		Контактная работа		Самостоятельная работа, час	
		Лекции, час	Практические занятия, час		
ОПК-2. ИОПК-2.2. ПК-3. ИПК-3.1	**Тема 1. Базовые понятия сущности комплексного обеспечения информационной безопасности (КОИБ)** Основное содержание: Сущность и задачи комплексного обеспечения информационной безопасности. Принципы организации и этапы разработки комплексного обеспечения информационной безопасности (КОИБ) автоматизированных систем и объектов информатизации. Факторы, влияющие на организацию КОИБ. Определение и нормативное закрепление состава защищаемой информации. Определение объектов защиты	4/ 2	-	-	Опрос по темам лекционных занятий Отчёт по практической работе
	Практическое занятие № 1. Определение объектов защиты и выделение угроз информационной безопасности предприятия	-	2/ 1	-	
	Самостоятельная работа	-	-	20 / 30	
ОПК-2. ИОПК-2.2. ПК-3. ИПК-3.2	**Тема 2.Сущностная характеристика компонентов КОИБ и определение условий их функционирования.** Основное содержание: Идентификация информационных активов. Анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.Определение потенциальных каналов и методов несанкционированного доступа к информации. Определение возможностей несанкционированного доступа к защищаемой информации.	4/ 2	-	-	Опрос по темам лекционных занятий Отчёты по практическим работам
	Практическое занятие № 2.Анализ рисков информационной безопасности. Разработка формализованной и неформализованной политики информационной безопасности на предприятии	-	4 / 1	-	
	Практическое занятие № 3. Разработка структуры КОИБ на предприятии	-	2 / 1	-	
	Практическое занятие № 4. Разработка нормативно-правовой и организационно-методической подсистем КОИБ предприятия	-	2 / 1	-	
	Самостоятельная работа	-	-	50/60	
ПК-4.	**Тема 3. Разработка модели КОИБ и её**	4 / 2	-	-	

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы			Формы текущего контроля (наименование оценочного средства)
		Контактная работа		Самостоятельная работа, час	
		Лекции, час	Практические занятия, час		
ИПК-4.3	**архитектуры** Основное содержание: Технологическое и организационное построение КОИБ. Кадровое обеспечение функционирования КОИБ. Материально-техническое и нормативно-методическое обеспечение функционирования КОИБ. Назначение, структура и содержание управления КОИБ. Принципы и методы построения архитектуры КОИБ. Сущность и содержание контроля функционирования КОИБ. Состав методов и моделей оценки эффективности КОИБ.				Опрос по темам лекционных занятий Отчёт по практическим работам
	Практическое занятие № 5.Разработка модели инженерно-технической подсистемы КОИБ на предприятии	-	4 / 2	-	
	Практическое занятие № 6.Разработка модели программно-аппаратной подсистемы КОИБ на предприятии	-	6/2	-	
	Самостоятельная работа	-	-	51 /67	
ОПК-2. ИОПК-2.2. ПК-3. ИПК-3.1 ИПК-3.2 ПК-4. ИПК-4.3	Выполнение курсового проекта /курсовой работы	-	-	36/36	Курсовой проект
	ИТОГО	**12 / 6**	**20 / 8**	**157/ 193**	

Примечание: *-/- объем часов соответственно для очной и очно-заочной форм обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися(включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

-балльно-рейтинговая технология оценивания;

- электронное обучение;

- проблемное обучение;

- проектное обучение;

- разбор конкретных ситуаций.

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2.Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиями выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

В ходе лекционных занятий необходимо вести конспектирование учебного материала.

4.3. Методические указания для обучающихся по освоению дисциплины на занятиях практического (семинарского) типа

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях с применением необходимых специализированных средств.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- получение навыков работы с кейсами и практическими заданиями в области профессиональной деятельности;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: решение прикладных задачи кейсов при изучении тем 1-3.

4.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 5.

В процессе самостоятельной работы при изучении дисциплины студенты могут использовать в специализированных аудиториях для самостоятельной работы компьютеры, обеспечивающему доступ к программному обеспечению, необходимому для изучения дисциплины, а также доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной

библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

Для обучающихся по очно-заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

4.5. Методические указания для выполнения курсового проекта

Выполнение курсового проекта способствует лучшему освоению обучающимися учебного материала, формирует практический опыт и умения по изучаемой дисциплине, способствует формированию у обучающихся готовности к самостоятельной профессиональной деятельности, является этапом к выполнению выпускной квалификационной работы.

Примерная тематика курсовых проектов

1. Разработка комплексной системы защиты информации производственного предприятия
2. Организация системы мониторинга информационной безопасности организации
3. Разработка комплекса мероприятий противодействия внутренним угрозам предприятия
4. Особенности использования методов защиты информации при разработке веб-приложения
5. Организация защиты информационных ресурсов корпоративной сети предприятия
6. Методы идентификации субъекта и их применение
7. Разработка комплексной системы защиты информации коммерческого предприятия
8. Проект управления рисками информационной безопасности предприятия
9. Особенности разработки комплексной системы защиты информации в банковской сфере
10. Программно-аппаратные средства шифрования
11. Разработка комплексной системы защиты информации вуза
12. Разработка системы инженерно-технической защиты информации предприятия
13. Разработка политики информационной безопасности в организации
14. Разработка программы проведения аудита безопасности информации в организации.
15. Разработка частной модели угроз безопасности персональных данных при их обработке в ИСПДн
16. Разработка мероприятий по контролю эффективности функционирования системы защиты информации в компании
17. Разработка комплекса мер по защите информации от утечки по техническим каналам в организации
18. Разработка организационно-распорядительных документов, регламентирующих обеспечение информационной безопасности сведений, составляющих ПДн
19. Организация обработки персональных данных в компании (организации)
20. Методы и способы защиты информации от утечки по техническим каналам
21. Методы и средства защиты информации от несанкционированного доступа в сети Интернет
22. Разработка предложений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
23. Разработка предложений по обеспечению безопасности информации в автоматизированных системах управления технологическими процессами
24. Анализ уязвимостей в социальных сетях
25. Исследование безопасности мобильных платформ
26. Разработка рекомендаций по использованию средств защиты от DDOS-атак в корпоративных сетях

27. Разработка рекомендаций по организации защиты информационной системы малого предприятия
28. Совершенствование системы защиты информации производственного предприятия

Структура и содержание курсового проекта

Содержание курсового проекта должно демонстрировать знакомство студента с основной литературой по теме проекта, умение выявить задачу исследования и определить методы ее решения, умение последовательно изложить существо рассматриваемых вопросов, владение необходимой терминологией и понятиями, приемлемый уровень языковой грамотности и владение стилем научного изложения.

Текстовая часть курсового проекта должна содержать следующие структурные элементы:

- титульный лист;
- лист задания;
- аннотация;
- содержание;
- введение;
- главы, разделы, излагающие основное содержание работы;
- заключение;
- список использованных источников;
- Приложения (не входят в объем основного содержания курсовой);
- рецензия на курсовой проект.

Требования к оформлению курсового проекта

Пояснительная записка курсового проекта набирается на компьютере на одной стороне стандартного листа бумаги формата А4. Объем пояснительной записки (без приложений) составляет 25…35 страниц. Текст печатается через 1,5 интервала 12 шрифтом.

Текстовая часть выполняется на листах формата А4без рамки, с соблюдением следующих размеров полей:

- левое – 30 мм,
- правое – 15 мм,
- верхнее – 20 мм,
- нижнее – 20 мм.

Пояснительная записка должна иметь сквозную нумерацию страниц, включая список литературы и приложения. Страницы нумеруются вверху страницы от центра. При этом следует учесть, что первой страницей является титульный лист, второй – лист задания. На них нумерация не ставится.

Заголовки разделов пояснительной записки выполняют основным шрифтом. Расстояние между заголовком и основным текстом составляет 1 строку. Перенос слов в заголовках не допускается.

Разделы должны иметь порядковую нумерацию в пределах всей работы и обозначаться арабскими цифрами. Введение и заключение не нумеруются.

Таблицы и иллюстрации (рисунки, графики, схемы) следует располагать непосредственно после текста, в котором они упоминаются впервые, или на следующей странице так, чтобы их было удобно рассматривать без поворота работы или с поворотом по часовой стрелке. Иллюстрации, таблицы, формулы нумеруются последовательно арабскими цифрами в пределах всей работы. Допускается нумерация в пределах раздела. Каждая таблица, график, рисунок (схема) должны иметь свой заголовок (название).

Номера таблиц ставят с правой стороны, на следующей строке указывается наименование (заголовок) таблицы. При переносе таблицы на следующую страницу в левом верхнем углу дают сведения о продолжении таблицы (например, Продолжение таблицы 1), и вместо «шапки» таблицы допускается указывать порядковые номера имеющихся граф.

На все иллюстрации и таблицы должны быть даны ссылки в тексте. Начинать разделы с

рисунков или таблиц не допускается. В пояснительной записке таблицы и рисунки помещаются после текста, в котором приводится на них ссылка.

Формулы выносятся в отдельную строку и сначала записываются в общем виде с пояснением значений символов, затем в том же порядке в формулы подставляют числовые значения символов. Пояснения значений символов нужно приводить непосредственно после формулы, в той же последовательности, в какой они даны в формуле. Значение каждого символа необходимо давать с новой строки. Первая строка пояснения должна начинаться со слова «где» без двоеточия без него.

Список использованных литературных источников должен быть оформлен в соответствии с требованиями ГОСТов. Ссылки на литературные источники в тексте следует делать непосредственно после информации (данных) или в конце фразы, указывая порядковый номер источника в списке. Номер ссылки берется в квадратные скобки [ ].

В соответствии с целями и задачами курсовой проект не должен быть пересказом изученного материала или простой компиляцией (несамостоятельное произведение, составленное путем заимствований, без собственных выводов и рассуждений).

Курсовой проект должен быть написан грамотным научным языком, с учетом особенностей научной речи, точности и однозначности терминологии и стиля. В курсовом проекте не употребляются личные местоимения «я» и «мы». Например, используется фраза «предполагается» вместо фразы «я предполагаю».

Порядок сдачи и защиты курсового проекта

Выполненный и оформленный курсовой проект сдается на кафедру для проверки и получения рецензии. Срок сдачи курсового проекта указывается в задании.

В случае положительной рецензии студент допускается к защите курсового проекта. Если рецензия предусматривает доработку, то в соответствии с указанными замечаниями студент исправляет работу и сдает на дополнительное рецензирование.

Защита курсового проекта является заключительным этапом курсового проектирования. Сроки защиты сообщаются студентам заранее, при выдаче задания.

По результатам защиты студенту выставляется балльная оценка, на которую влияют:

- обоснованность принятых решений;
- качество содержания и оформления пояснительной записки (оценка выставляется преподавателем, проверяющим пояснительную записку, и при необходимости сопровождается рецензией);
- качество доклада;
- правильность и полнота ответов на вопросы.

Итоговая оценка курсового проекта складывается из оценки содержания, оформления работы и устной защиты.

Студент, не представивший в установленный срок курсовой проект или не защитивший его, считается имеющим академическую задолженность.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие по направлению "Приклад. информатика" / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Документ read. - Москва : РИОР [и др.], 2022. - 336 с. - (Высшее образование). - Прил. - URL: https://znanium.com/read?id=393765 (дата обращения: 25.02.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01761-6. - 978-5-16-106532-7. - Текст : электронный. URL: https://znanium.com/read?id=393765

2. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2021. - 400 с. - (Высшее образование: Бакалавриат; Магистратура). - URL: https://znanium.com/read?id=367588 (дата обращения: 09.12.2020). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01759-3. - 978-5-16-013801-5. - 978-5-16-106478-8. - Текст : электронный. URL: https://znanium.com/read?id=367588

3. Конюх, В. Л. Проектирование автоматизированных систем производства : учеб. пособие для вузов по направлению "Автоматизир. технологии и производства" / В. Л. Конюх. - Документ read. - Москва : Курс [и др.], 2019. - 312 с. - Прил. - URL: https://znanium.com/read?id=355804 (дата обращения: 19.02.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-905554-53-7. - 978-5-16-009624-7. - 978-5-16-100905-5. - Текст : электронный. URL: https://znanium.com/read?id=355804

4. Нестеров, С. А. Основы информационной безопасности : учеб. пособие / С. А. Нестеров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 322 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/206279 (дата обращения: 20.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-4067-2. - Текст : электронный. URL: https://reader.lanbook.com/book/206279

5. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Изд. 4-е, стер. - Документ Reader. - Санкт-Петербург : Лань, 2022. - 124 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/217445 (дата обращения: 06.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-44201-0. - Текст : электронный. URL: https://reader.lanbook.com/book/217445

6. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник по направлению подгот. "Информ. безопасность" / М. В. Тумбинская, М. В. Петровский. - Изд. 2-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 344 с. - (Учебники для вузов. Специальная литература). - URL: https://reader.lanbook.com/book/256133 (дата обращения: 29.09.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45046-6 : 0-00. - Текст : электронный. URL: https://reader.lanbook.com/book/256133

Дополнительная литература

7. Бабаш, А. В. Актуальные вопросы защиты информации : монография / А. В. Бабаш, Е. К. Баранова. - Документ read. - Москва : РИОР [и др.], 2021. - 112 с. - (Научная мысль). - URL: https://znanium.com/read?id=375285 (дата обращения: 03.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01680-0. - 978-5-16-106277-7. - Текст : электронный. URL: https://znanium.com/read?id=375285.

8. Бильфельд, Н. В. Современные средства реализации автоматизированных систем. Работа с Google таблицами : учеб. пособие / Н. В. Бильфельд, Ю. И. Володина. - Документ read. - Москва : Риор [и др.], 2022. - 172 с. - (Высшее образование). - URL: https://znanium.ru/read?id=399264 (дата обращения: 17.01.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01721-0. - 978-5-16-106016-2. - Текст : электронный. URL: https://znanium.ru/read?id=399264

9. Ворона, В. А. Теоретические основы обеспечения безопасности объектов информатизации : учеб. пособие для вузов по направлению "Информ. безопасность" / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. - Москва : Горячая линия -Телеком, 2016. - 304 с. : ил. - (Учебное пособие для высших учебных заведений). - ISBN 978-5-9912-0524-5 : 588-50. - Текст : непосредственный..

10. Клименко, И. С. Информационная безопасность и защита информации. Модели и методы управления : монография / И. С. Клименко. - Документ read. - Москва : Инфра-М, 2022. - 180 с. - (Научная мысль). - URL: https://znanium.com/read?id=397337 (дата обращения: 02.03.2023). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-108124-2. - Текст : электронный. URL: https://znanium.com/read?id=397337

11. Коломейченко, А. С. Информационные технологии : учеб. пособие / А. С. Коломейченко, Н. В. Польшакова, О. В. Чеха. - Изд. 3-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2022. - 211 с. - Основ. термины и понятия. - Основ. сокращения. - URL: https://reader.lanbook.com/book/264086#1 (дата обращения: 22.09.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-45293-4. - Текст : электронный. URL: https://reader.lanbook.com/book/264086#1

12. Конфликтно-активное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / В. И. Новосельцев, С. С. Кочедыков, Д. Е. Орлова, К. А. Плющик ; под ред. В. И. Новосельцева. - Документ read. - Москва : ИНФРА-М, 2023. - 235 с. - (Научная мысль). - Прил. - URL: https://znanium.com/read?id=426480 (дата обращения: 02.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-111199-4. - Текст : электронный. URL: https://znanium.com/read?id=426480.

13. Олифер, В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - Москва : Горячая линия -Телеком, 2016. - 644 с. : ил. - Прил. - ISBN 978-5-9912-0420-0 : 823-90. - Текст : непосредственный.

14. Поддержка принятия решений при проектировании систем защиты информации : монография / В. В. Бухтояров, М. Н. Жукова, В. В. Золотарев [и др.]. - Документ read. - Москва : ИНФРА-М, 2020. - 131 с. - (Научная мысль). - URL: https://znanium.com/read?id=343296 (дата обращения: 19.02.2024. - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-100714-3. - Текст : электронный. URL: https://znanium.com/read?id=343296

15. Сычев, Ю. Н. Защита информации и информационная безопасность : учеб. пособие для студентов высш. учеб. заведений по направлению подгот. 10.03.01. "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю. Н. Сычев. - Документ read. - Москва : ИНФРА-М, 2022. - 201 с. - (Высшее образование - бакалавриат). - Прил. - URL: https://znanium.com/read?id=388766 (дата обращения: 26.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-107471-8. - Текст : электронный. URL: https://znanium.com/read?id=388766

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 03.12.2021). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
2. КонсультантПлюс : справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения 03.12.2021). - Текст : электронный.
3. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru(дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.
4. Электронно-библиотечная система Znanium.com: сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.
5. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.
6. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс](дата обращения 10.12.2022).– Режим доступа: https://fstec.ru/?ysclid=lt28avnafe147143067. – Загл. с экрана.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	MicrosoftOffice	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с

возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интеренет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

– компьютерные классы университета;

– библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети «Интернет».

Электронная информационно-образовательная среда университета (ЭИОС).

Каждыйобучающийсявтечениевсегопериодаобученияобеспечениндивидуальнымнеограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

– доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

– формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

– фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

– проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

– взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети «Интернет».

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины	
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл
Экзамен / защита КП	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3
			70-85,9	«хорошо» / 4
	повышенный	86-100	86-100	«отлично» / 5

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу).Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

Результат обучения считается сформированным (повышенный уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.

Результат обучения считается сформированным (пороговый уровень), если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Доклад/сообщение (опрос)	3	5	15
Выполнениепрактических заданий (отчёт по практическим работам № 1-4)	4	10	40
Выполнение практических заданий (отчёт по практическим работам № 5-6)	2	15	30
Творческий рейтинг (участие в конференциях, олимпиадах), дополнительные баллы за активное изучение дисциплины	1	15	15
			100 баллов

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическое занятие № 1. Определение объектов защиты и выделение угроз информационной безопасности предприятия

Задание.

Для выполнения практического задания необходимо выбрать конкретное предприятие и провести анализ его деятельности.

1. Описание и анализ деятельности должны включать следующие сведения: основные направления деятельности; описание существующего документооборота предприятия; программное и аппаратное обеспечение предприятия.
2. Подготовить функциональную модель разработки КОИБ для вашего предприятия с помощью BPWin (2-3 уровня детализации).
3. Выделить информационные активы предприятия, подлежащие защите.
4. На основе примеров, построить деревья угроз для выбранного предприятия.
5. Оформить отчёт по практической работе

Практическое занятие № 2. Анализ рисков информационной безопасности. Разработка формализованной и неформализованной политики информационной безопасности на предприятии

Задание.

Исследовать существующие методы и ПО для анализа информационных рисков с проведением сравнительного анализа

1. Изучить методику GRAMM.
2. Изучить методику FRAP
3. Изучить методику OCTAVE.
4. Изучить методику и ПО MSAT
5. Провести анализ рисков для предприятия с использованием одной из методик.
6. Провести анализ рисков и угроз информационной безопасности предприятия
7. Разработать политику информационной безопасности для предприятия в виде документа
8. Оформить отчёт по практической работе

Практическое занятие № 3. Разработка структуры КОИБ на предприятии

Задание.

По результатам выполнения предыдущих работ выполнить:

1. Перечислить существующие подходы к проектированию КОИБ. Выделить их достоинства и недостатки.
2. Построить математическую модель КОИБ предприятия.
3. Разработать структуру КОИБ для предприятия.
4. Оформить отчёт по практической работе.

Практическое занятие № 4. Разработка нормативно-правовой и организационно-методической подсистем КОИБ предприятия

Задание.

На основании разработанного ранее документа «Политика информационной безопасности для предприятия», выполнить следующие задания:

1. Построить список нормативно-правовых актов, регулирующих информационную безопасность.
2. Разработать нормативно-правовую подсистему КОИБ предприятия на основе анализа правовых документов и стандартов в области защиты информации.
3. Разработать организационно-методическую подсистему КОИБ предприятия, включающую (ОСУ ИБ, документы, инструкции и др).
4. Разработать план внедрения методов и средств разработанных подсистем с указанием мероприятий, сроков и ответственных (в таблице).
5. Оформить отчёт по практической работе.

Практическое занятие № 5. Разработка модели инженерно-технической подсистемы КОИБ на предприятии

Задание.

На основании разработанного ранее документа «Политика информационной безопасности для предприятия», выполнить следующие задания:

1. Разработать 2-3 модели инженерно-технической подсистемы КОИБ предприятия на основе анализа инженерно-технических методов и средств (выбор инженерно-технических средств проводить на основе аналитических таблиц сравнений по основным параметрам).
2. Выбрать оптимальную модель инженерно-технической подсистемы КОИБ предприятия (при выборе необходимо учитывать стоимость и качество методов и средств защиты).
3. Оформить отчёт по практической работе.

Практическое занятие № 6. Разработка модели программно-аппаратной подсистемы КСЗИ на предприятии

Задание.

На основании разработанного ранее документа «Политика информационной безопасности для предприятия», выполнить следующие задания:

1. Сформулировать требования, которые необходимо учесть при разработке программно-аппаратной подсистемы КОИБ.
2. Разработать 2-3 модели программно-аппаратной подсистемы КОИБ предприятия на основе анализа программно-аппаратных методов и средств (выбор программно-аппаратных средств проводить на основе аналитических таблиц сравнений по основным параметрам).
3. Выбрать оптимальную модель программно-аппаратной подсистемы КОИБ предприятия (при выборе необходимо учитывать стоимость и качество методов и средств защиты).
4. Оформить отчёт по практической работе.

8.2.2. Типовые вопросы для устного опроса

1. Понятие комплексной системы защиты информации на предприятии в разрезе современного электронного оборудования.
2. Сущность и задачи комплексного обеспечения информационной безопасности (КОИБ) на предприятии.
3. Принципы организации комплексной защиты информации на предприятии.
4. Требования к комплексной системе защиты информации на предприятии.
5. Определение потенциальных каналов и методов несанкционированного доступа к информации.
6. Определение возможностей несанкционированного доступа к защищаемой информации.
7. Методы и средства защиты информации, используемые в КОИБ.
8. Определение компонентов КОИБ.
9. Инженерно-техническая подсистема КОИБ на предприятии.
10. Использование международных и российских стандартов безопасности при разработке КСЗИ предприятия.
11. Классификация средств защиты информации от НСД.
12. Описать сущность системного подхода и его основные положения при выполнении анализа потребности в КОИБ и ее синтезе.
13. Описать возможность реализации системного подхода при разработке ТЗ для КОИБ.
14. Опишите сущность процессного подхода и возможность его практического применения для выбранной в задаче предметной области
15. Описать сущность проффесиографического подхода и его роль в деятельности ИС-службы, выполняющей защиту информации.
16. Опишите сущность структурного подхода к информатизации, в процессе выявления объектов защиты информации. Приведите примеры структурного анализа.
17. Укажите требования ГОСТ 34.602-89. предъявляемые к разработке ТЗ с точки зрения научных подходов.
18. Опишите характерные особенности структурного подхода и сделайте сравнительный анализ средств автоматизации, поддерживающий его возможности.
19. Охарактеризуйте особенности компетентностного подхода и составьте матрицу компетенций, которыми, на ваш взгляд, должен обладать специалист, для решения выбранной задачи* предметной области.
20. Дайте определение информатизации и приведите пример основных направлений информатизации, на которые сконцентрировано наибольшее внимание проводимой в стране Стратегии социально-экономического развития.
21. Каким образом информатизация связана с использованием современного электронного оборудования?
22. Дайте определение цифровизации и проведите сравнительный анализ понятий информатизация и цифровизация.
23. Дайте определение научного подхода и перечислите совокупность научных подходов, которые необходимо интегрировать для решения поставленных зада, пример.
24. Дайте характеристику функциональному подходу и опишите возможности его применения при решении выбранной задачи.
25. Дайте сравнительную характеристику программно-целевого подхода к проектированию КОИБ на предприятии.
26. Основное назначение инженерных методов защиты информации.
27. Основное назначение программных методов защиты информации.
28. Какое проектное решение можно считать эффективным?
29. Что такое неопределенность в информационной безопасности?
30. Что такое риск в информационной безопасности?
31. Как предотвратить риск информационной безопасности?

32. Какие нормативные документы направлены на снижение неопределенности и риска
33. Противодействие несанкционированному доступу к данным сторонних сотрудников предприятия: привести примеры рисковых ситуаций и угроз.
34. Перечислить математические методы, направленные на снижение неопределенности и риска в информационной безопасности.
35. Какие управленческие методы принятия проектных решений можно порекомендовать для реализации деятельности КОИБ?

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине:

- защита курсового проекта;
- экзамен (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Устно-письменная форма по билетам предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов к защите курсового проекта
ОПК-2: ИОПК-2.2; ПК-3: ИПК-3.1, ИПК-3.2; ПК-4: ИПК-4.3

1. Основная цель курсового проекта. Каковы исходные данные?
2. Актуальность темы проекта
3. Применяемые методы исследования
4. Методы и инструменты, используемые при выполнении курсового проекта
5. Информационные технологии, используемые при выполнении курсового проекта
6. Этапы выполнения курсового проекта
7. Практическая значимость работы

Перечень вопросов и заданий для подготовки к экзамену

ОПК-2: ИОПК-2.2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

1. Какие основные компоненты входят в понятие комплексного обеспечения информационной безопасности (КОИБ)?
2. Каким образом определяется сущность комплексного обеспечения информационной безопасности?
3. Какие принципы лежат в основе комплексного обеспечения информационной безопасности?
4. Какие цели и задачи ставит перед собой комплексное обеспечение информационной безопасности?
5. Какие принципиальные отличия между комплексным и частным обеспечением информационной безопасности?
6. Какие проблемы решает комплексное обеспечение информационной безопасности?
7. Какие методы и подходы используются в рамках комплексного обеспечения информационной безопасности?
8. Каким образом комплексное обеспечение информационной безопасности взаимодействует с другими системами и процессами в организации?
9. Какие технологии и инструменты чаще всего применяются в комплексном обеспечении информационной безопасности?
10. Какие риски и угрозы могут быть устранены или снижены с помощью комплексного обеспечения информационной безопасности?

11. Каким образом комплексное обеспечение информационной безопасности способствует защите конфиденциальности, целостности и доступности данных?
12. Какие этапы включает в себя процесс разработки комплексного обеспечения информационной безопасности?
13. Каким образом оценивается эффективность комплексного обеспечения информационной безопасности?
14. В каком документе ФСТЭК РФ регламентируются требования к организации защиты информации, содержащейся в информационной системе?
15. На основании чего осуществляется разработка системы защиты информации информационной системы?
16. Какие этапы работ включает в себя разработка концепции информационной системы в соответствие с ГОСТ 34.601?
17. Какие этапы работ включает в себя разработка технического проекта информационной системы в соответствие с ГОСТ 34.601?
18. Опишите определение комплексной системы защиты информации.
19. Что включают в себя организационно-правовые мероприятия по защите информации?
20. Что представляет собой семирубежная модель защиты информации?

ПК-3: ИПК-3.1, ИПК-3.2. Способен оценить угрозы безопасности информации автоматизированной системы и обосновать необходимость её защиты

21. Из каких этапов состоит процесс оценки угроз безопасности информации?
22. Что включает в себя этап определения негативных последствий при оценке угроз информационной безопасности?
23. Что включает в себя этап определения объектов воздействия при оценке угроз информационной безопасности?
24. Что включает в себя этап оценки реализации угроз и определение их актуальности при оценке угроз информационной безопасности?
25. Какие системы управления базами данных соответствуют 6 классу защиты?
26. Какие системы управления базами данных соответствуют 5 классу защиты?
27. Какие системы управления базами данных соответствуют 4 классу защиты?
28. Какие исходные данные используются для определения негативных последствий от реализации угроз безопасности информации?
29. Какие существуют нарушители информационной безопасности в зависимости от уровня их возможностей?
30. В каких случаях возможна угроза безопасности информации по определению?
31. Что относится к программно-аппаратным средствам защиты информации по определению?
32. Что можно назвать уязвимостью в системе информационной безопасности по определению?
33. Что является границей оценки угроз безопасности информации?
34. Каких экспертов рекомендуется включать в состав экспертной группы для оценки угроз безопасности информации?
35. В отношении каких параметров оценки угроз информационной безопасности рекомендуется проводить экспертную оценку?
36. Какие методы оценки угроз безопасности информации вы знаете?
37. В чём сущность метода угроз и уязвимостей (Threat and Vulnerability Assessment, TVA)?
38. В чём заключается метод пентестинга?
39. Какие инструменты применяются для анализа уязвимостей системы?
40. Какие шаги вы предпримете для обоснования необходимости защиты информации в вашей автоматизированной системе?
41. Каковы основные угрозы безопасности информации, с которыми сталкиваются автоматизированные системы?
42. Какие методы защиты информации вы бы рекомендовали для минимизации угроз безопасности в автоматизированных системах?
43. Как вы определяете критические активы и данные, требующие особой защиты?

44. Какие действия вы бы предприняли для обнаружения потенциальных угроз безопасности информации?
45. Как оценить эффективность мер безопасности, принятых для защиты информации в системе?
46. Какие технологии и методы шифрования информации используются для обеспечения безопасности данных?
47. Каков процесс анализа уязвимостей и угроз безопасности перед внедрением новых компонентов в автоматизированную систему?
48. Какие меры предосторожности существуют для защиты информации от внутренних угроз?
49. Какие средства мониторинга безопасности используют для оперативного обнаружения инцидентов?
50. Как проводится анализ последствий возможных нарушений безопасности информации в системе?

ПК-4: ИПК-4.3. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных

51. Какие основные принципы следует учитывать при разработке архитектуры системы защиты информации?
52. Какие стадии включает процесс разработки архитектуры системы защиты информации?
53. Что представляет собой архитектура системы информационной безопасности?
54. Каким базовым принципам должна соответствовать оптимальная система информационной безопасности?
55. Какие средства являются основными компонентами системы информационной безопасности?
56. Какие виды обеспечения информационно-вычислительной системы, необходимы для создания и поддержания функционирования системы защиты информации?
57. В чём заключается основная цель архитектуры системы безопасности?
58. Каковы основные задачи архитектуры системы безопасности?
59. В чём заключается принцип построения архитектуры системы безопасности «защиты в глубину»?
60. В чём заключается принцип построения архитектуры системы безопасности «минимизации привилегий»?
61. В чём заключается принцип построения архитектуры системы безопасности «разделения обязанностей»?
62. В чём заключается принцип построения архитектуры системы безопасности «аутентификации и авторизации»?
63. В чём заключается принцип построения архитектуры системы безопасности «непрерывности работы»?
64. В чём заключается принцип построения архитектуры системы безопасности «постоянного обновления и адаптации»?
65. Какова особенность архитектуры системы безопасности «Периметр»?
66. Какова особенность архитектуры системы безопасности «Защита по уровням»?
67. Какова особенность архитектуры системы безопасности «Централизованная»?
68. Какова особенность архитектуры системы безопасности «Распределенная»?
69. В чём заключается процесс анализа уязвимостей ИС?
70. Какие методы анализа уязвимостей можно выделить в сфере информационной безопасности?
71. Какие минимальные требования защиты от несанкционированного доступа к данным устанавливает документация ФСТЭК РФ?
72. Как обеспечить совместимость новой модели защиты информации с уже существующими системами и приложениями?
73. В чём особенность автоматизированной системы в защищенном исполнении?

74. Как осуществляется защита информации от утечки по техническим каналам утечки информации?
75. Какие мероприятия по защите от утечки по техническим каналам утечки информации относятся к организационным?
76. Какие мероприятия по защите от утечки по техническим каналам утечки информации относятся к техническим мероприятиям с использованием пассивных средств защиты информации?
77. Какие мероприятия по защите от утечки по техническим каналам утечки информации относятся к техническим мероприятиям с использованием активных средств защиты информации?
78. Как провести анализ эффективности мер по предотвращению угроз безопасности информации в рамках модели защиты данных?
79. Какие этапы разработки системы защиты информации выделяют на предпроектной стадии и стадии проектирования?
80. Какие этапы разработки системы защиты информации выделяют на стадии ввода в эксплуатацию?