Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 11 » апреля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Основы информационной безопасности
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: специалитет
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 27.05.01 Специальные организационно-технические системы
(код и наименование направления)

Направленность: Информационные технологии и программное обеспечение в специальных организационно-технических системах
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель - изучение принципов обеспечения информационной безопасности и защиты информации, подходов к анализу угроз безопасности информационных систем и освоение компетенций для решения основных задач защиты информации в информационных системах

Задачи дисциплины:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации;
- приобретение навыков анализа информационной инфраструктуры с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

1.2. Изучаемые объекты дисциплины

основные понятия, общеметодологические принципы теории информационной безопасности;
- основы государственной информационной политики по обеспечению безопасности информации;
- виды информации ограниченного доступа;
- угрозы безопасности информации и уязвимости информационных систем;
- информационные войны и информационное оружие;
- методы нарушения конфиденциальности, целостности и доступности информации;
- причины, виды каналы утечки информации и несанкционированного доступа;
- формальные модели безопасности информации;
- уровни и сервисы защиты информации;
- способы и средства защиты информации;
- критерии оценки защищенности информационных систем;
- основы организации защиты информации на предприятии.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-5	ИД-1ОПК-5	Знает основы правовой защиты информации, интеллектуальных прав для выявления, учета, обеспечения правовой охраны результатов интеллектуальной деятельности и распоряжения ими.	Знает основы интеллектуальных прав для выявления, учета, обеспечения правовой охраны результатов интеллектуальной деятельности и распоряжения ими	Отчёт по практическому занятию
ОПК-5	ИД-2ОПК-5	Умеет пользоваться правовыми основами защиты интеллектуальных прав для выявления, учета, обеспечения правовой охраны результатов интеллектуальной деятельности и распоряжения ими, в том числе в целях практического применения.	Умеет пользоваться основами интеллектуальных прав для выявления, учета, обеспечения правовой охраны результатов интеллектуальной деятельности и распоряжения ими, в том числе в целях практического применения	Отчёт по практическому занятию
ОПК-5	ИД-3ОПК-5	Владеет навыками использования информационно-правовых систем, предварительного проведения патентных исследований и патентного поиска в целях реализации своих информационных прав.	Владеет навыками предварительного проведения патентных исследований и патентного поиска	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		2
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	24	24
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	27	27
- контроль самостоятельной работы (КСР)	3	3
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	54	54
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
2-й семестр				
Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	2	0	2	4
Основные составляющие национальных интересов Российской Федерации в ин-формационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в инфор¬мационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Основные понятия и общеметодологические принципы теории информационной безопасности	2	0	2	4
Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности.				
Понятие и виды защищаемой информации.	2	0	2	4
Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.				
Понятие и виды угроз информационной безопасности	2	0	2	4
Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации.				
Информационная безопасность и информационное противоборство	2	0	2	4
Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Информационная война как способ воздействия на информационные системы различного назначения и объекты критической информационной инфраструктуры				
Уровни и сервисы защиты информации в информационных системах	2	0	2	4
Единые критерии безопасности информационных технологий. Законодательный, административный, процедурный уровни информационной безопасности. Содержание сервисов безопасности				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.				
Формальные модели безопасности автоматизированных систем	2	0	2	6
Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом.				
Способы и средства защиты информации	2	0	4	4
Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности, DLP, SIEM-системы. Комплексные решения в обеспечении защиты информации, SOC-центры.				
Критерии оценки защищенности информационных систем	2	0	2	6
Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.				
Защита информации от технических разведок	2	0	2	4
Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем. Понятие и классификация видов технических разведок. Классификация технических каналов утечки информации. Способы и средства защиты				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
информации от утечки по техническим каналам.				
Защита информации криптографическими методами	2	0	2	6
Понятие криптографической защиты информации. Системы Шеннона. Типы и свойства шифров. Симметричные и асимметричные криптосистемы. Преобразование по схеме Фейстеля. Шифр DES, ГОСТ 28147-89. Алгоритм шифрования RSA.Управление криптографическими ключами. Протокол Kerberos. Криптографическая система □ Эл Гамаля. Понятие Хэш-функции. Инфраструктура открытых ключей (PKI). Средства криптографической защиты информации и электронной подписи. Криптографические средства защиты информации.				
Основы безопасности сетевых технологий	2	0	3	4
Базовая эталонная модель взаимодействия открытых систем (OSI). Уровни и основные протоколы сетевого взаимодействия. Концепция сетевых зон. Протокол IPsec. VPN. Типы брандмауэров и принципы фильтрации трафика. Системы обнаружения/предотвращения вторжений (IDS/IPS). Защита Web-приложений.				
ИТОГО по 2-му семестру	24	0	27	54
ИТОГО по дисциплине	24	0	27	54

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере (СЗ)
2	Основные понятия и общеметодологические принципы теории информационной безопасности (СЗ)
3	Определение видов информации ограниченного доступа и состава защищаемой информации (ПЗ)
4	Угрозы безопасности информации и разработка модели угроз информационной безопасности(ПЗ)
5	Информационная безопасность и информационное противоборство (СЗ)
6	Уровни и сервисы защиты информации в информационных системах (СЗ)
7	Формальные модели безопасности автоматизированных систем (ПЗ)
8	Способы и средства защиты информации (ПЗ)
9	Методы и критерии оценки защищенности информационных систем (ПЗ)
10	Защита информации от технических разведок (СЗ)

№ п.п.	Наименование темы практического (семинарского) занятия
11	Защита информации криптографическими методами (ПЗ)
12	Защита информации при сетевом взаимодействии (ПЗ)

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Галатенко В. А. Основы информационной безопасности : учебное пособие для вузов / В. А. Галатенко. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2008.	5

2	Галатенко В. А. Основы информационной безопасности : учебное пособие для вузов / В. А. Галатенко. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2010.	1
3	Галатенко В. А. Основы информационной безопасности : учебное пособие для вузов / В. А. Галатенко. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2012.	2
4	Данилов А. Н. Основы информационной безопасности : учебное пособие / А. Н. Данилов, С. А. Данилова, А. А. Зорин. - Пермь: Изд-во ПГТУ, 2008.	62
5	Основы информационной безопасности : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол: ТНТ, 2017.	2
6	Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов [и др.]. - Москва: Горячая линия-Телеком, 2011.	2
7	Цирлов В. Л. Основы информационной безопасности : краткий курс / В. Л. Цирлов. - Ростов-на-Дону: Феникс, 2008.	9
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Завгородний В. И. Комплексная защита информации в компьютерных системах : учебное пособие для вузов / В. И. Завгородний. - Москва: Логос, 2001.	27
2	Рагозин Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. - Санкт-Петербург: ИЦ Интермедия, 2018.	4
3	Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - Москва: ДМК Пресс, 2017.	3
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Основы информационной безопасности и защиты информации	https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1	сеть Интернет; свободный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный компьютер	10

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине
«Основы информационной безопасности»
Приложение к рабочей программе дисциплины

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (2-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим заданиям и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ПЗ**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знать основы интеллектуальных прав для выявления, учета, обеспечения правовой охраны результатов интеллектуальной деятельности и распоряжения ими.		ТО1	ПЗ1	Т		ТВ
Освоенные умения						
У.1 Уметь пользоваться основами интеллектуальных прав для выявления, учета, обеспечения правовой охраны результатов интеллектуальной деятельности и распоряжения ими, в том числе в целях практического применения.			ПЗ 2 ПЗ 3	Т		ПЗ
Приобретенные владения						
В.1 Владеть навыками предварительного проведения патентных исследований и патентного поиска			ПЗ 4 ПЗ 5 ПЗ 6 ПЗ 7	Т		КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в журнал преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

Вопросы для самостоятельного изучения:

Тема 1. Проблемы региональной информационной безопасности.

Тема 2. Общеметодологические принципы теории информационной безопасности.

Тема 3. Основные понятия информационной безопасности.

Тема 4. Понятие интеллектуальной собственности и особенности ее защиты.

Тема 5. Основные элементы канала реализации угрозы безопасности информации.

Тема 6. Информационная война как способ воздействия на информационные системы различного назначения и объекты критической информационной инфраструктуры.

Тема 7. Туннелирование, как сервис информационной безопасности.

Тема 8. Ролевое управление доступом.

Тема 9. Комплексные решения в обеспечении защиты информации, SOC-центры.

Тема 10. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

Тема 11. Средства криптографической защиты информации и электронной подписи.

Тема 12. Системы обнаружения/предотвращения вторжений (IDS/IPS).

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 7 практических занятий. Темы практических занятий приведены в РПД.

Отчет по выполнению практического задания проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Стратегия национальной безопасности Российской Федерации. Стратегические национальные приоритеты обеспечения национальной безопасности РФ.

2. Доктрина информационной безопасности Российской Федерации. Национальные интересы РФ в информационной сфере.

3. Основные угрозы информационной безопасности РФ и основные направления по обеспечению информационной безопасности РФ.

4. Роль специалиста по защите информации в обеспечении национальной безопасности государства.

5. Основные понятия информационной безопасности и их источники.

6. Общеметодологические принципы теории информационной безопасности.

7. Понятие и сущность информации ограниченного доступа. Особенности доступа и ограничения доступа к информации.

8. Права и обязанности обладателя информации.

9. Виды информации ограниченного доступа. Перечень сведений конфиденциального характера.

10. Понятие интеллектуальной собственности и особенности ее защиты.

11. Понятие угрозы безопасности информации.

12. Факторы, воздействующие на информацию. Типы дестабилизирующих факторов.

13. Классификация и виды угроз информационной безопасности.

14. Внутренние и внешние источники угроз безопасности информации.

15. Угрозы утечки информации и угрозы несанкционированного доступа.

16. Основные элементы канала реализации угрозы безопасности информации.

17. Субъекты и цели информационного противоборства.

18. Способы, принципы и стадии информационного противоборства.

19. Информационное оружие, его классификация и возможности.

20. Информационная война как способ воздействия на информационные системы.

21. Использования социальных сетей в информационных войнах.

22. Информационная безопасность объектов критической информационной инфраструктуры.

23. Использование кибернетического оружия в информационной войне.

24. Автоматизированная система, как объект информационной безопасности.

25. Уровни информационной безопасности объекта оценки информационных технологий.

26. Характеристика законодательного, административного и процедурного уровней информационной безопасности.

27. Перечень сервисов безопасности программно-технического уровня.

28. Идентификация и аутентификация как сервисы безопасности.

29. Управление доступом и его виды. Авторизация как сервис безопасности.

30. Протоколирование, аудит и управление, как сервисы безопасности.

31. Экранирование, туннелирование и анализ защищенности как сервисы безопасности.

32. Назначение формальных моделей безопасности. Варианты моделей защиты и сущность политики безопасности.

33. Дискреционная модель безопасности и ее особенности на примере модели Харрисона-Руззо-Ульмана.

34. Мандатная модель безопасности ее особенности на примере модели Белла-Лападулы.

35. Формальные модели целостности.

36. Ролевое управления доступом.

37. Основные способы защиты информации и их характеристика.

38. Понятие и классификация средств защиты информации. Техника защиты информации.

39. Средства физической, криптографической и программно-технической защиты информации.

40. Перечень и характеристика разновидностей современных средств защиты информации.

41. Критерии оценки безопасности компьютерных систем «Оранжевая книга».

42. Требования к средствам вычислительной техники (СВТ) и автоматизированным системам (АС) по защите информации от НСД.

43. Общие критерии безопасности информационных технологий.

44. Основные руководящие документы ФСТЭК России, определяющие требования по защите информации.

45. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

46. Понятие и классификация видов технических разведок.

47. Классификация технических каналов утечки информации. Структура канала утечки информации.

48. Способы и основные средства защиты информации от утечки по техническим каналам.

49. Характеристика организационных и технических мер по защите от утечки информации.

50. Криптография и криптографическая защита информации. Основные понятия.

51. Классификация шифров. Принцип симметричного и асимметричного шифрования.

52. Алгоритм преобразования по схеме Фейстеля.

53. Примеры симметричных криптографических систем. Шифр DES. Шифр ГОСТ 28147-89.

54. Примеры криптографических систем с открытым ключом. Криптографическая система RSA.

55. Управление криптографическими ключами. Протокол Kerberos.

56. Распределение ключей по схеме Диффи-Хеллмана.

57. Криптографическая система Эль-Гамаля.

58. Понятие и классы Хэш-функции. Алгоритм SHA-1

59. Инфраструктура открытых ключей (PKI).

60. Средства шифрования и электронной подписи. Виды и классификация электронных подписей.

Типовые практические задания для контроля освоенных умений:

1. Определить виды информации ограниченного доступа, обрабатываемые на объекте информатизации.
2. Определить состав носителей информации ограниченного доступа.
3. Изучить порядок формирования и структуру Базы данных (список) уязвимостей информационных систем.
4. Проанализировать деятельность организации (предприятия), выявить уязвимости информационной системы.
5. Классифицировать состав угроз информационной безопасности.
6. Определить состав характерных угроз информационной безопасности для автоматизированной системы.
7. Определить содержание административного уровня обеспечения информационной безопасности (перечислить основные нормативные документы, которые разрабатываются на объекте информатизации и обеспечивают его информационную безопасность).
8. Определить содержание процедурного уровня обеспечения информационной безопасности предприятия (перечислить применяемые процедурные меры).
9. Определить состав применяемых сервисов безопасности программно-технического уровня для варианта автоматизированной системы, с учетом особенностей объекта информатизации.
10. Сформировать матрицу (оформить рисунок) полномочий доступа для варианта информационной системы. При условии большого количества пользователей – фрагмент матрицы.
11. Оптимизировать состав матрицы управления доступа за счет введения ролевого управления доступом.
12. Сформировать перечень основных мер по обеспечению безопасности информации для ИСПДн 1,2,3,4 УЗ.
13. Предложить состав мер по противодействию утечке информации на объекте информатизации.
14. Выполнить практическое задание по реализации функции шифрования, с использованием ОС Windows.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.