ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом ректора
от «08» мая 2020 г. № 266-1

Б1.Б.1.22 Основы информационной безопасности

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма обучения – очная
Нормативный срок обучения – 5 лет
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 4
Часов по учебному плану – 144

Формы промежуточной аттестации в семестрах:
экзамен 3, курсовая работа 3

Распределение часов дисциплины в семестре

Семестр	3	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**54**	**54**
– лекции	18	18
– практические (семинарские)	36	36
Самостоятельная работа	**54**	**54**
Экзамен	**36**	**36**
Итого	**144**	**144**

ИРКУТСК

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.
1.2 Задачи освоения дисциплины	
1	изучить основные положения государственной политики в области обеспечения информационной безопасности Российской Федерации, основные понятия в области защиты информации и методологических принципов создания систем защиты информации
2	изучить виды защищаемой информации, угроз информационной безопасности, методов и средств обеспечения информационной безопасности, механизмов защиты информации, моделей безопасности, критериев оценки защищенности и обеспечения безопасности информационных систем
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	
Научно-образовательное воспитание обучающихся	
Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества. Цель достигается по мере решения в единстве следующих задач: – формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности; – создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками; – популяризация научных знаний среди обучающихся; – содействие повышению привлекательности науки, поддержка научно-технического творчества; – создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества; – совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.В.ДВ.05.01 Введение в специальность
2	Б1.Б.1.07 Алгебра и геометрия
3	Б1.Б.1.02 История
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.Б.1.30 Управление информационной безопасностью
2	Б1.Б.1.27 Организационное и правовое обеспечение информационной безопасности
3	Б1.В.06 Комплексная защита в информационных системах персональных данных
4	Б2.Б.01(У) Учебная - учебно-лабораторный практикум
5	Б2.Б.02(П) Производственная - по получению профессиональных умений и опыта профессиональной

	деятельности

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

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
Минимальный уровень освоения компетенции	
Знать	Основы определения ценности информации
Уметь	Решать задачи по определению ожидаемого ущерба от утраты информации
Владеть	Навыками сбора и обработки информации
Базовый уровень освоения компетенции	
Знать	Основные подходы к определению экономики защиты информации
Уметь	Решать задачи по определению ценности информации
Владеть	Методиками решения задач
Высокий уровень освоения компетенции	
Знать	Основные методы определения ценности информации
Уметь	Определять эффективность затрат по защите информации
Владеть	Способами проведения комплексных научных исследований

ПК–4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Минимальный уровень освоения компетенции	
Знать	Сущность и понятие информации, информационной безопасности и характеристику ее составляющих
Уметь	Анализировать и оценивать угрозы информационной безопасности объекта
Владеть	Профессиональной терминологией в области информационной безопасности
Базовый уровень освоения компетенции	
Знать	Источники и классификацию угроз информационной безопасности
Уметь	Разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем
Владеть	Методами формирования требований по защите информации
Высокий уровень освоения компетенции	
Знать	Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации
Уметь	Разрабатывать частные политики информационной безопасности информационных систем
Владеть	Методологическими принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты

ПК–11: способность разрабатывать политику информационной безопасности автоматизированной системы	
Минимальный уровень освоения компетенции	
Знать	Сущность обобщения, анализа, восприятия информации, постановки цели и выбору путей ее достижения
Уметь	Обобщать, анализировать и воспринимать информацию при выборе и постановке цели
Владеть	Способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления
Базовый уровень освоения компетенции	
Знать	Методику анализа, восприятия информации, постановке цели и выбору путей ее достижения
Уметь	Применять современные достижения информатики и вычислительной техники
Владеть	Достижениями информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации
Высокий уровень освоения компетенции	
Знать	Методы анализа изучаемых явлений, процессов и проектных решений
Уметь	Использовать большие объемы информации проводить целенаправленный поиск в различных источниках информации
Владеть	Основными закономерностями и правилами перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации

В результате освоения дисциплины обучающийся должен

Знать	
1	сущность и понятие информации информационной безопасности и характеристику ее составляющих
2	место и роль информационной безопасности в системе национальной безопасности Российской Федерации
3	основы государственной информационной политики, стратегию развития формационного общества в России
4	источники и классификацию угроз информационной безопасности
5	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации
Уметь	
1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
2	классифицировать и оценивать угрозы информационной безопасности для объектов информатизации
Владеть	
1	специальной профессиональной терминологией
2	основными элементами защиты информации

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
1.0	**Раздел 1. Теория информационной безопасности**				
1.1	Введение /Лек/	3	2	ОК–5	Л1.1, Л2.3 Э1, Э2
1.2	Сущность и понятие информационной безопасности /Лек/	3	2	ОК–5	Л1.2, Л2.2 Э1
1.3	Проработка лекционного материала по теме «Сущность и понятие информационной безопасности» /Ср/	3	2	ОК–5	Л1.2, Л2.1 Э2
1.4	Значение информационной безопасности и ее место в системе национальной безопасности /Пр/	3	2	ОК–5	Л1.3, Л2.3 Э2
1.5	Современная Доктрина информационной безопасности Российской Федерации /Лек/	3	2	ПК–4, ПК–11	Л1.1, Л2.3 Э1,
1.6	Проработка лекционного материала, подготовка к семинарскому занятию по теме «Современная Доктрина информационной безопасности Российской Федерации» /Ср/	3	2	ПК–4, ПК–11	Л1.2, Л2.1 Э1, Э2
1.7	Современная Доктрина информационной безопасности Российской Федерации /Пр/	3	2	ПК–4, ПК–11	Л1.2, Л.1.3, Л2.3 Э1, Э2
2.0	**Раздел 2. Методология защиты информации**				
2.1	Сущность и понятие защиты информации /Лек/	3	2	ПК–4	Л1.1, Л1.2, Л2.2 Э1, Э2
2.2	Проработка лекционного материала по теме «Сущность и понятие защиты информации» /Ср/	3	2	ПК–4	Л1.1, Л2.3 Э1, Э2
2.3	Цели и значение защиты информации /Пр/	3	2	ПК–4	Л1.1, Л1.2, Л2.2 Э1, Э2
2.4	Теоретические и концептуальные основы защиты информации /Лек/	3	2	ПК–11	Л1.1, Л1.3, Л2.1 Э1, Э2
2.5	Проработка лекционного материала и подготовка к семинарскому занятию по теме «Теоретические и концептуальные основы защиты информации» /Ср/	3	2	ПК–11	Л1.3, Л2.1 Э1, Э2
2.6	Теоретические и концептуальные основы защиты информации /Пр/	3	2	ПК–11	Л1.2, Л1.3, Л2.2 Э1, Э2
2.7	Организационные основы и методологические принципы защиты информации /Лек/	3	2	ПК–4	Л1.1, Л1.3, Л2.3 Э1, Э2

2.8	Проработка лекционного материала «Организационные основы и методологические принципы защиты информации» /Ср/	3	2	ОК–5	Л1.1, Л2.3, Л2.1 Э1, Э2
2.9	Современные факторы, влияющие на защиту информации /Пр/	3	2	ПК–4	Л1.2, Л2.2 Э1, Э2
2.10	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности /Лек/	3	2	ПК–11	Л1.2, Л1.3, Л2.3 Э1, Э2
2.11	Проработка лекционного материала по теме «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности» /Ср/	3	2	ПК–11	Л1.3, Л2.3 Э1, Э2
2.12	Критерии, условия и принципы отнесения информации к защищаемой /Пр/	3	2	ПК–11	Л1.2, Л2.2 Э1, Э2
2.13	Каналы и методы несанкционированного доступа к конфиденциальной информации /Лек/	3	2	ПК–4	Л1.1, Л1.3, Л2.3 Э1, Э2
2.14	Подготовка к семинарскому занятию по теме «Состав и классификация носителей защищаемой информации» /Ср/	3	2	ПК–4	Л1.1, Л1.2, Л2.1 Э1, Э2
2.15	Состав и классификация носителей защищаемой информации /Пр/	3	2	ПК–4	Л1.2, Л2.1, Л2.2 Э1, Э2
2.16	Классификация видов, методов и средств защиты информации /Лек/	3	2	ОК–5	Л1.2, Л1.3, Л2.2 Э1, Э2
2.17	Проработка лекционного материала по теме «Классификация видов, методов и средств защиты информации» /Ср/	3	2	ОК–5	Л1.1, Л1.3, Л2.1 Э1, Э2
2.18	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности /Пр/	3	1	ОК–5	Л1.2, Л1.3, Л2.3 Э1, Э2
2.19	подготовка к семинарскому занятию по теме «Классификация защищаемой информации по собственникам и владельцам» /Ср/	3	2	ОК–5	Л1.1, Л1.2, Л2.1 Э1, Э2
2.20	Классификация защищаемой информации по собственникам и владельцам /Пр/	3	1	ОК–5	Л1.1, Л1.3, Л2.1 Э2
2.21	подготовка к семинарскому занятию по теме «Понятие и структура угроз защищаемой информации» /Ср/	3	2	ОК–5	Л1.1, Л1.2, Л2.1 Э1, Э2
2.22	Понятие и структура угроз защищаемой информации /Пр/	3	1	ПК–11	Л1.2, Л1.3, Л2.3 Э1, Э2
2.23	подготовка к семинарскому занятию по теме «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию» /Ср/	3	2	ПК–11	Л1.1, Л1.2, Л2.2, Л2.3 Э1, Э2
2.24	Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию /Пр/	3	1	ПК–11	Л1.3, Л2.1, Л2.2, Л2.3 Э1, Э2
2.25	подготовка к семинарскому занятию по теме «Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию» /Ср/	3	2	ПК–4	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.26	Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию /Пр/	3	2	ПК–4	Л1.2, Л1.3, Л2.1, Л2.3 Э1, Э2
2.27	подготовка к семинарскому занятию по теме «Каналы и методы несанкционированного доступа к конфиденциальной информации» /Ср/	3	2	ПК–4	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.28	Каналы и методы несанкционированного доступа к конфиденциальной информации /Пр/	3	2	ПК–4	Л1.3, Л2.1, Л2.2, Л2.3 Э1, Э2
2.29	подготовка к семинарскому занятию по	3	2	ОК-5	Л1.1, Л1.2,

	теме «Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации» /Ср/				Л2.2, Л2.3 Э1, Э2
2.30	Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации /Пр/	3	2	ОК-5	Л1.1, Л1.3, Л2.1, Л2.2, Э1, Э2
2.31	подготовка к семинарскому занятию по теме «Объекты защиты информации» /Ср/	3	2	ОК-5	Л1.1, Л1.3, Л2.1, Л2.2, Э1, Э2
2.32	Объекты защиты информации /Пр/	3	2	ОК-5	Л1.1, Л1.2, Л2.2, Л2.3 Э1, Э2
2.33	подготовка к семинарскому занятию по теме «Кадровое и ресурсное обеспечение защиты информации» /Ср/	3	2	ОК-5	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.34	Кадровое и ресурсное обеспечение защиты информации /Пр/	3	2	ОК-5	Л1.3, Л2.1, Л2.2, Л2.3 Э1, Э2
2.35	подготовка к семинарскому занятию по теме «Технологическое обеспечение защиты информации» /Ср/	3	2	ПК–11	Л1.1, Л1.2, , Л2.1, Л2.3 Э1, Э2
2.36	Технологическое обеспечение защиты информации /Пр/	3	2	ПК–11	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.37	подготовка к семинарскому занятию по теме «Назначение и структура систем защиты информации» /Ср/	3	2	ПК–11	Л1.1, Л1.2, Л2.2, Л2.3 Э1, Э2
2.38	Назначение и структура систем защиты информации /Пр/	3	2	ПК–11	Л1.3, Л2.1, Л2.2, Л2.3 Э1, Э2
2.39	Проработка теоретической части курсовой работы /Ср/	3	8	ОК–5	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.40	Разработка практической части курсовой работы /Ср/	3	10	ОК–5	Л1.1, Л1.2, Л2.2, Э1, Э2
2.41	Защита курсовой работы /Пр/	3	4	ОК–5	Л1.1, Л1.2, Л1.3, Л2.1,
3.0	**Форма промежуточной аттестации - экзамен**	3	36	ОК–5, ПК–4, ПК–11	Л1.1, Л1.2, Л1.3, Л2.1, Л2.2, Л2.3 Э1, Э2

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплины и размещаются в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн

Л1.1	С.А. Нестеров	Основы информационной безопасности: учебное пособие [Электронный ресурс] //e.lanbook.com/book/90153	СПб:Издательство Лань, 2017	100% онлайн
Л1.2	М.А. Лапина, А.Г. Ревин, В.И. Лапин	Информационное право: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=685428	М. : Юнити-Дана, 2017	100% онлайн
Л1.3	О.В. Порядина	Управление информационными ресурсами: учебно-методическое пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=439328	Йошкар-Ола: ПГТУ, 2015	100% онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др	Организация безопасной работы информационных систем: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=277794	Издательство ФГБОУ ВПО «ТГТУ, 2014	100% онлайн
Л2.2	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации : учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=276557	- М. ; Берлин : Директ-Медиа, 2015	100% онлайн
Л2.3	Аверченков, В.И.	Служба защиты информации: организация и управление: учебное пособие для вузов [Электронный ресурс] biblioclub.ru/index.php?page=book&id=93356	М. : Флинта, 2011	100% онлайн
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия: учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с	- Иркутск: ИрГУПС, 2013	55
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Середкин С.П.	Материалы для самостоятельной работы студентов	Личный кабинет обучающегося	100% онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Федеральная служба по техническому и экспортному контролю, www.fstec.ru			
Э.2	СЗИ от НСД Secret Net, СКрипт3И М-506А-ХР, www.securitycode.ru			
6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)				
6.3.1 Перечень базового программного обеспечения				
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01; Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01; FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/; Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/; Яндекс.			

	Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License
6.3.2 Перечень специализированного программного обеспечения	
6.3.2.1	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01; Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html; Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/; MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01; MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01
6.3.3 Перечень информационных справочных систем	
6.3.3.1	«Консультант +» http://www.consultant.ru/
6.3.3.2	«Техэксперт» http://www.cntd.ru
6.4 Перечень правовых и нормативных документов	
6.4.1	Не предусмотрено

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

7.1	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации).
7.2	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
7.3	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.
7.4	Помещение А-521 (для хранения и профилактического обслуживания учебного оборудования).

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее

	самостоятельно выполнить задание на самостоятельную работу и выучить лекционный материал к следующей теме. Систематическое выполнение заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины.
Реферат	Реферат – краткое письменное изложение материала по определенной теме, выполняется; цель – привить обучающимся навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу. Реферат – это самостоятельная учебно-исследовательская работа обучающегося, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер. Ознакомиться со структурой и оформление реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Курсовая работа	Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме. Инструкция по выполнению требований к оформлению курсовой работы (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Самостоятельная работа	Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим занятиям, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Приложение 1 к рабочей программе по дисциплине
Б1.Б.1.22 «Основы информационной безопасности»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.Б.1.22 «Основы информационной безопасности»

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дисциплина «Основы информационной безопасности» участвует в формировании компетенций:

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

ПК-4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК-11: способность разрабатывать политику информационной безопасности автоматизированной системы

Таблица траекторий формирования у обучающихся компетенций ОК-5, ПК-4, ПК-11 при освоении образовательной программы

Код компе-тенции	Наименование компетенции	Индекс и наименование дисциплин / практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Б1.Б.1.32 Культурология	1	1
		Б1.Б.1.22 Основы информационной безопасности	3	2
		Б1.В.ДВ.05.01 Введение в специальность	3	2
ПК-4	способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Б1.Б.1.22 Основы информационной безопасности	3	1
		Б1.В.05 Методология анализа информационных рисков	8	2
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	3
		Б2.Б.04(Н) Производственная - научно-исследовательская работа	А	4
		Б2.Б.06(Пд) Производственная - преддипломная	А	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	4
ПК-11	способность разрабатывать политику информационной безопасности автоматизированной системы	Б1.Б.1.22 Основы информационной безопасности	3	1
		Б1.В.04 Теоретические основы компьютерной безопасности	56	2
		Б1.В.ДВ.04.01 Защита электронного документооборота	9	3
		Б1.В.ДВ.04.02 Защита и обработка	9	3

		конфиденциальных документов		
		Б2.Б.06(Пд) Производственная - преддипломная	А	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	4

Таблица соответствия уровней освоения компетенций ОК-5, ПК-4, ПК-11 планируемым результатам обучения

Код компе-тенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации	Минимальный уровень	Знать: основы определения ценности информации
				Уметь: решать задачи по определению ожидаемого ущерба от утраты информации
				Владеть: навыками сбора и обработки информации
			Базовый уровень	Знать: основные подходы к определению экономики защиты информации
				Уметь: решать задачи по определению ценности информации
				Владеть: методиками решения задач
			Высокий уровень	Знать: основные методы определения ценности информации
				Уметь: определять эффективность затрат по защите информации
				Владеть: способами проведения комплексных научных исследований
ПК-4	способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации	Минимальный уровень	Знать: сущность и понятие информации, информационной безопасности и характеристику ее составляющих
				Уметь: анализировать и оценивать угрозы информационной безопасности объекта
				Владеть: профессиональной терминологией в области информационной безопасности
			Базовый уровень	Знать: источники и классификацию угроз информационной безопасности
				Уметь: разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем
				Владеть: методами формирования требований по защите информации
			Высокий	Знать: основные средства и

			уровень	способы обеспечения информационной безопасности, принципы построения систем защиты информации
				Уметь: разрабатывать частные политики информационной безопасности информационных систем
				Владеть: методологическими принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты
ПК-11	способность разрабатывать политику информационной безопасности автоматизированной системы	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации	Минимальный уровень	Знать: сущность обобщения, анализа, восприятия информации, постановки цели и выбору путей ее достижения
				Уметь: обобщать, анализировать и воспринимать информацию при выборе и постановке цели
				Владеть: способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления
			Базовый уровень	Знать: методику анализа, восприятия информации, постановке цели и выбору путей ее достижения
				Уметь: применять современные достижения информатики и вычислительной техники
				Владеть: достижениями информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации
			Высокий уровень	Знать: методы анализа изучаемых явлений, процессов и проектных решений
				Уметь: использовать большие объемы информации проводить целенаправленный поиск в различных источниках информации
				Владеть: основными закономерностями и правилами перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации

Программа контрольно-оценочных мероприятий
за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
3 семестр					
1	1	Текущий контроль	Тема «Сущность и понятие информационной безопасности»	ОК–5	Реферат (письменно)
2	1	Текущий контроль	Тема «Значение информационной безопасности и ее место в системе национальной безопасности»	ОК–5	Доклад, сообщение (устно)
3	1-2	Текущий контроль	Тема «Современная Доктрина информационной безопасности Российской Федерации»	ПК-4, ПК–11	Реферат (письменно). Доклад, сообщение (устно)
4	2	Текущий контроль	Тема «Сущность и понятие защиты информации»	ПК-14	Реферат (письменно)
5	3	Текущий контроль	Тема «Цели и значение защиты информации»	ПК-14	Доклад, сообщение (устно)
6	3	Текущий контроль	Тема «Теоретические и концептуальные основы защиты информации»	ПК-11	Реферат (письменно). Доклад, сообщение (устно)
7	4	Текущий контроль	Тема «Организационные основы и методологические принципы защиты информации»	ОК–5	Реферат (письменно)
8	4	Текущий контроль	Тема «Современные факторы, влияющие на защиту информации»	ПК-4	Доклад, сообщение (устно)
9	4	Текущий контроль	Тема «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности»	ПК-11	Реферат (письменно)
10	5	Текущий контроль	Тема «Критерии, условия и принципы отнесения информации к защищаемой»	ПК-11	Доклад, сообщение (устно)
11	5-6	Текущий контроль	Тема «Состав и классификация носителей защищаемой информации»	ПК-4	Реферат (письменно). Доклад, сообщение (устно)
12	6	Текущий контроль	Тема «Классификация видов, методов и средств защиты информации»	ОК–5	Реферат (письменно)
13	6	Текущий контроль	Тема «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности»	ОК–5	Доклад, сообщение (устно)
14	7	Текущий контроль	Тема «Классификация защищаемой информации по собственникам и владельцам»	ОК–5	Реферат (письменно). Доклад, сообщение (устно)
15	8	Текущий контроль	Тема «Понятие и структура угроз защищаемой информации»	ОК–5, ПК-11	Реферат (письменно). Доклад, сообщение (устно)
16	9	Текущий контроль	Тема «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию»	ПК-11	Реферат (письменно). Доклад, сообщение (устно)
17	9-10	Текущий контроль	Тема «Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию» Тема «Каналы и методы несанкционированного доступа к конфиденциальной информации»	ПК-4	Реферат (письменно). Доклад, сообщение (устно)
18	11-12	Текущий контроль	Тема «Направления, виды и особенности деятельности	ОК–5	Реферат (письменно). Доклад, сообщение

			разведывательных служб по несанкционированному доступу к конфиденциальной информации» Тема «Объекты защиты информации»		(устно)
19	13	Текущий контроль	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации	ОК–5, ПК–4, ПК–11	Тестирование (компьютерные технологии)
20	14	Текущий контроль	Тема «Кадровое и ресурсное обеспечение защиты информации»	ОК–5	Реферат (письменно). Доклад, сообщение (устно)
21	15-16	Текущий контроль	Тема «Технологическое обеспечение защиты информации» Тема «Назначение и структура систем защиты информации»	ПК-11	Реферат (письменно). Доклад, сообщение (устно)
22	17	Текущий контроль	Защита курсовой работы	ОК–5, ПК–4, ПК–11	Курсовая работа (письменно, устно)
23	18	Промежуточная аттестация – экзамен	Разделы: Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации	ОК–5, ПК–4, ПК–11	Собеседование (устно). Тестирование (компьютерные технологии)

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

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Реферат	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор реферата раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Может быть использовано для оценки знаний и умений обучающихся	Темы рефератов

2	Доклад, сообщение	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
3	Тестирование	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	Курсовая работа	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Темы типовых групповых и / или индивидуальных работ и типовое задание на курсовую работу
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме экзамена, а также шкала для оценивания уровня освоения компетенций

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Реферат

Шкала оценивания	Критерии оценивания
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы
«удовлетворительно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Реферат обучающимся не представлен

Доклад, сообщение

Шкала оценивания	Критерии оценивания

«отлично»	Доклад создан с использованием компьютерных технологий (презентация Power Point, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация Power Point, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсовой работы в целом не соответствует заданию. Имеются более

	двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. Программа не разработана и/или находится в нерабочем состоянии. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала. курсовой работы не представлена преподавателю. Обучающийся не явился на защиту курсовой работы.

Тестирование

Критерии и шкала оценивания текущего контроля

Шкала оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»		Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»		Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«не удовлетворительно»	«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Результаты тестирования могут быть использованы при проведении промежуточной аттестации.

Критерии и шкала оценивания промежуточной аттестации в форме экзамена

Шкала оценивания	Критерии оценивания
«отлично»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»	Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»	Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«не удовлетворительно»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Перечень типовых тем рефератов

1. Структура государственной системы защиты информации (схема).
2. Система документации по технической защите информации (схема).
3. Действующие документы по защите информации с учетом категорий доступа к ней и видов информационных систем.
4. Определение информационной безопасности.
5. Определение защиты информации.
6. Меры по обеспечению информационной безопасности.
7. Основные организационно-технические мероприятиям по защите информации.
8. Источники угрозы информационной безопасности.
9. Угрозы информационной безопасности.
10. Уязвимости информационной безопасности.
11. Атаки информационной безопасности.

12. Построить логическую цепочку реализации угрозы информационной безопасности.
13. Построить схему классификации источников угроз ИБ.
14. Объективные уязвимости.
15. Субъективные уязвимости.
16. Случайные уязвимости.
17. Понятие лицензии (пользовательская лицензия).
18. Определение лицензионной политики.
19. Понятие коммерческой лицензии.
20. Понятие открытой лицензии.
21. Гарантируемые права открытой лицензии.
22. Понятие нелицензионного программного обеспечения.
23. Угрозы при использовании нелицензионного программного обеспечения.
24. Закон, определяющий правовые основы информационной безопасности (наименование, когда принят, основные требования).

3.2 Перечень типовых тем докладов, сообщений

1. Закон, определяющий требования к защите персональных данных (наименование, когда принят, основные требования).
2. Источники угроз утечки информации по техническим каналам.
3. Понятие побочных электромагнитных излучений и наводок.
4. Определение технического канала утечки информации.
5. Классификация ТКУИ.
6. Перечислить виды связи для передачи информации.
7. Виды аппаратуры для перехвата информации.
8. Перечень аппаратуры для перехвата речевой информации.
9. Стационарные средства для наблюдения за объектами на значительном расстоянии.
10. Классификация технических каналов утечки информации обрабатываемых техническими средствами передачи информации (ТСПИ).
11. Наименование технических каналов утечки информации (ТКУИ).
12. Необходимые действия при создании СЗКИ.
13. Стадии создания СЗКИ.
14. Этапы предпроектного обследования.
15. Техническое задание на разработку СЗКИ – содержание разделов.
16. Проектирование и создание ИСКИ (СЗКИ) - содержание разделов.
17. Этапы ввода в действие ИСКИ (СЗКИ).
18. Основной аспект назначения СЗКИ.
19. Требования к функционированию СЗКИ в условиях чрезвычайных ситуаций.

3.3 Перечень типовых тем курсовых работ

1. Виды и состав угроз информационной безопасности.
2. Задачи, принципы и методы обеспечения информационной безопасности.
3. Критерии, условия, принципы и формы отнесения информации к защищаемой.
4. Анализ существующих подходов к классификации конфиденциальной информации по видам тайны.
5. Виды и характеристика носителей защищаемой информации.
6. Структура и характеристика угроз защищаемой информации.
7. Соотношение угроз защищаемой информации с видами носителей и формами проявления уязвимости информации.
8. Соотношение видов разведывательной деятельности с каналами и методами несанкционированного доступа к конфиденциальной информации.

9. Классификация и характеристика объектов защиты информации.
10. Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.
11. Сущность, назначение и структура систем защиты информации.
12. Состав угроз информационной безопасности.
13. Методы обеспечения информационной безопасности.
14. Значение защиты информации во внешнеполитической деятельности.
15. Значение защиты информации в военной области.
16. Значение защиты информации в экономической сфере.
17. Социальные последствия защиты информации.
18. Влияние политико-правовых и социально-экономических реальностей на защиту информации.
19. Основные положения теории защиты информации.
20. Понятие и назначение концепции защиты информации.
21. Социально-экономические и организационно-правовые аспекты концепции защиты информации.
22. Требования к концепции защиты информации.
23. Уровни концепции защиты информации.
24. Понятие «носитель защищаемой информации». Способы фиксирования информации в носителях.
25. Свойства и значение типов носителей защищаемой информации. Соотношение видов носителей информации с категориями защищаемой информации и формами проявления ее уязвимости.
26. Показатели разделения конфиденциальной информации на виды тайны.
27. Общее и различия между степенью и грифом конфиденциальности (секретности).
28. Сферы действия государственной и служебной тайны.
29. Сферы действия коммерческой тайны.
30. Сферы действия личной и профессиональной тайны.
31. Формы собственности на информацию.
32. Собственники и владельцы информации, составляющей различные виды тайны.
33. Современные подходы к понятию угрозы защищаемой информации.
34. Признаки и составляющие угрозы защищаемой информации.
35. Состав и характеристика источников дестабилизирующего воздействия на информацию.
36. Виды и способы дестабилизирующего воздействия на информацию со стороны людей.
37. Виды и способы дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.
38. Соотношение видов дестабилизирующего воздействия на информацию с формами проявления уязвимости информации.
39. Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию.
40. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны людей.
41. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.
42. Соотношение каналов несанкционированного доступа к информации с каналами утечки информации.
43. Соотношение каналов несанкционированного доступа к информации с источниками дестабилизирующего воздействия на информацию.

44. Методы несанкционированного доступа к информации через допущенных к ней лиц.

45. Методы несанкционированного доступа к информации через агентуру.

46. Методы несанкционированного доступа к информации через средства обработки, передачи информации и системы обеспечения их функционирования.

47. Методы несанкционированного физического проникновения на защищаемый объект.

48. Соотношение методов несанкционированного доступа к информации с используемыми техническими средствами.

49. Органы политической, военной и радиотехнической разведки в США.

50. Органы политической и военной разведки ведущих стран Западной Европы.

51. Соотношение между видами и направлениями разведывательной деятельности.

52. Состав подлежащих защите объектов хранения информации.

53. Состав подлежащих защите технических средств изготовления, обработки, воспроизведения и передачи информации.

54. Виды и способы дестабилизирующего воздействия на объекты защиты информации.

55. Классификация видов защиты информации.

56. Классификация методов защиты информации.

57. Классификация программных и криптографических средств защиты информации.

58. Классификация технических средств защиты информации.

59. Полномочия руководства предприятия и служб защиты информации в области защиты информации.

60. Состав и значение ресурсного обеспечения защиты информации.

61. Состав и сферы действия систем защиты информации.

62. Сущность и значение комплексной системы защиты информации.

3.4 Типовые контрольные задания для тестирования

Структура фонда тестовых заданий по дисциплине
«Основы информационной безопасности»

Компетенция	Тема в соответствии с РПД/РПП (с соответствующим номером)	Содержательный элемент	Характеристика содержательного элемента	Количество тестовых заданий, типы ТЗ
ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Раздел 1. Теория информационной безопасности	1. Сущность информационной безопасности 2. Понятие информационной безопасности 3. Значение информационной безопасности и её место в системе национальной безопасности	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы		1. Современная доктрина информационной безопасности Российской Федерации 2. Стратегические цели и основные направления обеспечения информационной безопасности 3. Организационные основы обеспечения информационной безопасности	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-11: способность разрабатывать политику		1. Современная доктрина информационной	Знание	4 – ОТЗ 4 – ЗТЗ

информационной безопасности автоматизированной системы		безопасности Российской Федерации 2. Стратегические цели и основные направления обеспечения информационной безопасности 3. Организационные основы обеспечения информационной безопасности		
ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики		1. Организационные основы и методологические принципы защиты информации 2. Классификация видов, методов и средств защиты информации 3. Понятие и структура угроз защищаемой информации	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы		1. Сущность и понятие защиты информации 2. Каналы и методы несанкционированного доступа к конфиденциальной информации 3. Состав и классификация носителей защищаемой информации	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-11: способность разрабатывать политику информационной безопасности автоматизированной системы		1. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности 2. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию 3. Технологическое обеспечение защиты информации	Знание	4 – ОТЗ 4 – ЗТЗ
Итого				24 – ОТЗ 24 – ЗТЗ

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

Образец типового варианта итогового теста,
предусмотренного рабочей программой дисциплины
(9 – ОТЗ/ 9 – ЗТЗ)

1. Автоматизированная система (АС) – это:

а) набор неделимых элементов, сконцентрированных в конкретном порядке для достижения конкретных результатов.

б) система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

в) совокупность содержащейся в базах данных информации.

г) система для хранения, поиска и обработки информации.

2. Безопасность информации – это состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать _____, _____ и _____.

3. Закладочное устройство – это:

а) средство съёма информации, скрытно внедряемое в места возможного съёма информации.

б) элемент средства съёма информации, скрытно внедряемый в места возможного съёма информации.

в) специальное устройство, предназначенное для выявления технических каналов утечки информации и использования этих каналов.

г) специальное устройство, предназначенное для выявления технических каналов утечки информации и перекрытия этих каналов.

4. Защищаемая информация — это:

а) информация, для которой её обладателем или в соответствии с законодательством РФ определены характеристики её безопасности.

б) информация, реализованная в соответствии с требованиями стандартов и (или) иных нормативных документов по защите информации.

в) информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничен в соответствии с законодательством РФ.

г) информация, для которой её обладателем определены характеристики её безопасности.

5. Персональные данные – это:

а) любая информация, относящаяся к определённому или определяемому лицу на основании такой информации физическому лицу, в том числе его имя, фамилия, отчество, год, месяц, дата рождения, адрес, семейное, социальное, имущественное положение, образование, профессия доходы, другая информация.

б) вся информация о человеке.

в) любая информация, относящаяся к определённому или определяемому лицу на основании такой информации физическому лицу, в персональные данные не входит социальный статус, образование, доходы.

г) персональные данные, доступ не ограниченного круга лиц которым. предоставлен с согласия субъекта персональных данных.

6. Защищаемые помещения – это _____.

7. Информационная система – это:

а) совокупность содержащейся в базе данных информации.

б) набор неделимых элементов, сконцентрированных в закономерном порядке для достижения конкретных целей.

в) совокупность содержащейся в базе данных информации и обеспечивающих её обработку информационных технологий и технических средств.

г) совокупность содержащейся в базе данных информации и обеспечивающих её обработку.

8. Информация – это _____.

9. Коммерческая тайна – это:

а) режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

б) обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

в) информация, для которой обладателем информации определены характеристики её безопасности.

г) доступ к информации, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или АС.

10. Модель угроз – это _____.

11. Объект доступа – это _____.

12. Технический канал утечки информации – это:

а) это несанкционированный процессор, с помощью которого мошенники получают информацию.

б) это физический сигнал, который передает мошенник.

в) это физический путь сигнала от источника передачи данных к приемному устройству мошенника.

г) это совокупность технической разведки физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

13. Угроза информации – это _____.

14. Целостность информации – это:

а) состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на неё в процессе обработки или хранения.

б) обязательное, для выполнения лицом, получившего доступ к определённой информации, требование не передавать такую информацию третьим лицам без соглашения правообладателя.

в) возможность получения информации и её использования.

г) состояние защищённости информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность.

15. Обладатель информации – это:

а) лицо(государственное, юридическое лицо, человек), самостоятельно создавшее информацию либо получившее на основании закона или договора право размещать или ограничивать доступ к информации, определяемой по каким-либо признакам.

б) государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

в) лицо (государственное, юридическое лицо, человек), самостоятельно создавшее информацию либо получившее доступ к информации от её обладателя.

г) субъект доступа, имеющий право собирать, систематизировать, накапливать, хранить, уточнять, использовать, распространять, обезличивать, блокировать, уничтожать информацию.

16. Несанкционированный доступ (НСД) – это _____.

17. Предоставление информации – это _____.

18. Информационные технологии – это _____.

3.5 Перечень теоретических вопросов к экзамену

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности
4. Место информационной безопасности в системе национальной безопасности
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере
7. Интересы государства в информационной сфере
8. Угрозы информационному обеспечению государственной политики Российской Федерации
9. Виды угроз информационной безопасности
10. Внешние источники угроз информационной безопасности
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации
20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности
25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности
27. Защита от несанкционированного доступа
28. Антивирусная защита
29. Межсетевые экраны
30. VPN-технологии
31. Криптографические методы защиты информации

3.5 Перечень типовых простых практических заданий к экзамену

1. Построить логическую цепочку реализации угрозы информационной безопасности.
2. Построить схему классификации источников угроз ИБ.
3. Построить схему общий порядок организации обеспечения безопасности конфиденциальной информации
4. Построить диаграмму угроз информационной безопасности
5. Разработать краткий перечень должностных лиц организующих работу по защите информации на заданном преподавателем предприятии (ООО ЕВРААС).

4 Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Реферат	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит реферат или по результатам освоения темы, объемом до 20 стр. текста размером 12 пунктов, интервал 1,2; предоставляет реферат преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Доклад, сообщение	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тестирование	Обучаемый самостоятельно, под руководством преподавателя выполняет курсовую работу на заданную тему. Тема предлагается в общем виде. Конкретные методы и инструменты для ее разработки обучаемый выбирает самостоятельно. Обучаемый подбирает литературу по теме, не менее 3-4 источников, включая самостоятельный поиск в интернет (обязательно), разрабатывает ее, готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования. Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Курсовая работа	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.

Для организации и проведения промежуточной аттестации (в форме экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

- перечень теоретических вопросов к зачету для оценки знаний;
- перечень типовых простых практических заданий к зачету для оценки умений;
- перечень типовых практических заданий к зачету для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к экзамену обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления.

Образец экзаменационного билета

ИРГУПС ____-____ учебный год	**Экзаменационный билет № 1** **по дисциплине «_____»** **__ ____ семестр**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. ……. 2. ……. 3. …….. 4. …….. 5 ……..……		