

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.11 Основы информационной безопасности рабочая программа дисциплины

Направление подготовки – 10.03.01 Информационная безопасность

Профиль подготовки – Безопасность автоматизированных систем

Программа подготовки – академический бакалавриат

Квалификация выпускника – бакалавр

Форма обучения – очная

Нормативный срок обучения – 4 года

Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 3

Формы промежуточной аттестации в семестрах:

Часов по учебному плану – 108

зачет 2, курсовая работа 2

Распределение часов дисциплины по семестрам

Семестр	2	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
Итого	108	108

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	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
2	изучение видов 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	
Научно-образовательное воспитание обучающихся	
Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества. <p>Цель достигается по мере решения в единстве следующих задач:</p> <ul style="list-style-type: none"> – 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 	
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. <p>Цель достигается по мере решения в единстве следующих задач:</p> <ul style="list-style-type: none"> – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологи профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли 	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.Б.01 История
2	Б1.Б.22 Документоведение
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.Б.16 Техническая защита информации
2	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности
3	Б1.В.07 Аудит информационной безопасности
4	Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ,

**СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ
ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Минимальный уровень освоения компетенции

Знать	основные методы управления информационной безопасностью информационных систем
Уметь	формировать требования к системе охраны объекта
Владеть	административно-управленческие особенности формирования комплекса мер по информационной безопасности

Базовый уровень освоения компетенции

Знать	принципы и методы построения систем управления информационной безопасностью с учетом угроз информационной безопасности
Уметь	уметь разрабатывать модели угроз и нарушителей информационной безопасности
Владеть	принципами и правилами построения организационных структур системы управления с учетом поддержания выполнения комплекса мер по информационной безопасности

Высокий уровень освоения компетенции

Знать	Принципы построения организационной структуры системы управления с учетом поддержания выполнения комплекса мер по информационной безопасности
Уметь	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем
Владеть	административно-управленческими методами реализации комплекса мер по информационной безопасности

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности

Минимальный уровень освоения компетенции

Знать	Особенности работы малого коллектива
Уметь	Организовать взаимодействие работников малого коллектива друг с другом
Владеть	Технологией организации работы малого коллектива исполнителей с учетом требований защиты информации

Базовый уровень освоения компетенции

Знать	правила эксплуатации средств вычислительной техники, измерительных приборов или технологического оборудования, имеющегося в подразделении;
Уметь	использовать на практике методы анализа организационно-технического уровня изучаемого аппаратного и программного обеспечения инструментальных систем и их компонентов; принимать участие в проведении и оформлении научных исследований; пользоваться периодическими реферативными и справочно-информационными изданиями по профилю работы подразделения;
Владеть	методами и средствами выявления угроз безопасности; методами и средствами анализа и моделирования современных вычислительных объектов профессиональной деятельности и их компонентов;

Высокий уровень освоения компетенции

Знать	основные характеристики устройств хранения обработки и передачи информации; потенциальные каналы утечки информации, способы их выявления и методы оценки опасности; методы и средства инженерно-технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
Уметь	ориентироваться в особенностях применяемых программно- аппаратных, технических и инженерно-технических комплектов обеспечения комплексной защиты объектов информатизации, использовать стандартные и специализированные диагностические средства.
Владеть	методами организации и управления деятельности служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты информации.

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Минимальный уровень освоения компетенции

Знать	Основные средства и способы обеспечения информационной безопасности
Уметь	Определять комплекс мер и мероприятий для обеспечения информационной безопасности АС
Владеть	Профессиональной терминологией в области управления ИБ
Базовый уровень освоения компетенции	
Знать	Основные методы управления информационной безопасностью
Уметь	Разрабатывать предложения по совершенствованию системы управления ИБ АС
Владеть	Методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации
Высокий уровень освоения компетенции	
Знать	Основные положения стандартов единой системы конструкторской и программной документации (ФСТЭК России, ФСБ России)
Уметь	Методы аттестации уровней защищенности АС
Владеть	Методиками модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

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 информационного 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»
	Раздел 1. Теория информационной безопасности				
1.1	Введение /Лек/	2	2	ПК-13	Л1.1, Л2.3 Э1, Э2
1.2	Сущность и понятие информационной безопасности /Лек/	2	2	ПК-13	Л1.2, Л2.2 Э1
1.3	Проработка лекционного материала по теме «Сущность и понятие информационной безопасности» /Ср/	2	2	ПК-13	Л1.2, Л2.1 Э2
1.4	Значение информационной безопасности и ее место в системе национальной безопасности /Пр/	2	2	ПК-13	Л1.3, Л2.3 Э2
1.5	Современная Доктрина информационной безопасности Российской Федерации /Лек/	2	2	ПК-14	Л1.1, Л2.3 Э1,
1.6	Подготовка к практическому занятию по теме «Современная Доктрина ИБ Российской Федерации» /Ср/	2	2	ПК-14	Л1.2, Л2.1 Э1, Э2
1.7	Современная Доктрина информационной безопасности Российской Федерации /Пр/	2	2	ПК-14	Л1.2, Л1.3, Л2.3 Э1, Э2
	Раздел 2. Методология защиты информации				
2.1	Сущность и понятие защиты информации	2	2	ПК-13 ПК-15	Л1.1, Л1.2,

	/Лек/				Л2.2 Э1, Э2
2.2	Подготовка к практическому занятию по теме «Цели и значение защиты информации» /Ср/	2	2	ПК-13 ПК-15	Л1.1, Л2.3 Э1, Э2
2.3	Цели и значение защиты информации /Пр/	2	1	ПК-13 ПК-15	Л1.1, Л1.2, Л2.2 Э1, Э2
2.4	Теоретические и концептуальные основы защиты информации /Лек/	2	2	ПК-15	Л1.1, Л1.3, Л2.1 Э1, Э2
2.5	Подготовка к практическому занятию по теме «Теоретические и концептуальные основы защиты информации» /Ср/	2	2	ПК-15	Л1.3, Л2.1 Э1, Э2
2.6	Теоретические и концептуальные основы защиты информации /Пр/	2	2	ПК-15	Л1.2, Л1.3, Л2.2 Э1, Э2
2.7	Организационные основы и методологические принципы защиты информации /Лек/	2	2	ПК-13 ПК-14	Л1.1, Л1.3, Л2.3 Э1, Э2
2.8	Подготовка к практическому занятию по теме «Современные факторы, влияющие на защиту информации» /Ср/	2	2	ПК-13 ПК-14	Л1.1, Л2.3, Л2.1 Э1, Э2
2.9	Современные факторы, влияющие на защиту информации /Пр/	2	1	ПК-13 ПК-14	Л1.2, Л2.2 Э1, Э2
2.10	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности /Лек/	2	2	ПК-13 ПК-14	Л1.2, Л1.3, Л2.3 Э1, Э2
2.11	Подготовка к практическому занятию по теме «Критерии, условия и принципы отнесения информации к защищаемой» /Ср/	2	2	ПК-13 ПК-14	Л1.3, Л2.3 Э1, Э2
2.12	Критерии, условия и принципы отнесения информации к защищаемой /Пр/	2	1	ПК-13 ПК-14	Л1.2, Л2.2 Э1, Э2
2.13	Каналы и методы несанкционированного доступа к конфиденциальной информации /Лек/	2	2	ПК-15	Л1.1, Л1.3, Л2.3 Э1, Э2
2.14	Подготовка к практическому занятию по теме «Состав и классификация носителей защищаемой информации» /Ср/	2	2	ПК-15	Л1.1, Л1.2, Л2.1 Э1, Э2
2.15	Состав и классификация носителей защищаемой информации /Пр/	2	1	ПК-15	Л1.2, Л2.1, Л2.2 Э1, Э2
2.16	Классификация видов, методов и средств защиты информации /Лек/	2	2	ПК-15	Л1.2, Л1.3, Л2.2 Э1, Э2
2.17	Подготовка к практическому занятию по теме «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности» /Ср/	2	2	ПК-15	Л1.1, Л1.3, Л2.1 Э1, Э2
2.18	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности /Пр/	2	2	ПК-15	Л1.2, Л1.3, Л2.3 Э1, Э2
2.19	Подготовка к практическому занятию по теме «Классификация защищаемой информации по собственникам и владельцам» /Ср/	2	2	ПК-13 ПК-14 ПК-15	Л1.1, Л1.2, Л2.1 Э1, Э2
2.20	Классификация защищаемой информации по собственникам и владельцам /Пр/	2	2	ПК-13	Л1.1, Л1.3, Л2.1 Э2
2.21	Подготовка к практическому занятию по теме «Понятие и структура угроз защищаемой информации» /Ср/	2	2	ПК-13	Л1.1, Л1.2, Л2.1 Э1, Э2
2.22	Понятие и структура угроз защищаемой информации /Пр/	2	2	ПК-13	Л1.2, Л1.3, Л2.3 Э1, Э2
2.23	Подготовка к практическому занятию по теме «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию» /Ср/	2	2	ПК-13	Л1.1, Л1.2, Л2.2, Л2.3 Э1, Э2
2.24	Источники, виды и способы дестабилизирующего воздействия на	2	2	ПК-15	Л1.3, Л2.1, Л2.2, Л2.3

	защищаемую информацию /Пр/				Э1, Э2
2.25	Подготовка к практическому занятию по теме «Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию» /Ср/	2	2	ПК-15	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.26	Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию /Пр/	2	2	ПК-15	Л1.2, Л1.3, Л2.1, Л2.3 Э1, Э2
2.27	Подготовка к практическому занятию по теме «Каналы и методы несанкционированного доступа к конфиденциальной информации» /Ср/	2	2	ПК-14	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.28	Каналы и методы несанкционированного доступа к конфиденциальной информации /Пр/	2	2	ПК-14	Л1.3, Л2.1, Л2.2, Л2.3 Э1, Э2
2.29	Подготовка к практическому занятию по теме «Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации» /Ср/	2	2	ПК-14	Л1.1, Л1.2, Л2.2, Л2.3 Э1, Э2
2.30	Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации /Пр/	2	2	ПК-13 ПК-14	Л1.1, Л1.3, Л2.1, Л2.2, Э1, Э2
2.31	Подготовка к практическому занятию по теме «Объекты защиты информации» /Ср/	2	2	ПК-13 ПК-14	Л1.1, Л1.3, Л2.2, Э1, Э2
2.32	Объекты защиты информации /Пр/	2	2	ПК-13 ПК-14	Л1.1, Л1.2, Э1, Э2
2.33	Подготовка к практическому занятию по теме «Кадровое и ресурсное обеспечение защиты информации» /Ср/	2	2	ПК-13 ПК-14	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.34	Кадровое и ресурсное обеспечение защиты информации /Пр/	2	2	ПК-15	Л1.3, Л2.1, Л2.2, Э1, Э2
2.35	Подготовка к практическому занятию по теме «Технологическое обеспечение защиты информации» /Ср/	2	2	ПК-15	Л1.1, Л1.2, Л2.3 Э1, Э2
2.36	Технологическое обеспечение защиты информации /Пр/	2	2	ПК-15	Л1.1, Л1.3, Л2.1, Э1, Э2
2.37	Подготовка к практическому занятию по теме «Назначение и структура систем защиты информации» /Ср/	2	2	ПК-13 ПК-15	Л1.1, Л1.2, Л2.2, Л2.3 Э1, Э2
2.38	Назначение и структура систем защиты информации /Пр/	2	2	ПК-13 ПК-14 ПК-15	Л1.3, Л2.1, Л2.2, Э1, Э2
2.39	Проработка теоретической части курсовой работы /Ср/	2	4	ПК-13 ПК-14 ПК-15	Л1.1, Л1.2, Л1.3, Л2.1, Э1, Э2
2.40	Разработка практической части курсовой работы /Ср/	2	6	ПК-13 ПК-14 ПК-15	Л1.1, Л1.2, Л2.3 Э1, Э2
2.41	Защита курсовой работы /Пр/	2	4	ПК-13 ПК-14 ПК-15	Л1.1, Л1.2, Л1.3, Л2.1,
	Раздел 3. Контроль знаний				
3.1	Зачет	3	8	ПК-13 ПК-14 ПК-15	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 дисциплине разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной

итоговой аттестации № П.312000.06.7.188-2017.

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	Ю.М. Краковский	Информационная безопасность и защита информации: учебное пособие	М: ИрГУПС, 2016	50
Л1.2	М.А. Лапина, А.Г. Ревин, В.И. Лапин ;	Информационное право: учебное пособие [Электронный ресурс] biblioclub.ru/index.php?page=book&id=118624	М. : Юнити-Дана, 2015	100% онлайн
Л1.3	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
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	С.А. Нестеров	Основы информационной безопасности: Учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=363040	СПб. : Политехнический университет, 2014	100% онлайн
Л2.2	О.В. Порядина	Управление информационными ресурсами: учебно-методическое пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=439328	Поволжский государственный технологический университет. - Йошкар-Ола , 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 студента	100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»	
Э.1	Линия защиты «Сюртель» www.suritel.ru
Э.2	Федеральная служба по техническому и экспортному контролю, www.fstec.ru
6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем	
6.3.1 Перечень базового программного обеспечения	
6.3.1.1	ОС Microsoft Windows XP Professional, количество – 227, лицензия № 44718499; ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083; Libre Office v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org
6.3.2 Перечень специализированного программного обеспечения	
6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.
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	
1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	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), служажими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации).
3	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
4	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.
5	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; пометать 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.
Практическая работа (семинар)	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

	<p>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.</p> <p>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.</p>
Реферат	<p>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.</p> <p>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.</p> <p>Ознакомиться со структурой и оформлением реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).</p>
Курсовая работа	<p>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).</p>
Самостоятельная работа студента	<p>Для успешного выполнения самостоятельной работы, студенту необходимо обратиться к лекционному материалу, основным и дополнительным источникам литературы, указанным в рабочей программе. Если этого будет недостаточно для выполнения поставленного задания, необходимо в обязательном порядке посетить консультацию преподавателя.</p>
<p>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.</p>	

**Приложение 1 к рабочей программе по дисциплине
Б1.Б.11 «Основы информационной безопасности»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости
и промежуточной аттестации по дисциплине
Б1.Б.11 «Основы информационной безопасности»

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

Дисциплина «Основы информационной безопасности» участвует в формировании компетенций:

ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;

ПК-14: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Таблица траекторий формирования у обучающихся компетенций ПК-13, ПК-14, ПК-15 при освоении образовательной программы

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин / практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Б1.В.ДВ.07.02 Методология определения ценности информации	6	1
		Б1.Б.21 Основы управления информационной безопасностью	78	2
		Б1.В.08 Методология построения защищенных автоматизированных систем	8	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3
ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	Б1.В.ДВ.03.02 Корпоративные информационные системы	3	1
		Б1.Б.26 Основы управленческой деятельности	7	2
		Б1.Б.21 Основы управления информационной безопасностью	78	2
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации,	Б1.Б.15 Организационное и правовое обеспечение информационной безопасности	4	1
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	1
		Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта	7	2
		Б1.В.ДВ.02.01 Защита и обработка конфиденциальных документов	7	2
		Б1.В.ДВ.02.02 Защита электронного документооборота	7	2
		Б1.Б.21 Основы управления информационной безопасностью	78	2
		Б1.В.05 Комплексная защита в информационных системах персональных данных	8	3
Б2.В.04(Пд) Производственная практика -	8	3		

Федеральной службы по техническому и экспортному контролю	преддипломная		
	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3

**Таблица соответствия уровней освоения компетенций ПК-13, ПК-14, ПК-15
планируемым результатам обучения**

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации Раздел 3. Контроль знаний	Минимальный уровень	Знать: Основные методы управления информационной безопасностью информационных систем
				Уметь: Формировать требования к системе охраны объекта
				Владеть: Административно-управленческие особенности формирования комплекса мер по информационной безопасности
			Базовый уровень	Знать: Принципы и методы построения систем управления информационной безопасностью с учетом угроз информационной безопасности
				Уметь: Разрабатывать модели угроз и нарушителей информационной безопасности
				Владеть: Принципами и правилами построения организационных структур системы управления с учетом поддержания выполнения комплекса мер по информационной безопасности
			Высокий уровень	Знать: Принципы построения организационной структуры системы управления с учетом поддержания выполнения комплекса мер по информационной безопасности
				Уметь: Определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем
				Владеть: Административно-управленческими методами реализации комплекса мер по информационной безопасности
ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты информации	Минимальный уровень	Знать: Особенности работы малого коллектива
				Уметь: Организовать взаимодействие работников малого коллектива друг с другом
				Владеть: Технологией организации работы малого коллектива исполнителей с учетом требований защиты информации

		Раздел 3. Контроль знаний	Базовый уровень	<p>Знать: Правила эксплуатации средств вычислительной техники, измерительных приборов или технологического оборудования, имеющегося в подразделении;</p> <p>Уметь: Использовать на практике методы анализа организационно-технического уровня изучаемого аппаратного и программного обеспечения инструментальных систем и их компонентов; принимать участие в проведении и оформлении научных исследований; пользоваться периодическими реферативными и справочно-информационными изданиями по профилю работы подразделения;</p> <p>Владеть: Методами и средствами выявления угроз безопасности; методами и средствами анализа и моделирования современных вычислительных объектов профессиональной деятельности и их компонентов;</p>
			Высокий уровень	<p>Знать: Основные характеристики устройств хранения обработки и передачи информации; потенциальные каналы утечки информации, способы их выявления и методы оценки опасности; методы и средства инженерно-технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.</p> <p>Уметь: Ориентироваться в особенностях применяемых программно- аппаратных, технических и инженерно-технических комплектов обеспечения комплексной защиты объектов информатизации, использовать стандартные и специализированные диагностические средства.</p> <p>Владеть: Методами организации и управления деятельности служб защиты информации на предприятии; технологией проектирования, построения и эксплуатации комплексных систем защиты информации.</p>
ПК-15	способность организовывать технологический процесс защиты информации ограниченного	Раздел 1. Теория информационной безопасности Раздел 2. Методология защиты	Минимальный уровень	<p>Знать: Основные средства и способы обеспечения информационной безопасности</p> <p>Уметь: Определять комплекс мер и мероприятий для обеспечения информационной безопасности АС</p>

доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	информации Раздел 3. Контроль знаний	Базовый уровень	Владеть: Профессиональной терминологией в области управления ИБ
			Знать: Основные методы управления информационной безопасностью
			Уметь: Разрабатывать предложения по совершенствованию системы управления ИБ АС
		Высокий уровень	Владеть: Методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации
			Знать: Основные положения стандартов единой системы конструкторской и программной документации (ФСТЭК России, ФСБ России)
			Уметь: Методы аттестации уровней защищенности АС
Владеть: Методиками модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России			

**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)
2 семестр				
1	1	Текущий контроль	Тема «Сущность и понятие информационной безопасности»	ПК-13 Реферат (письменно)
2	1	Текущий контроль	Тема «Значение информационной безопасности и ее место в системе национальной безопасности»	ПК-13 Доклад, сообщение (устно)
3	1	Текущий контроль	Тема «Современная Доктрина ИБ Российской Федерации»	ПК-14 Реферат (письменно)
4	2	Текущий контроль	Тема «Современная Доктрина ИБ Российской Федерации»	ПК-14 Доклад, сообщение (устно)
5	2	Текущий контроль	Тема «Цели и значение защиты информации»	ПК-13, ПК-15 Реферат (письменно)
6	3	Текущий контроль	Тема «Цели и значение защиты информации»	ПК-13, ПК-15 Доклад, сообщение (устно)
7	3	Текущий контроль	Тема «Теоретические и концептуальные основы защиты информации»	ПК-15 Реферат (письменно)
8	3	Текущий контроль	Тема «Теоретические и концептуальные основы защиты информации»	ПК-15 Доклад, сообщение (устно)
9	4	Текущий контроль	Тема «Современные факторы, влияющие на защиту информации»	ПК-14, ПК-15 Реферат (письменно)
10	4	Текущий контроль	Тема «Современные факторы, влияющие на защиту информации»	ПК-14, ПК-15 Доклад, сообщение (устно)

			информации»		
11	4	Текущий контроль	Тема «Критерии, условия и принципы отнесения информации к защищаемой»	ПК-14, ПК-15	Реферат (письменно)
12	5	Текущий контроль	Тема «Критерии, условия и принципы отнесения информации к защищаемой»	ПК-14, ПК-15	Доклад, сообщение (устно)
13	5	Текущий контроль	Тема «Состав и классификация носителей защищаемой информации»	ПК-15	Реферат (письменно)
14	6	Текущий контроль	Тема «Состав и классификация носителей защищаемой информации»	ПК-15	Доклад, сообщение (устно)
15	6	Текущий контроль	Тема «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности»	ПК-15	Реферат (письменно)
16	6	Текущий контроль	Тема «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности»	ПК-13, ПК-14, ПК-15	Доклад, сообщение (устно)
17	7	Текущий контроль	Тема «Классификация защищаемой информации по собственникам и владельцам»	ПК-13	Реферат (письменно)
18	7	Текущий контроль	Тема «Классификация защищаемой информации по собственникам и владельцам»	ПК-13	Доклад, сообщение (устно)
19	8	Текущий контроль	Тема «Понятие и структура угроз защищаемой информации»	ПК-13	Реферат (письменно)
20	8	Текущий контроль	Тема «Понятие и структура угроз защищаемой информации»	ПК-13	Доклад, сообщение (устно)
21	9	Текущий контроль	Тема «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию»	ПК-15	Реферат (письменно)
22	9	Текущий контроль	Тема «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию»	ПК-15	Доклад, сообщение (устно)
23	9	Текущий контроль	Тема «Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию»	ПК-15	Реферат (письменно)
24	10	Текущий контроль	Тема «Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию»	ПК-15	Доклад, сообщение (устно)
25	10	Текущий контроль	Тема «Каналы и методы несанкционированного доступа к конфиденциальной информации»	ПК-14	Реферат (письменно)
26	10	Текущий контроль	Тема «Каналы и методы несанкционированного доступа к конфиденциальной информации»	ПК-14	Доклад, сообщение (устно)
27	11	Текущий контроль	Тема «Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации»	ПК-14	Реферат (письменно)
28	11	Текущий контроль	Тема «Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу	ПК-13, ПК-14	Доклад, сообщение (устно)

			к конфиденциальной информации»		
29	12	Текущий контроль	Тема «Объекты защиты информации»	ПК-13, ПК-14	Реферат (письменно)
30	12	Текущий контроль	Тема «Объекты защиты информации»	ПК-13, ПК-14	Доклад, сообщение (устно)
31	13	Тест	Изученный материал	ПК-13, ПК-14, ПК-15	Перечень тестовых заданий
32	14	Текущий контроль	Тема «Кадровое и ресурсное обеспечение защиты информации»	ПК-13	Реферат (письменно)
33	14	Текущий контроль	Тема «Кадровое и ресурсное обеспечение защиты информации»	ПК-15	Доклад, сообщение (устно)
34	15	Текущий контроль	Тема «Технологическое обеспечение защиты информации Объекты защиты информации»	ПК-15	Реферат (письменно)
35	15	Текущий контроль	Тема «Технологическое обеспечение защиты информации»	ПК-15	Доклад, сообщение (устно)
36	16	Текущий контроль	Тема «Назначение и структура систем защиты информации»	ПК-13, ПК-14, ПК-15	Реферат (письменно)
37	16	Текущий контроль	Тема «Назначение и структура систем защиты информации»	ПК-13, ПК-14, ПК-15	Доклад, сообщение (устно)
38	17	Текущий контроль	Защита курсовой работы /Пр/	ПК-13, ПК-14, ПК-15	Курсовая работа
39	18	Промежуточная аттестация – зачет	Разделы: 1 Теория информационной безопасности 2 Методология защиты информации 3 Контроль знаний	ПК-13, ПК-14, ПК-15	Оценка качества ответов на вопросы преподавателя в ходе беседы по теме вопроса; устно; оценка ответов на вопросы теста.

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	Сообщение, доклад	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	Тест	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	Курсовой 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 курсовой работу
5	Зачет (дифференцированный зачет)	Средство, позволяющее оценить знания, умения, навыки 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 зачету

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

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
	Обучающийся с небольшими неточностями	Базовый

«зачтено»	ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

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.) Используются 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

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	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 Типовые контрольные задания для выполнения контрольных работ

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения контрольных работ.

Образец типового варианта контрольной работы

1. Структура государственной системы защиты информации (схема).
2. Система документации по технической защите информации (схема).
3. Определение информационной безопасности.
4. Определение защиты информации.

3.2 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования

1. Значение информационной безопасности и ее место в системе национальной безопасности;
2. Современная Доктрина информационной безопасности Российской Федерации;
3. Цели и значение защиты информации;
4. Теоретические и концептуальные основы защиты информации;
5. Современные факторы, влияющие на защиту информации;
6. Критерии, условия и принципы отнесения информации к защищаемой;
7. Состав и классификация носителей защищаемой информации;
8. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности;
9. Классификация защищаемой информации по собственникам и владельцам;
10. Понятие и структура угроз защищаемой информации;
11. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;
12. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию;
13. Каналы и методы несанкционированного доступа к конфиденциальной информации;
14. Направления, виды и особенности деятельности разведывательных служб по

несанкционированному доступу к конфиденциальной информации;

15. Объекты защиты информации;
16. Кадровое и ресурсное обеспечение защиты информации;
17. Технологическое обеспечение защиты информации;
18. Назначение и структура систем защиты информации.

3.3 Типовые контрольные задания для написания конспекта

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для написания конспектов.

Образец тем конспектов

1. Значение информационной безопасности и ее место в системе национальной безопасности;
2. Современная Доктрина информационной безопасности Российской Федерации;
3. Цели и значение защиты информации;
4. Теоретические и концептуальные основы защиты информации;
5. Современные факторы, влияющие на защиту информации;
6. Критерии, условия и принципы отнесения информации к защищаемой;
7. Состав и классификация носителей защищаемой информации;
8. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности;
9. Классификация защищаемой информации по собственникам и владельцам;
10. Понятие и структура угроз защищаемой информации;
11. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;
12. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию;
13. Каналы и методы несанкционированного доступа к конфиденциальной информации;
14. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации;
15. Объекты защиты информации;
16. Кадровое и ресурсное обеспечение защиты информации;
17. Технологическое обеспечение защиты информации;
18. Назначение и структура систем защиты информации.

3.4 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-2.6	Тема 1. Значение информационной безопасности и ее место в системе национальной безопасности	Знание	1 – ОТЗ
		Умение	2 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-2.6	Тема 2. Современная Доктрина информационной безопасности Российской Федерации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
		Навык	1 – ЗТЗ
ОПК-2.6	Тема 3. Цели и значение защиты информации	Знание	2 – ОТЗ

		Умение	2 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-2.6	Тема 4. Теоретические и концептуальные основы защиты информации	Знание	1 – ЗТЗ
		Умение	2 – ОТЗ
ОПК-2.6	Тема 5. Современные факторы, влияющие на защиту информации	Навык	2 – ЗТЗ
		Знание	1 – ОТЗ
ОПК-2.6	Тема 6. Критерии, условия и принципы отнесения информации к защищаемой	Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-2.6	Тема 7. Состав и классификация носителей защищаемой информации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
ОПК-2.6	Тема 8. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности	Навык	2 – ЗТЗ
		Знание	2 – ОТЗ
ОПК-2.6	Тема 9. Классификация защищаемой информации по собственникам и владельцам	Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-2.6	Тема 10. Понятие и структура угроз защищаемой информации	Знание	1 – ЗТЗ
		Умение	2 – ОТЗ
ОПК-2.6	Тема 11. Источники, виды, условия и способы дестабилизирующего воздействия на защищаемую информацию	Навык	2 – ЗТЗ
		Знание	1 – ОТЗ
ОПК-2.6	Тема 12. Каналы и методы несанкционированного доступа к конфиденциальной информации	Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-2.6	Тема 13. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
ОПК-2.6	Тема 14. Объекты защиты информации	Навык	1 – ЗТЗ
		Знание	1 – ОТЗ
ОПК-2.6	Тема 15. Кадровое и ресурсное обеспечение защиты информации	Умение	1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-2.6	Тема 16. Технологическое обеспечение защиты информации	Знание	1 – ЗТЗ
		Умение	1 – ОТЗ
ОПК-2.6	Тема 17. Назначение и структура систем защиты информации	Навык	1 – ЗТЗ
		Знание	1 – ОТЗ
		Итого	30 – ОТЗ 30 – ЗТЗ

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

1. Выберите правильное определение термина «информация»:
 - а) совокупность содержащихся в базах данных сведений;

- б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
- в) сведения (сообщения, данные) воспроизводимые различными системами;
- г) **сведения (сообщения, данные) независимо от формы их представления.**

2. Выберите правильное определение термина «обладатель информации»:

- а) лицо, самостоятельно создавшее информацию;
- б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
- в) **лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;**
- г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Предоставление информации – это

Ответ: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

4. Защищаемые помещения – это

Ответ: помещения, специально предназначенные для проведения конфиденциальных мероприятий.

5. Выберите правильное определение термина «контролируемая зона»:

- а) **пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;**
- б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;
- в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;
- г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

6. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

- а) **методы и способы защиты информации от несанкционированного доступа;**
- б) методы и способы сокрытия информации от внутренних нарушителей;
- в) методы и способы устранения конкурентов;
- г) **методы и способы защиты информации от утечки по техническим каналам.**

7. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):

- а) полуактивные;
- б) **пассивные;**
- в) разноплановые;
- г) удостоверяющие;
- д) **активные.**

8. Технический канал утечки информации – это

Ответ: совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

9. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно _____

Ответ: 16.

10. Техническими каналами утечки информации являются (выберите все верные варианты ответов):

- а) кражи технических средств информационной системы;
- б) утечки акустической (речевой) информации;**
- в) утечки информации, реализуемые через общедоступные информационные сети;
- г) утечки видовой информации;**
- д) утечки информации по каналам побочных электромагнитных излучений;**
- е) утечки информации, реализуемые через интернет.

11. Несанкционированный доступ к информации – это

Ответ: доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.

12. Механизм контроля целостности СЗИ Secret Net предназначен для

- а) формирования цифровых отпечатков данных;
- б) контроля информационных потоков;
- в) слежения за неизменностью содержимого ресурсов компьютера.**

13. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

- а) ограничения использования программного обеспечения на компьютере;**
- б) установки ограниченного количества программ;
- в) сбора сведений об используемых приложениях.

14. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

- а) «конфиденциально»;**
- б) «секретно»;
- в) «строго конфиденциально»;
- г) «неконфиденциально».**

15. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного _____

Ответ: логарифма.

16. Хэш-функции предназначены, главным образом, для _____

Ответ: контроля целостности данных.

17. Длина хэш-кода алгоритма MD5 составляет _____

Ответ: 128 бит.

18. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

Ответ: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы.

3.5 Перечень теоретических вопросов к зачету

(для оценки знаний)

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.

3.6 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

Практические занятия по дисциплине «Основы информационной безопасности» заключаются в построении моделей информационных систем, определении элементов информационных систем, подверженных угрозам, и преобразования структуры информационных систем за счет добавления средств защиты информации, нейтрализующих данные угрозы. Используемые средства – схематичные способы



представления систем и процессов, например IDEF0 (рис. 1).

Рисунок 1 – Модель информационной системы «Электронная почта»

Угрозы конфиденциальности выявляются следующим образом – каждому входному элементу, управляющему элементу и механизму должна быть поставлена в соответствие угроза. Перечень угроз, направленных на информационную систему:

- несанкционированный (н/с) текст – отправка запрещенной к передаче конфиденциальной информации (разглашение информации);
- н/с адрес – отправка информации не по адресу получателя (случайно или преднамеренно);

- н/с почтовая программа – использование неразрешенного (например, самовольно установленного) программного обеспечения, возможно, зараженного вирусом;
- н/с отправитель – отправка письма от чужого имени, например должностного лица, с указаниями по передаче конфиденциальной информации.

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
Контрольная работа	Преподаватель на установочном занятии доводит до обучающихся: темы, количество заданий в контрольной работе. Контрольная работа должна быть выполнена в установленный срок и в соответствии с правилами к оформлению (текстовой и графической частей), сформулированными в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» в последней редакции. Выполненная контрольная работа передается для проверки преподавателю в установленные сроки. Если контрольная работа выполнена не в соответствии с указаниями или не в полном объеме, она возвращается на доработку
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Конспект	Защита конспектов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему конспектов и требования, предъявляемые к их выполнению и защите

Для организации и проведения промежуточной аттестации 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 и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

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

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.