

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.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта

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. – 4

Формы промежуточной аттестации в семестрах:

Часов по учебному плану – 144

экзамен 7

Распределение часов дисциплины по семестрам

Семестр	7	Итого
Число недель в семестре	14	
Вид занятий	Часов по учебному плану	Часов по учебному плану
Аудиторная контактная работа по видам учебных занятий	56	56
– лекции	28	28
– практические (семинарские)	28	28
Самостоятельная работа	52	52
Экзамен	36	36
Итого	144	144

ИРКУТСК

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	изучение состояния проблемы обеспечения информационной безопасности и методов и средств защиты информации в автоматизированных системах железнодорожного транспорта (АС ЖТ).
1.2 Задачи освоения дисциплины	
1	изучение и принцип функционирования основных автоматизированных систем железнодорожного транспорта
2	изучение основных приложений в системе железнодорожного транспорта, а также прикладных систем и задач автоматизированных систем
3	Способы и требования организации работ по обеспечению защиты информации в автоматизированных системах управления ОАО «РЖД»
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.	
Цель достигается по мере решения в единстве следующих задач:	
<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.	
Цель достигается по мере решения в единстве следующих задач:	
<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 психологии 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.25 Информационные технологии
2	Б1.Б.11 Основы информационной безопасности
3	Б1.В.ДВ.04.01 Катастрофоустойчивость и надежность информационных систем
4	Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем
2	Б2.В.04(Пд) Производственная практика - преддипломная

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ПК-5: способность применять программные средства системного, прикладного и специального	

назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Минимальный уровень освоения компетенции	
Знать	положение по аттестации объектов информатизации по требованиям безопасности информации в области железнодорожного транспорта;
Уметь	осуществлять предварительное ознакомление с аттестуемым объектом;
Владеть	основными понятиями в области аттестации объектов информатизации и знанием требований безопасности информации в области железнодорожного транспорта (систем управления РЖД).
Базовый уровень освоения компетенции	
Знать	порядок проведения аттестации и контроля объекта информатизации по требованиям безопасности информации;
Уметь	проводить аттестационные испытания объектов информатизации;
Владеть	навыками проведения аттестационных испытаний объектов информатизации по требованиям безопасности.
Высокий уровень освоения компетенции	
Знать	требования к нормативным и методическим документам по аттестации объектов информатизации;
Уметь	разрабатывать методику проведения аттестации объекта информатизации, учитывая требования нормативных и методических документов по аттестации объектов информатизации;
Владеть	навыками анализа результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждения заключения по результатам аттестации.

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	организационную структуру и функциональную часть автоматизированных систем управления (АСУ) федерального ЖТ;
2	принципы и стандарты построения современных защищенных АС;
3	основные уязвимости и угрозы ИБ для АС ЖТ;
4	основные тенденции и закономерности развития средств и методов защиты информации в АС ЖТ;
5	политики безопасности и меры защиты в АС ЖТ;
6	комплексный подход к построению эшелонированной защиты для АС ЖТ;
Уметь	
1	анализировать текущее состояние ИБ на предприятии с целью разработки требований к защищенным АС;
2	определять и устранять основные угрозы ИБ для АС ЖТ;
3	строить модели угроз и нарушителя ИБ для АС ЖТ;
4	выявлять и устранять уязвимости в основных компонентах АС ЖТ;

5	проектировать защищенные АС;
6	применять организационные, организационно-технические и технические средства, методы и мероприятия по защите информации на АС ФЖТ;
7	применять стандартные решения для защиты информации в АС и квалифицированно оценивать их качество;
8	реализовывать системы защиты информации в АС ЖТ в соответствии со стандартами по оценке защищенных систем;
9	применять комплексный подход к обеспечению ИБ для АС ЖТ;
10	осуществлять управление и администрирование защищенных АС ЖТ;
Владеть	
1	терминологией и системным подходом построения защищенных ОИС;
2	навыками анализа угроз ИБ и уязвимостей в АС ЖТ;
3	организационными, организационно-техническими, техническими и компьютерными средствами и методами по защите информации на АС ЖТ;
4	навыками разработки политик ИБ для АС ЖТ.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ					
Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	Раздел 1. Управление деятельностью предприятия; классификация информационных систем (ИС). Этапы разработки				
1.1	Информационный контур управления. ИС как объект управления. Эволюция ИС. Требования к ИС. /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
1.2	Подготовка к практическому занятию по теме «Состав и формирование требований, проектируемых автоматизированных ИС»/Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
1.3	Состав и формирование требований, проектируемых автоматизированных ИС /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 2. Понятие корпоративных сетей. Комплексная информационно-вычислительная сеть ЖТ				
2.1	Обзор служб, сервисов и технологий Интернет. Управление корпоративными системами. /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
2.2	Подготовка к практическому занятию по теме «Базовые технологии дорожного (регионального) уровня» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
2.3	Базовые технологии дорожного (регионального) уровня /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 3. Организационная и функциональная части АСУ ЖТ				
3.1	АС оперативного управления перевозками. АСУ сортировочными станциями. АС резервирования мест и продажи билетов «Экспресс». АС управления вагонным парком. Обеспечивающая часть АСУ ЖТ. Техническое, информационное, математическое и программное обеспечение. /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
3.2	Подготовка к практическому занятию по теме «Открытая система R3; архитектура «клиент-сервер»; масштабируемость системы R3» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
3.3	Открытая система R3; архитектура «клиент-сервер»; масштабируемость	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1

	системы R3 /Пр/				Л2.2 Э1
	Раздел 4. Архитектура ЕК АСУФР				
4.1	Цели создания ЕК АСУФР. Место ЕК АСУФР в информационном комплексе ОАО «РЖД». Базовые принципы ЕК АСУФР. Основные архитектурные решения проекта и структура ЕК АСУФР. /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
4.2	Подготовка к практическому занятию по теме «Функциональные, дорожные и обеспечивающие под проекты» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
4.3	Функциональные, дорожные и обеспечивающие под проекты /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 5. Концепция вычислительной инфраструктуры ЕК АСУФР. Технические требования				
5.1	Ландшафт вычислительной системы. Возможности развития системы ЕК АСУФР. Повышение защищенности информационных ресурсов ЕК АСУФР от злонамеренного использования или разрушения. Концепция системы управления проектом. Принципы вертикальной и горизонтальной интеграции. Сохранение компетенции в ОАО «РЖД». /Лек/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
5.2	Подготовка к практическому занятию по теме «Технические требования к ЕК АСУФР. Виды обеспечения выполнения технических требований. Стратегия реализации проекта» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
5.3	Технические требования к ЕК АСУФР. Виды обеспечения выполнения технических требований. Стратегия реализации проекта /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 6. Концептуальные аспекты защиты информации и обеспечения информационной безопасности				
6.1	Объекты ИБ. Основные угрозы ИБ. Описание общей структуры подсистемы защиты информации ЕК АСУФР. Взаимодействие структурных подразделений по вопросам ИБ ЕК АСУФР. Инфраструктура ИБ. Защита серверов ЕК АСУФР. Защита рабочих станций пользователей ЕК АСУФР. /Лек/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
6.2	Подготовка к практическому занятию по теме «ЕК АСУФР: защита информации на сетевом уровне» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
6.3	ЕК АСУФР: защита информации на сетевом уровне /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 7. Правовой режим информационных ресурсов ЖТ				
7.1	Основа правовых методов ИБ. Анализ нормативно-правовой базы области защиты информации. Правовые основы лицензирования и сертификации. Стандарты в области защиты информации /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
7.2	Подготовка к практическому занятию по теме «Стандарты в области защиты информации» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
7.3	Стандарты в области защиты информации	7	2	ПК-5 ПК-15	Л1.1 Л1.2

	/Пр/				Л1.3 Л2.1 Л2.2 Э1
	Раздел 8. Защита информационных и технических ресурсов от несанкционированного межсетевого доступа в сетях ЖТ				
8.1	Принципы построения и функционирования межсетевых экранов. Фильтрация трафика; выполнение функций посредничества. Классификация межсетевых экранов. Фильтрующий маршрутизатор; шлюз сеансового уровня модели OSI/ISO. /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
8.2	Подготовка к практическому занятию по теме «Межсетевой экран Cisco PIX Firewall» /Ср//	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
8.3	Межсетевой экран Cisco PIX Firewall /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 9. Идентификация и аутентификация абонентов и объектов сети ЖТ				
9.1	Идентификация и подтверждение подлинности абонентов корпоративной сети. Протоколы взаимной проверки подлинности объектов /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
9.2	Подготовка к практическому занятию по теме «Протоколы взаимной проверки подлинности объектов» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
9.3	Протоколы взаимной проверки подлинности объектов /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 10. Обеспечение целостности информации в АС ЖТ				
10.1	ЭП на основе симметричных криптоалгоритмов. ЭП на основе асимметричных криптоалгоритмов. Алгоритм ЭП DSA. Алгоритм ЭП ГОСТ 34.10-2001. Алгоритм хеширования SHA-2. /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
10.2	Подготовка к практическому занятию по теме «Отечественный стандарт хеширования» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
10.3	Отечественный стандарт хеширования /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 11. Защищенные виртуальные сети (VPN). Реализация VPN в сетях ЖТ				
11.1	Варианты создания защищенных виртуальных каналов. Протоколы VPN. Протоколы канального, сетевого и сеансового уровней. Средства создания VPN /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
11.2	Подготовка к практическому занятию по теме «Средства создания VPN» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
11.3	Средства создания VPN /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
	Раздел 12. Средства защиты информации в системах баз данных СБД АС ЖТ				
12.1	Общая характеристика СБД АС ЖТ. RACF как средство доступа к наборам данных и	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1

	ресурсам систем /Лек/				Л2.2 Э1
12.2	Подготовка к практическому занятию по теме «RACF как средство доступа к наборам данных и ресурсам систем» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
12.3	RACF как средство доступа к наборам данных и ресурсам систем /Пр/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
Раздел 13. Средства антивирусной защиты в корпоративных сетях ФЖТ					
13.1	Основные типы вредоносного программного обеспечения. Организация антивирусной защиты /Лек/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
13.2	Подготовка к практическому занятию по теме «Средства антивирусной защиты» /Ср/	7	4	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
13.3	Средства антивирусной защиты /Пр/	7	2	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1
Раздел 14. Контроль знаний					
14.1	Экзамен	7	36	ПК-5 ПК-15	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Э1

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	И.В. Рябов	Автоматизированные информационно-управляющие системы: учебное пособие [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=439330	Йошкар-Ола : ПГТУ, 2015.	100% онлайн
Л1.2	О.В. Шишов	Современные технологии промышленной автоматизации: учебное пособие [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=364093	М.; Берлин: Директ-Медиа, 2015	100% онлайн
Л1.3	О.В. Прохорова	Информационная безопасность и защита информации: учебник [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации : учебное	М.; Берлин : Директ-Медиа,	100% онлайн

		пособие [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=276557	2015	
Л2.2	Ю. М. Краковский	Информационная безопасность и защита информации: учебное пособие	Иркутск: ИрГУПС, 2016	50
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.И.	Материалы для самостоятельной работы студентов	Личный кабинет обучающегося	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), служащими 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	<p>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 удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.</p>
Практическое занятие	<p>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.</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>
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.В.09 «Теория и практика защиты информации в
автоматизированных системах железнодорожного транспорта»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости
и промежуточной аттестации по дисциплине
Б1.В.09 «Теория и практика защиты информации в
автоматизированных системах железнодорожного
транспорта»

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

Дисциплина «Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта» участвует в формировании компетенций:

ПК-5: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

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-5, 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-5	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Б1.Б.33 Метрология, стандартизация и сертификация	4	1
		Б2.В.03(П) Производственная практика - эксплуатационная	6	2
		Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта	7	3
		Б1.В.08 Методология построения защищенных автоматизированных систем	8	4
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4
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	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 - преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3

**Таблица соответствия уровней освоения компетенций ПК-5, 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-5	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	<p>Раздел 1. Управление деятельностью предприятия; классификация информационных систем (ИС). Этапы разработки</p> <p>Раздел 2. Понятие корпоративных сетей. Комплексная информационно-вычислительная сеть ЖТ</p> <p>Раздел 3. Организационная и функциональная части АСУ ЖТ</p> <p>Раздел 4. Архитектура ЕК АСУФР</p> <p>Раздел 5. Концепция вычислительной инфраструктуры ЕК АСУФР. Технические требования</p> <p>Раздел 6. Концептуальные аспекты защиты информации и обеспечения информационной безопасности</p> <p>Раздел 7. Правовой режим информационных ресурсов ЖТ</p> <p>Раздел 8. Защита информационных и технических ресурсов от несанкционированного межсетевоего доступа в сетях ЖТ</p> <p>Раздел 9. Идентификация и аутентификация абонентов и объектов сети ЖТ</p> <p>Раздел 10. Обеспечение целостности информации в АС ЖТ</p> <p>Раздел 11. Защищенные виртуальные сети (VPN). Реализация</p>	Минимальный уровень	<p>Знать: Положение по аттестации объектов информатизации по требованиям безопасности информации в области железнодорожного транспорта;</p> <p>Уметь: Осуществлять предварительное ознакомление с аттестуемым объектом;</p> <p>Владеть: Основными понятиями в области аттестации объектов информатизации и знанием требований безопасности информации в области железнодорожного транспорта (систем управления РЖД).</p>
		Базовый уровень	<p>Знать: Порядок проведения аттестации и контроля объекта информатизации по требованиям безопасности информации;</p> <p>Уметь: Проводить аттестационные испытания объектов информатизации;</p> <p>Владеть: Навыками проведения аттестационных испытаний объектов информатизации по требованиям безопасности.</p>	
		Высокий уровень	<p>Знать: Требования к нормативным и методическим документам по аттестации объектов информатизации;</p> <p>Уметь: Разрабатывать методику проведения аттестации объекта информатизации, учитывая требования нормативных и методических документов по аттестации объектов информатизации;</p> <p>Владеть: Навыками анализа результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждения заключения по результатам аттестации.</p>	

		<p>VPN в сетях ЖТ</p> <p>Раздел 12. Средства защиты информации в системах баз данных</p> <p>СБД АС ЖТ</p> <p>Раздел 13. Средства антивирусной защиты в корпоративных сетях ФЖТ</p> <p>Раздел 14. Контроль знаний</p>		
ПК-15	<p>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</p>	<p>Раздел 1. Управление деятельностью предприятия; классификация информационных систем (ИС). Этапы разработки</p> <p>Раздел 2. Понятие корпоративных сетей. Комплексная информационно-вычислительная сеть ЖТ</p> <p>Раздел 3. Организационная и функциональная части АСУ ЖТ</p> <p>Раздел 4. Архитектура ЕК АСУФР</p> <p>Раздел 5. Концепция вычислительной инфраструктуры ЕК АСУФР. Технические требования</p> <p>Раздел 6. Концептуальные аспекты защиты информации и обеспечения информационной безопасности</p> <p>Раздел 7. Правовой режим информационных ресурсов ЖТ</p> <p>Раздел 8. Защита информационных и технических ресурсов от несанкционированного межсетевоего доступа в сетях ЖТ</p> <p>Раздел 9. Идентификация и аутентификация абонентов и объектов сети ЖТ</p> <p>Раздел 10. Обеспечение целостности информации в АС ЖТ</p> <p>Раздел 11.</p>	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> <p>Владеть: Профессиональной терминологией в области управления ИБ</p>
			Базовый уровень	<p>Знать: Основные методы управления информационной безопасностью</p> <p>Уметь: Разрабатывать предложения по совершенствованию системы управления ИБ АС</p> <p>Владеть: Методиками ФСТЭК России, ФСБ России по аттестации и сертификации объектов информатизации</p>
			Высокий уровень	<p>Знать: Основные положения стандартов единой системы конструкторской и программной документации (ФСТЭК России, ФСБ России)</p> <p>Уметь: Методы аттестации уровней защищенности АС</p> <p>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</p>

		Защищенные виртуальные сети (VPN). Реализация VPN в сетях ЖТ Раздел 12. Средства защиты информации в системах баз данных СБД АС ЖТ Раздел 13. Средства антивирусной защиты в корпоративных сетях ФЖТ Раздел 14. Контроль знаний		
--	--	--	--	--

**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)
7 семестр				
1	1	Текущий контроль	Тема «Состав и формирование требований, проектируемых автоматизированных ИС»	ПК-5, ПК-15 Реферат (письменно)
2	1	Текущий контроль	Тема «Состав и формирование требований, проектируемых автоматизированных ИС»	ПК-5, ПК-15 Доклад, сообщение (устно)
3	2	Текущий контроль	Тема «Базовые технологии дорожного (регионального) уровня»	ПК-5, ПК-15 Реферат (письменно)
4	2	Текущий контроль	Тема «Базовые технологии дорожного (регионального) уровня»	ПК-5, ПК-15 Доклад, сообщение (устно)
5	3	Текущий контроль	Тема «Открытая система R3; архитектура «клиент-сервер»; масштабируемость системы R3»	ПК-5, ПК-15 Реферат (письменно)
6	3	Текущий контроль	Тема «Открытая система R3; архитектура «клиент-сервер»; масштабируемость системы R3»	ПК-5, ПК-15 Доклад, сообщение (устно)
7	4	Текущий контроль	Тема «Функциональные, дорожные и обеспечивающие под проекты»	ПК-5, ПК-15 Реферат (письменно)
8	4	Текущий контроль	Тема «Функциональные, дорожные и обеспечивающие под проекты»	ПК-5, ПК-15 Доклад, сообщение (устно)
9	5	Текущий контроль	Тема «Технические требования к ЕК АСУФР. Виды обеспечения выполнения технических требований. Стратегия реализации проекта»	ПК-5, ПК-15 Реферат (письменно)
10	5	Текущий контроль	Тема «Технические требования к ЕК АСУФР. Виды обеспечения выполнения технических требований. Стратегия реализации проекта»	ПК-5, ПК-15 Доклад, сообщение (устно)
11	6	Текущий контроль	Тема «ЕК АСУФР: защита информации на сетевом уровне»	ПК-5, ПК-15 Реферат (письменно)
12	6	Текущий контроль	Тема «ЕК АСУФР: защита информации на сетевом уровне»	ПК-5, ПК-15 Доклад, сообщение (устно)
13	6	Текущий контроль	Тема «Стандарты в области защиты информации»	ПК-5, ПК-15 Реферат (письменно)
14	7	Текущий контроль	Тема «Стандарты в области	ПК-5, ПК-15 Доклад, сообщение (устно)

			защиты информации»	ПК-15	(устно)
15	7	Текущий контроль	Тема «Межсетевой экран Cisco PIX Firewall»	ПК-5, ПК-15	Реферат (письменно)
16	7	Текущий контроль	Тема «Межсетевой экран Cisco PIX Firewall»	ПК-5, ПК-15	Доклад, сообщение (устно)
17	8	Текущий контроль	Тема «Протоколы взаимной проверки подлинности объектов»	ПК-5, ПК-15	Реферат (письменно)
18	8	Текущий контроль	Тема «Протоколы взаимной проверки подлинности объектов»	ПК-5, ПК-15	Доклад, сообщение (устно)
19	9	Текущий контроль	Тема «Отечественный стандарт хеширования»	ПК-5, ПК-15	Реферат (письменно)
20	9	Текущий контроль	Тема «Отечественный стандарт хеширования»	ПК-5, ПК-15	Доклад, сообщение (устно)
21	10	Тест	Изученный материал	ПК-5, ПК-15	Перечень тестовых заданий
22	11	Текущий контроль	Тема «Средства создания VPN»	ПК-5, ПК-15	Реферат (письменно)
23	11	Текущий контроль	Тема «Средства создания VPN»	ПК-5, ПК-15	Доклад, сообщение (устно)
24	12	Текущий контроль	Тема «RACF как средство доступа к наборам данных и ресурсам систем»	ПК-5, ПК-15	Реферат (письменно)
25	12	Текущий контроль	Тема «RACF как средство доступа к наборам данных и ресурсам систем»	ПК-5, ПК-15	Доклад, сообщение (устно)
26	13	Текущий контроль	Тема «Средства антивирусной защиты»	ПК-5, ПК-15	Реферат (письменно)
27	13	Текущий контроль	Тема «Средства антивирусной защиты»	ПК-5, ПК-15	Доклад, сообщение (устно)
28	14	Промежуточная аттестация – экзамен	Разделы: 1. Управление деятельностью предприятия; классификация информационных систем (ИС). Этапы разработки 2. Понятие корпоративных сетей. Комплексная информационно-вычислительная сеть ЖТ 3. Организационная и функциональная части АСУ ЖТ 4. Архитектура ЕК АСУФР 5. Концепция вычислительной инфраструктуры ЕК АСУФР. Технические требования 6. Концептуальные аспекты защиты информации и обеспечения информационной безопасности 7. Правовой режим информационных ресурсов ЖТ 8. Защита информационных и технических ресурсов от несанкционированного межсетевого доступа в сетях ЖТ 9. Идентификация и аутентификация абонентов и объектов сети ЖТ 10. Обеспечение целостности информации в АС ЖТ 11. Защищенные виртуальные сети (VPN). Реализация VPN в сетях ЖТ	ПК-5, ПК-15	Оценка качества ответов на вопросы преподавателя в ходе беседы по теме вопроса; устно; оценка ответов на вопросы теста.

			12. Средства защиты информации в системах баз данных СБД АС ЖТ 13. Средства антивирусной защиты в корпоративных сетях ФЖТ 14. Контроль знаний		
--	--	--	---	--	--

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	Экзамен	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 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

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
«отлично»	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
«хорошо»	Обучающийся с небольшими неточностями 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	Базовый
«удовлетворительно»	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
«неудовлетворительно»	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.) 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

Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий
Минимальный уровень освоения компетенции	30	Тестовые задания с выбором одного правильного ответа из нескольких
		Тестовые задания с выбором нескольких правильных ответов из множества ответов
		Тестовые задания на установление соответствия
		Тестовые задания на установление правильной последовательности
Базовый уровень освоения компетенции	7	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)
Высокий уровень освоения компетенции	3	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено» Обучающийся при тестировании набрал 93-99 баллов	Высокий

«хорошо»		Обучающийся при тестировании набрал 76-92 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 60-75 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-59 баллов	Компетенция не сформирована

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. Основные направления развития АСУ на ЖДТ
2. Схема автоматизированной системы управления ЖДТ
3. Основные виды АСУ применяемые на ЖДТ
4. Основные направления применения спутниковых технологий на ЖДТ
5. Схема многоуровневой системы безопасности
6. Задачи ОАО РЖД в области внедрения спутниковых технологий
7. Основные функции интеллектуального железнодорожного транспорта
8. Основные функции интеллектуального поезда
9. Назначение технических средств регулирования и обеспечения безопасности движения поездов
10. Классификация систем интервального регулирования движения поездов
11. Схема системы управления маршрутами
12. Принципы построения многоуровневой системы управления движением поездов и обеспечение их безопасности
13. Назначение трех уровней структуры системы АБТЦ-М
14. Назначение и функции АРМ дежурного по станции (АРМ-ДСП-АБ)
15. Комплексное локомотивное устройство безопасности (КЛУБ-У) назначение
16. Наименование основных блоков комплексного локомотивного устройства безопасности (КЛУБ-У)
17. Схема прогрессивной системы интервального регулирования движением поездов
18. Назначение информационных технологий в АСУ ЖДТ
19. Автоматизированная системы управления контейнерными перевозками

3.2 Перечень типовых тем докладов, сообщений

1. Основные направления развития АСУ на ЖДТ
2. Схема автоматизированной системы управления ЖДТ
3. Основные виды АСУ применяемые на ЖДТ
4. Основные направления применения спутниковых технологий на ЖДТ
5. Схема многоуровневой системы безопасности
6. Задачи ОАО РЖД в области внедрения спутниковых технологий
7. Основные функции интеллектуального железнодорожного транспорта
8. Основные функции интеллектуального поезда
9. Назначение технических средств регулирования и обеспечения безопасности движения поездов
10. Классификация систем интервального регулирования движения поездов

11. Схема системы управления маршрутами
12. Принципы построения многоуровневой системы управления движением поездов и обеспечение их безопасности
13. Назначение трех уровней структуры системы АБТЦ-М
14. Назначение и функции АРМ дежурного по станции (АРМ-ДСП-АБ)
15. Комплексное локомотивное устройство безопасности (КЛУБ-У) назначение
16. Наименование основных блоков комплексного локомотивного устройства безопасности (КЛУБ-У)
17. Схема прогрессивной системы интервального регулирования движением поездов
18. Назначение информационных технологий в АСУ ЖДТ

3.3 Тестирование по дисциплине

3.3.1 Структура фонда тестовых заданий по дисциплине

Структура тестовых материалов по дисциплине «Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта»

Раздел дисциплины	Количество ТЗ, типы ТЗ
Раздел 1. Управление деятельностью предприятия; классификация автоматизированных систем (АС). Организационная и функциональная части АСУ ЖТ	10 – тип А 10 - тип В 10 – тип С 6 – тип D
Итого по разделу	$\sum 36$ 10 – тип А 10-тип В 10 – тип С 6 – тип D
Раздел 2. Концептуальные аспекты защиты информации и обеспечения информационной безопасности в сетях ЖТ	20 – тип А 10 - тип В 3 – тип С 3 – тип D
Итого по разделу	$\sum 36$ 20– тип А 10 - тип В 3 – тип С 3 – тип D
Итого по дисциплине	$\sum 72$ 30– тип А 20 - тип В 13– тип С 9 – тип D

Используемые типы тестовых заданий (ТЗ):

ТЗ типа А: тестовое задание закрытой формы (ТЗ с выбором одного или нескольких правильных ответов);

ТЗ типа В: тестовое задание открытой формы (с конструируемым ответом: ТЗ с кратким регламентируемым ответом (ТЗ дополнения); ТЗ свободного изложения (с развернутым ответом в произвольной форме);

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа D: тестовое задание на установление правильной последовательности.

3.3.2. Структура и образец типового итогового теста по дисциплине «Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта» за весь период ее освоения

Структура типового итогового теста по дисциплине за весь период ее освоения

Раздел дисциплины	Количество ТЗ, типы ТЗ
Раздел 1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	3 – тип А 3 – тип В 1 – тип С
Итого по разделу	$\Sigma 7$ 3 – тип А 3 – тип В 1 – тип С
Раздел 2. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	3 – тип А 3 – тип В 1 – тип С 1 – тип D
Итого по разделу	$\Sigma 8$ 3 – тип А 3 – тип В 1 – тип С 1 – тип D
Итого по дисциплине	$\Sigma 15$ 6 – тип А 6 – тип В 2 – тип С 1 – тип D

Образец типового итогового теста по дисциплине за весь период ее освоения

Описание требований к тесту: тематика теста; перечень знать, уметь, владеть; виды и количество предъявляемых обучающемуся тестовых заданий; проходной балл; критерии оценки; норма времени; дополнительные требования, включая необходимость использования справочных таблиц и проч.

Описание требований к тесту.

1. Тестирование осуществляется по двум изученным в семестре разделам (раздел 1 – Организация аттестации объектов информатизации на соответствие требованиям безопасности информации, раздел 2 - Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации).

2. Обучающемуся случайным образом дается 25 тестовых заданий из ФТЗ. Время на подготовку – 60 минут.

3. Оценивание осуществляется по 100-балльной системе. Для получения допуска к экзамену обучающийся должен набрать более 69 баллов.

Описание требований к тесту: итоговый тест по дисциплине «Аттестация объектов информатизации» предполагает оценку того, насколько студент:

– знает: основные нормативные правовые акты и стандарты по аттестации объектов информатизации; основные угрозы безопасности информации для объектов информатизации; основные документы, разрабатываемые в процессе аттестации объектов информатизации; основные требования по проверке работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации; основные требования к сертификации средств защиты информации автоматизированных систем.

– умеет: применять нормативные правовые акты в профессиональной деятельности;

проводить анализ защищенности автоматизированных систем в ходе аттестации объектов информатизации; разрабатывать и анализировать проектные решения в процессе

аттестации объектов информатизации; проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

Владеть навыками: работы с нормативными правовыми актами и методическими документами; анализа защищенности объектов информатизации; проектных решения в процессе аттестации объектов информатизации; проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации; экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; проведения инструментального мониторинга защищенности информации в автоматизированной системе;

разработки политик информационной безопасности в процессе аттестации объектов информатизации; формирования комплекса мер (правила, процедуры, методы) для защиты информации ограниченного доступа автоматизированной системы; применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности в процессе аттестации объектов информатизации.

Студенту необходимо выполнить 41 тестовых заданий. Максимальное количество составляет 100%. Проходной составляет 75%. Обучающийся, набравший более 75% правильных ответов сдал тест, менее 75% – нет. Время на выполнение тестового задания – 60 минут.

Образец типового теста содержит задания для оценки знаний, для оценки умений, для оценки навыков и (или) опыта деятельности (необходимо указать все правильные ответы).

Образец типового итогового теста по дисциплине за весь период освоения

1. Главные цели АСУ ЖТ:

- А. Совершенствование качества управления работой отрасли и, прежде всего, ее эксплуатационной деятельностью, оптимизация всех видов планирования и оперативного руководства работой производственных звеньев;
- Б. Наилучшее использование автоматизированных систем;
- В. Повышение производительности работы.

2. Основные виды АСУ, применяемые на ЖДТ

- А. АС ЭТРАН — автоматизированная система централизованной подготовки и оформления перевозочных документов;
- Б. 1С Бухгалтерия;
- В. 1С Зарплата и управление персоналом.

3. Наименование документа, определяющее требования корпоративной политики информационной безопасности:

- А. Распоряжение ОАО РЖД №1872р;
- Б.ГОСТ Р ИСО/МЭК 27001-2006;

В. Распоряжение ОАО РЖД № 3062р

4. Состав комплекса информационных технологий в ОАО РЖД
 - А. Управление перевозочным процессом;
 - Б. Управление инфраструктурой железнодорожного транспорта;
 - В. Управление маркетингом, экономикой и финансами.
5. Базовые механизмы обеспечения безопасности: АСУ «Экспресс-3»
 - А. Идентификация и аутентификация пользователей и взаимодействующих объектов;
 - Б. Управление доступом, понимаемое как избирательное разрешение или отклонение запросов авторизованных пользователей (объектов) на доступ к ресурсам;
 - В. Конфиденциальность данных, гарантирующая их раскрытие только теми людьми (объектами), которым они предназначены.
6. Криптографические шлюзы (VPN) назначение:
 - А. Обеспечение защиты от вторжения со стороны сетей передачи данных (Интернет), обеспечения конфиденциальности при передаче информации по открытым каналам связи (VPN), а также организации безопасного доступа пользователей к ресурсам сетей общего пользования;
 - Б. Обеспечение аутентификации;
 - В. Настройки параметров безопасности операционной системы.
7. Основные функции криптошлюзов:
 - А. Обеспечение конфиденциальности и целостности данных;
 - Б. Функции межсетевых экранов;
 - В. Проверка подлинности
8. Контроль доступа в сеть (Network Access Control – NAC- основные функции:
 - А. Глубокий анализ трафика, выявления и предотвращения атак и фактов несанкционированной или запрещённой активности;
 - Б. Система контроля доступа в сеть, обеспечивающая централизованное управление политиками идентификации пользователей и устройств, политиками их доступа к КИС;
 - В. Разграничение доступа.
9. Защита и контроль web-трафика (Web Security)- состав, функции
 - А. Защита от шпионских программ, вредоносного мобильного кода, фишинга, ботов, и другие;
 - Б. Проверка подлинности пользователя;
 - В. Функции межсетевых экранов.
10. Сетевые системы предотвращения вторжений (Network IPS)- функции:
 - А. Функции межсетевых экранов;
 - Б. Анализа и контроля трафика;
 - В. Защита от шпионских программ, вредоносного мобильного кода.
11. Руководящий документ по реализации обязательных мероприятий при проведении работ по защите информации в АСУ:
 - А. Приказ ФСТЭК России N 21;

- Б. Приказ ФСТЭК России N 17;
В. Приказ ФСТЭК России N 31.
12. Требования к проведению работ по защите информации в АСУ
- А. Формирование требований к защите информации в автоматизированной системе управления производственными и технологическими процессами; разработка системы защиты автоматизированной системы управления; внедрение системы защиты автоматизированной системы управления;
Б. Аттестация автоматизированной системы;
В. Лицензирование.
13. Руководящий документ для моделирования угроз ИБ:
- А. Методика оценки угроз безопасности информации» Утвержден ФСТЭК России 5 февраля 2021;
Б. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.);
В. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007г.).
14. Целью определения угроз безопасности информации является:
- А. Установления потенциальных угроз безопасности;
Б. Установления потенциальных уязвимостей АС ТП;
В. Установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе.
15. Руководящий документ РЖД об организации работ по обеспечению защиты информации в автоматизированных системах управления:
- А. Распоряжение N 543р;
Б. Распоряжение № 2688р;
В. Распоряжение №130р.

3.4 Перечень теоретических вопросов к экзамену

1. Основные направления развития АСУ на ЖДТ
2. Схема автоматизированной системы управления ЖДТ
3. Основные виды АСУ применяемые на ЖДТ
4. Основные направления применения спутниковых технологий на ЖДТ
5. Схема многоуровневой системы безопасности
6. Задачи ОАО РЖД в области внедрения спутниковых технологий
7. Основные функции интеллектуального железнодорожного транспорта
8. Назначение технических средств регулирования и обеспечения безопасности движения поездов
9. Классификация систем интервального регулирования движения поездов
10. Схема системы управления маршрутами
11. Принципы построения многоуровневой системы управления движением поездов и обеспечение их безопасности

12. Назначение трех уровней структуры системы АБТЦ-М
13. Назначение и функции АРМ дежурного по станции (АРМ-ДСП-АБ)
14. Комплексное локомотивное устройство безопасности (КЛУБ-У) назначение
15. Наименование основных блоков комплексного локомотивного устройства безопасности (КЛУБ-У)
16. Схема прогрессивной системы интервального регулирования движением поездов
17. Назначение информационных технологий в АСУ ЖДТ
18. Прикладные системы и комплексы задач Главного вычислительного центра ОАО «РЖД»
19. Автоматизированная система управления пассажирскими перевозками (АСУПП) «Экспресс» краткая характеристика
20. Краткое описание комплекса защиты информации АСУ «Экспресс-3
21. Криптографические шлюзы (VPN) описание, назначение, функции
22. Аутентификация –определение, состав, функции корпоративной системы аутентификации
23. Контроль доступа в сеть (Network Access Control – NAC- состав, основные функции
24. Защита и контроль web-трафика (Web Security)- состав, функции
25. Сетевые системы предотвращения вторжений (Network IPS)- состав, функции
26. Автоматизированная система управления грузовыми перевозками (АСУГП) краткая характеристика
27. Основные функции, реализованные в системе АСОУП 2
28. Способы защиты информации в АСОУП 2
29. Автоматизированная система управления тяговыми ресурсами ДИСТПС назначение, объекты управления
30. Автоматизированная система управления контейнерными перевозками (ДИСКОН) назначение, функции, объекты управления
31. Перечень обязательных мероприятий при проведении работ по защите информации в АСУ
32. Требования к проведению работ по защите информации в АСУ
33. Уровни безопасности автоматизированной системы
34. Требование к модели угроз безопасности в АСУ
35. Защита автоматизированной системы управления при проектировании
36. Требования к разработке системы защиты автоматизированной системы управления
37. Внедрение системы защиты автоматизированной системы управления и ввод ее в действие
38. Настройка параметров программирования системы
39. Требования к организационно-распорядительным документам
40. Требования при внедрении мер защиты информации
41. Предварительные испытания системы защиты
42. Анализ уязвимостей автоматизированной системы
43. Приемочные испытания системы
44. Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления
45. Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления
46. Требования к мерам защиты информации в автоматизированной системе управления

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 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 на следующем занятии после проведения контрольно-оценочного мероприятия (или указание другого срока информирования); оцененные/проверенные работы преподаватель возвращает обучающимся.
Сообщение, доклад	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 1-2 источников, включая самостоятельный поиск в интернете), готовит сообщение (доклад) по результатам освоения темы, объемом до 15 стр. текста размером 12 пунктов, интервал 1,2; предоставляет сообщение (доклад) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы на следующем занятии после проведения контрольно-оценочного мероприятия (или указание другого срока информирования); оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы на следующем занятии после проведения контрольно-оценочного мероприятия (или указание другого срока информирования); 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 экзамену для оценки знаний;
- перечень типовых простых практических заданий к экзамену для оценки умений;
- перечень типовых практических заданий к экзамену 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

 <p>ИрГУПС 2016-2017 учебный год</p>	<p>Экзаменационный билет № 1 по дисциплине « _____ » _____ семестр</p>	<p>Утверждаю: Заведующий кафедрой « _____ » ИрГУПС _____</p>
<p>1 Внедрение системы защиты автоматизированной системы управления и ввод ее в действие 2 Способы защиты информации в АСОУП 2 3 Схема автоматизированной системы управления ЖДТ Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм</p>		