АННОТАЦИЯ
дисциплины
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ И ИНФОРМАЦИОННО-ЛОГИСТИЧЕСКИХ СИСТЕМ ТРАНСПОРТА»

Направление подготовки – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – специалист

Специализация – «Информационная безопасность автоматизированных систем на транспорте»

1. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность информационно-управляющих и информационно-логистических систем транспорта» (Б1.Б.36) относится к базовой части и является обязательной дисциплиной.

2. Цель и задачи дисциплины

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин профессионального цикла в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатационная и специализацией «Информационная безопасность автоматизированных систем на транспорте».

Для достижения поставленной цели определены следующие задачи изучения дисциплины:

– подготовка студента по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;

– подготовка студента к изучению дисциплин, определённых учебным планом в соответствии с указанными компетенциями;

– развитие социально-воспитательного компонента учебного процесса.

При изучении дисциплины решаются следующие конкретные задачи:

– изучение методологии проведения комплексного анализа защищенности и инструментального мониторинга информационно-логистических и информационно-управляющих систем на транспорте;

– изучение принципов проектирования и оценивания надежности результатов разработки программных элементов информационно-логистических и информационно-управляющих систем на транспорте;

– анализ возможностей эксплуатации программно-аппаратных средств защиты информационно-логистических и информационно-управляющих систем с учетом специфики угроз информации в них.

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование следующих профессионально-специализированных компетенций:

– способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно логистических систем на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-10.1);

– способностью осуществлять рациональный выбор средств и разрабатывать предложения по обеспечению информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.3);

– способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом нормативных требований по защите информации (ПСК-10.4).

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

– основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;

УМЕТЬ:

– используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на транспорте;

– реализовывать системы защиты информации в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах на транспорте в соответствии со стандартами по оценке защищенных систем;

– анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте, применять автоматизированные средства мониторинга, аудита и анализа защищенности данных систем;

ВЛАДЕТЬ:

– навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте;

– навыками анализа угроз и навыками построения политик безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта;

– методами эксплуатации средств защиты информации;

– системным подходом к организации информационных процессов (в том числе систем управления ресурсами предприятия и технологий поддержки жизненного цикла), анализу информационной безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта.

4. Содержание и структура дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
		Модуль 1
1	Информационная безопасность систем управления движением поездов, пассажирскими и грузовыми перевозками	Общая характеристика информационно-управляющих систем как объектов информационной безопасности. Информационные системы сети центров управления перевозками. Структура и основные функции центров управления перевозками (ЦУП). Информационное обеспечение ЦУП. Программно-технический комплекс единого диспетчерского центра управления (ЕДЦУ). Подсистема, методы и средства обеспечения информационной безопасности ЕДЦУ. Защищаемые объекты и угрозы информационной безопасности информационных систем управления движением (системы железнодорожной автоматики и телемеханики, бортовые системы управления, системы диспетчерского управления). Подсистема, методы и средства обеспечения информационной безопасности и защиты информации информационных систем управления движением.
		Модуль 2
2	Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем	Общая характеристика сетевой интегрированной корпоративной информационно-управляющей системы «СИРИУС». Подсистема, методы и средства обеспечения информационной безопасности и защиты информации системы «СИРИУС». Общая характеристика, методы и средства обеспечения информационной безопасности и защиты информации автоматизированной системы оперативного управления перевозками (АСОУП), АСУ «Грузовой экспресс», АСУ вагонным и контейнерным парком. Общая характеристика системы «ГИД “Урал-ВНИИЖТ”». Состав и основные компоненты центрального комплекса системы ГИД. Взаимодействие подсистем, АРМов и пользователей ГИД. Подсистемы, методы и средства обеспечения информационной безопасности и защиты информации системы «ГИД “Урал-ВНИИЖТ”». Назначение и структура автоматизированного комплекса системы фирменного транспортного обслуживания (АКС ФТО). Функции и

		характеристика программно-аппаратной платформы АС «ЭТРАН». АС «ЭТРАН» как объект информационной безопасности.
3	Информационная безопасность автоматизированных систем управления пассажирскими перевозками	Общая характеристика информационно-логистических систем как объектов информационной безопасности. Назначение, состав и основные функциональные подсистемы АСУ «Экспресс-3». Программно - аппаратный комплекс АСУ «Экспресс-3». Угрозы и защищаемые объекты АСУ «Экспресс-3». Система обеспечения информационной безопасности АСУ «Экспресс-3». Средства обеспечения информационной безопасности АСУ «Экспресс-3».
Модуль 3		
4	Системы защиты информации и обеспечения информационной безопасности корпоративного и дорожного уровней	Назначение и архитектура систем управления доступом. Примеры типовых систем управления доступом. Система учета и регистрации заявок на доступ к информационным ресурсам ОАО «РЖД». Основные принципы и требования к построению системы антивирусной защиты. Система антивирусной защиты ОАО «РЖД». Защищенный сегмент электронной почтовой системы (ЭПС). Принципы построения и функционирования ЭПС ОАО «РЖД». Методы и средства обеспечения информационной безопасности и защиты информации ЭПС. Защищенный электронный технологический документооборот (ЭТД). Принципы построения, функционирования и защиты информации ЭТД ОАО «РЖД». Средства аудита информационной безопасности и защиты информации региона ведения железной дороги. Типовые программно-аппаратные средства защиты информации региона ведения железной дороги. Основные решения и средства обеспечения информационной безопасности, применяемые в СПД и ЛВС подразделений ОАО «РЖД». Сетевые средства защиты информации.

5. Объем дисциплины и виды учебной работы

Объем дисциплины – 3 зачетных единицы (108 час.), в том числе:

лекции – 32 час.

лабораторные работы – 16 час.

самостоятельная работа – 51 час.

контроль – 9 час.

Форма контроля знаний – зачет.