Аннотация рабочей программы дисциплины/практики
Б1.В.22 Безопасность информационных технологий и систем
Специальность/направление подготовки: 09.03.02 Информационные системы и технологии
Специализация/профиль: Информационные системы и технологии на транспорте

1. Цели освоения дисциплины(модуля)/практики
Целью изучения дисциплины "Безопасность информационных технологий и систем" является формирование у обучаемых знаний, умений и навыков (уровня сформированности соответствующих компетенций) в результате последовательного изучения содержательно связанных между собой разделов (тем) учебных занятий, а также подготовить студентов к организации и эксплуатации средств защиты компьютерной информации.

2. Компетенции, формируемые в результате освоения дисциплины (модуля)\ практики	
УК-8: Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	
Индикатор	УК-8.1. Знать: классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения; причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций; принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации.
Индикатор	УК-8.2. Уметь: поддерживать безопасные условия жизнедеятельности; выявлять признаки, причины и условия возникновения чрезвычайных ситуаций; оценивать вероятность возникновения потенциальной опасности и принимать меры по ее предупреждению.
Индикатор	УК-8.3. Владеть: методами прогнозирования возникновения опасных или чрезвычайных ситуаций; навыками по применению основных методов защиты в условиях чрезвычайных ситуаций.
ПКР-1: Способность выполнять интеграцию программных модулей и компонент	
Индикатор	ПКР-1.1. Знать: методы и средства интеграции модулей и компонент программного обеспечения; интерфейсы взаимодействия модулей системы между собой и с внешней средой; методы и средства разработки процедур развертывания программного обеспечения; методы и средства верификации работоспособности выпусков программной продукции; языки, утилиты и среды программирования, средства пакетного выполнения процедур.
Индикатор	ПКР-1.2. Уметь: Выполнять процедуры сборки программных модулей и компонент в программный продукт. Проводить оценку работоспособности программного продукта; документировать произведенные действия, выявленные проблемы и способы их устранения; производить настройки параметров программного продукта и осуществлять запуск процедур сборки; проводить оценку работоспособности программного продукта; создавать резервные копии программ и данных, выполнять восстановление, обеспечивать целостность программного продукта и данных.
Индикатор	ПКР-1.3. Иметь навыки: интеграции программных компонент собственной разработки и приобретенных; разработки и осуществления процедур верификации выпусков (сборок) программной продукции.
ПКС-2: Способность разрабатывать, эксплуатировать, ремонтировать электронные устройства цифровой автоматики на железной дороге	
Индикатор	ПКС-2.1. Знать: принципы проектирования, разработки и эксплуатации устройств цифровой автоматики на железной дороге, включая программируемые с использованием микропроцессоров и микроконтроллеров.
Индикатор	ПКС-2.2. Уметь: разрабатывать устройства цифровой автоматики, осуществлять техническое обслуживание, поиск и устранение неисправностей с применением современных программных и аппаратных инструментов; разрабатывать и применять проектную и эксплуатационную техническую документацию устройств цифровой автоматики.
Индикатор	ПКС-2.3. Иметь навыки: разработки устройств цифровой автоматики, их документирования, поиска и устранения неисправностей с применением современных аппаратных и аппаратных инструментов.
ПКС-3: Способность разрабатывать и модифицировать программное обеспечение, включая написание и отладку программных компонент	
Индикатор	ПКС-3.1. Знать: базовые принципы и современные методы алгоритмизации, написания программ и автономной отладки при программировании последовательных, параллельных, распределенных приложений, приложений реального времени; современные языки и средства программирования.
Индикатор	ПКС-3.2. Уметь: осуществлять разработку и формализованное описание алгоритма решения задачи на современных языках программирования и манипулирования данными, разрабатывать и применять процедуры автономной отладки.
Индикатор	ПКС-3.3. Иметь навыки: алгоритмизации, разработки и автономной отладки программных модулей и компонент с использованием современных языков и средств программирования и манипулирования данными при создании последовательных, параллельных, распределенных приложений и приложений

	реального времени.

3. В результате освоения дисциплины (модуля)/практики обучающийся должен

3.1	**Знать:**
3.1.1	принципы и методы организации угроз, атак и вторжения; - модели безопасности и секретности.
3.2	**Уметь:**
3.2.1	обнаруживать угрозы, атаки и вторжения, шифровать
3.3	**Владеть:**
3.3.1	программными и техническими средства защиты компьютерной информации.

4. Структура и содержание дисциплины (модуля)/практики

Наименование разделов
Раздел 1. Основные понятия и положения защиты информации в компьютерных системах
Введение. Доктрина информационной безопасности России. Основные понятия и определения информационной безопасности. /Лек/
Понятия экономической и информационной безопасности. Ключевые вопросы ИБ. Экономическая и информационная безопасность. Составляющие информационной безопасности. /Лек/
Предмет и объект защиты. Угрозы безопасности информации в компьютерных системах. /Лек/
Виды угроз информационной безопасности и классификация источников угроз. Основные виды защищаемой информации. /Лек/
Краткий обзор зарубежного законодательства в области информационной безопасности. Российское законодательство в области информационной безопасности. Закон «Об информации, информационных технологиях и защите информации». Другие законы и нормативные акты. /Лек/
Основы законодательства в области обеспечения информационной безопасности /Пр/
Раздел 2. Направления обеспечения информационной безопасности.
Правовая защита. Организационная защита. Инженерно-техническая защита. /Лек/
Программные средства защиты. Криптографические средства защиты. /Лек/
Хакерские утилиты и прочие вредоносные программы. Классические компьютерные вирусы. Скрипт-вирусы. Троянские программы. Сетевые черви. /Пр/
Обеспечение антивирусной защиты операционных систем на основе продуктов компании «Лаборатория Касперского». /Пр/
От чего надо защищаться в первую очередь? Как надо защищаться? Антивирусная защита. Современные средства биометрической идентификации. /Пр/
Идентификация и аутентификация. Парольная зашита. /Пр/
Классические методы шифрования. /Лаб/
Изучение криптографического стандарта DES /Лаб/
Изучение криптографического стандарта ГОСТ 28147-89 /Лаб/
Раздел 3. Построения системы информационной безопасности
Основные аспекты построения системы информационной безопасности. Программа информационной безопасности. Модели ИБ, требования и основные этапы реализации информационной безопасности. /Лек/
Мероприятия по защите информации. Политика информационной безопасности. /Лек/
Анализ и управление рисками при реализации информационной безопасности. Соотношение эффективности и рентабельности систем информационной безопасности. /Лек/
Раздел 4. Защита информации в информационных системах и компьютерных сетях
Определение защищенной информационной системы. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. /Лек/
Методология анализа защищенности информационной системы. Концепция защищенных виртуальных частных сетей. /Лек/
Раздел 5. Защита информации от утечки по техническим каналам
Способы защиты информации. Характеристика защитных действий. /Лек/
Защита информации от утечки по визуально-оптическим каналам. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным. Защита информации от утечки по материально-вещественным каналам. /Лек/
Раздел 6. Противодействие несанкционированному доступу к источникам конфиденциальной информации
Способы несанкционированного доступа. Технические средства несанкционированного доступа к информации. Защита от наблюдения и фотографирования. Защита от подслушивания. /Лек/
Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра. /Лек/

Защита от копирования. /Лаб/
Передача зашифрованных сообщений по электронной почте /Лаб/
Раздел 7. Защита информации в электронных платежных системах
Принципы функционирования электронных платежных систем. Электронные пластиковые карты. /Лек/
Персональный идентификационный номер. Универсальная электронная платежная система UEPS. Обеспечение безопасности электронных платежей через сеть Internet. /Лек/
Раздел 8. Самостоятельная работа
Подготовка к лекциям /Ср/
Подготовка к практическим занятиям /Ср/
Подготовка к лабораторным занятиям /Ср/
Раздел 9. Контактные часы на аттестацию
Аттестация /КЭ/

Трудоёмкость: 5 ЗЕ.