АННОТАЦИЯ

Дисциплины

«Информационная безопасность и защита информации на транспорте»

Направление подготовки – 09.04.02 «Информационные системы и технологии»

Квалификация (степень) выпускника – магистр

Магистерская программа – «Информационные системы и технологии на транспорте»

**1. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Информационная безопасность и защита информации на транспорте» (Б1.В.ДВ.2.2) относится к вариантивной части и является дисциплиной по выбору.

**2. Цель и задачи дисциплины**

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других 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: организационно-управленческая, аналитическая, научно-исследовательская, педагогическая и специализацией «Информационные системы и технологии на транспорте».

Для достижения поставленной цели решаются следующие задачи:

* изучение принципов и методологии управления информационной безопасностью;
* изучение методов и процесса управления инцидентами информационной безопасности;
* изучение методологии проведения комплексного анализа защищенности и ин­ст­ру­мен­таль­ного мо­ни­то­рин­га автоматизированных транспортных систем.

**3. Перечень планируемых результатов обучения по дисциплине**

Изучение дисциплины направлено на формирование следующих **общекультурных компетенций (ОК)**:

* ОК-1) – способностью совершенствовать и развивать свой интеллектуальный и общекультурный уровень;
* (ОК-2) – способностью к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;

Изучение дисциплины направлено на формирование следующих **общепрофессиональных компетенций (ОПК)**:

* (ОПК-6) – способность анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями;

Изучение дисциплины направлено на формирование следующих **профессиональных компетенций (ПК)**, соответствующих виду профессиональной деятельности, на который ориентирована программа магистратуры:

* проектно-конструкторская деятельность:
* умением разрабатывать стратегии проектирования, определением целей проектирования, критериев эффективности, ограничений применимости (ПК-1);
* научно-исследовательская деятельность:
* способностью прогнозировать развитие информационных систем и технологий (ПК-13).

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

 источники и классификацию угроз информационной безопасности;

 основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

 основные методы управления информационной безопасностью;

УМЕТЬ:

 анализировать и оценивать угрозы информационной безопасности объекта;

 разрабатывать модели угроз и нарушителей информационной безопасности информационных транспортных систем;

 выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных транспортных систем;

 оценивать информационные риски в информационных транспортных системах;

 разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных транспортных систем;

ВЛАДЕТЬ:

 методами мониторинга и аудита, выявления угроз информационной безопасности информационных транспортных систем;

 методами управления информационной безопасностью информационных транспортных систем;

 методами оценки информационных рисков.

**4. Содержание и структура дисциплины**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Организационно-правовые аспекты и процессная модель управления информационной безопасностью | Основные понятия и определения. Система управления информационной безопасностью (СУИБ). Организационно-правовые аспекты построения и функционирования СУИБ. Технические аспекты построения СУИБ. Подходы к построению системы управления информационной безопасностью корпорации и корпоративных информационных систем и сетей. Процесс управления информационной безопасностью. Задание требований к системе управления информационной безопасностью. |
| 2 | Управление рисками информационной безопасности | Критерии и процессы управления рисками. Методология оценки рисков информационной безопасности. Примеры методов оценки риска, основанных на использовании таблиц. Методики построения систем защиты информации, включающие этап анализа рисков. Методики и программные продукты для оценки рисков. |
| 3 | Управление инцидентами информационной безопасности | Основные категории инцидентов. Процесс управления инцидентами. Нормативные документы по управлению инцидентами. Процедура управления инцидентами. Модель управления инцидентами. Формальное описание процесса управления инцидентами. Эффект от внедрения процесса управления инцидентами. Средства автоматизации процесса управления инцидентами. |
| 4 | Аудит информационной безопасности | Понятие аудита информационной безопасности. Концепция аудита информационной безопасности систем информационных технологий и организаций. Цель и задачи аудита информационной безопасности. Формы аудита информационной безопасности. Принципы аудита информационной безопасности. Виды аудита информационной безопасности. Основные этапы проведения аудита информационной безопасности. |
| 5 | Информационная безопасность ERP-систем | Система управления ресурсами предприятия (ERP-система). Понятие, назначение и функции ERP-систем. Общие принципы построения ERP-системы. Реализация ERP-системы на программно-аппаратной платформе SAPR/3.  Функции и состав Единой корпоративной автоматизированной системы управления финансами и ресурсами (ЕК АСУФР/ТР) Характеристика программно-аппаратного комплекса ЕК АСУФР/ТР. Характеристика угроз информационной безопасности ЕК АСУФР/ТР.  Подсистема, методы и средства обеспечения информационной безопасности ERP-систем. Характеристика объектов защиты и мер обеспечения информационной безопасности ЕК АСУФР/ТР. Система требований к информационной безопасности ЕК АСУФР/ТР. |
| 6 | Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем | 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. |
| 7 | 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». |

**5. Объем дисциплины и виды учебной работы**

Объем дисциплины – 5 зачетных единиц (180 час.), в том числе:

практические занятия – 18 час.

лабораторные работы – 18 час.

самостоятельная работа – 90 час.

Форма контроля знаний – экзамен.