АННОТАЦИЯ

Дисциплины

«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

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 «Управление информационной безопасностью» (Б1.Б.19) относится 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 принципов и методологии управления информационной безопасностью;

− изучение методов и процесса управления инцидентами информационной безопасности;

− изучение методов и процесса проведения аудита информационной безопасности для оценивания защищенности автоматизированных, информационно-управляющих и распределенных информационных транспортных систем и построения эффективной системы обеспечения информационной безопасности организации.

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

Изучение дисциплины направлено на формирование следующих профессиональных компетенций (ПК), соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

научно-исследовательская деятельность:

- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

проектно-конструкторская деятельность:

- способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

- способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

организационно-управленческая деятельность:

- способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

эксплуатационная деятельность:

- способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

- способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

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 автоматизированных систем;

- выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;

- оценивать информационные риски в автоматизированных системах;

- разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

ВЛАДЕТЬ:

- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;

- методами управления информационной безопасностью автоматизированных систем;

- методами оценки информационных рисков.

**4. Содержание и структура дисциплины**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Методология управления информационной безопасностью | Проблема информационной безопасности и защиты информации.Верификационный и риск-ориентированный подходы к обеспечению и управлению информационной безопасностью.Организационно-правовые аспекты и процессная модель управления информационной безопасностью.Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте. |
| 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 | Технические аспекты управления информационной безопасностью | Управление и обеспечение информационной безопасности компьютерных сетей организации - функциональные области, базовые задачи, архитектура, основные характеристики. Управление на основе контроля состояния. Управление аппаратными средствами компьютеров на основе технологии WFM. Управление на основе правил системной политики: стандарты LDAP, DEN, COPS. |

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

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

лекции – 34 час.

лабораторные работы – 34 час.

самостоятельная работа – 67 час.

Форма контроля знаний – экзамен.