АННОТАЦИЯ

Дисциплины

«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

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 «Теоретические основы компьютерной безопасности» (Б1.В.ОД.9) относится вариативной 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 компьютерной системы как объектно-субъектной модели;

- изучение основных теоретических положений, используемых при разработке механизма идентификации и аутентификации;

- изучение основных теоретических положений, используемых при разработке механизма авторизации;

- изучение алгоритмов реализации аудита и регистрации событий, используемых при разработке механизма идентификации и аутентификации и анализа матрицы доступа;

- изучение средств антивирусной защиты.

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

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

- способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

- способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3).

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

научно-исследовательская деятельность:

- способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

проектно-конструкторская деятельность:

- способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-11).

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

- угрозы компьютерной безопасности;

- уязвимости и изъяны системы защиты;

- классификацию атак на защищённые компьютерные системы;

- требования, предъявляемые к защищённым компьютерным системам и архитектуру защищенных компьютерных систем;

- теоретические основы построения механизмов защиты компьютерных систем;

- формальные и неформальные модели разграничения доступа субъектов к объектам компьютерной системы;

- модели разграничения доступа в распределённых компьютерных системах;

- классификацию вирусов и средства антивирусной защиты;

- критерии безопасности.

УМЕТЬ:

- разрабатывать модели механизма идентификации и аутентификации;

- разрабатывать модели политик разграничения доступа субъектов к объектам компьютерной системы;

- разрабатывать алгоритмы, реализующие политики аудита и регистрации событий.

ВЛАДЕТЬ:

- теоретическими знаниями, позволяющими применять математический аппарат, языки и инструментальные средства программирования, для решения профессиональных задач, связанных с разработкой механизмов защиты компьютерных систем.

**4. Содержание и структура дисциплины**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем | Сущность, субъект, доступ, информационный поток.  Классическая классификация угроз безопасности информации.  Виды информационных потоков. Виды политик управления доступом и информационными потоками. Утечка права доступа и нарушение безопасности КС  Основные виды формальных моделей безопасности. Проблема адекватности реализации модели безопасности в реальной компьютерной системе |
| 2 | Модели компьютерных систем с дискреционным управлением доступом | Модель матрицы доступов Харрисона–Руззо–Ульмана. Описание модели. Анализ безопасности систем ХРУ  Модель типизированной матрицы доступов |
| 3 | Модели компьютерных систем с мандатным управлением доступом | Модель Белла–ЛаПадулы. Классическая модель Белла–ЛаПадулы. Пример некорректного определения свойств безопасности. Политика low-watermark в модели Белла–ЛаПадулы. Примеры реализации запрещенных информационных потоков. Безопасность переходов |
| 4 | Модели компьютерных систем с ролевым управлением доступом | Понятие ролевого управления доступом. Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом. Основные положения. Администрирование множеств авторизованных ролей пользователей. Администрирование множеств прав доступа. Администрирование иерархии ролей. Модель мандатного ролевого управления доступом. Защита от угрозы конфиденциальности информации. Защита от угроз конфиденциальности и целостности информации |
| 5 | Общие сведения о компьютерных вирусах | Что такое компьютерный вирус. Какие бывают вирусы. Кто и зачем пишет вирусы. Общие сведения о методах борьбы с компьютерными вирусами.  Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Макровирусы. Сетевые и почтовые вирусы и черви. Распространение вирусов. |
| 6 | Борьба с компьютерными вирусами | Обнаружение вирусов. Анализ косвенных признаков. Контрольные суммы. Использование сигнатур для детектирования полиморфных вирусов. Метаморфные вирусы и их детектирование. Эвристические методы детектирования вирусов. Концепция современного антивирусного средства.  Борьба с вирусами без использования антивирусов. |

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

Объем дисциплины – 4 зачетных единицы (144 час.), в том числе:

лекции – 34 час.

лабораторные работы – 34 час.

самостоятельная работа – 40 час.

Форма контроля знаний – экзамен, курсовой проект.