АННОТАЦИЯ

Дисциплины

«ОСНОВЫ ИНФОРМАЦИОННОЙ 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 «Основы информационной безопасности» (Б1.Б.11) 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:

− формирование понимания социальной значимости своей будущей профессии;

− формирование способности к активной состязательной деятельности в условиях информационного противоборства;

− формирование способности к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.

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

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

− способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

Изучение дисциплины направлено на формирование следующих профессиональных компетенций (ПК), соответствующих видам

профессиональной деятельности, на которые ориентирована программа специалитета:

- научно-исследовательская деятельность:

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4).

- проектно-конструкторская деятельность:

способностью участвовать в разработке защищенных

автоматизированных систем в сфере профессиональной деятельности (ПК-9);

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

- контрольно-аналитическая деятельность:

способностью участвовать в проведении экспериментально¬-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16).

- организационно-управленческая деятельность:

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

- эксплуатационная деятельность:

- способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

- способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

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

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

 основы обеспечения информационной безопасности информацион-ных систем;

 нормативные документы РФ в области защиты информации;

 правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

 основные угрозы безопасности информации и модели нарушителя в информационных системах;

 основные меры по защите информации в информационных систе-мах (организационные, правовые, программно-аппаратные, криптографи-ческие, технические);

 основные методы управления информационной безопасностью.

УМЕТЬ:

 классифицировать защищаемую информацию по видам информа-ции ограниченного доступа;

 классифицировать и оценивать информационные угрозы для объек-та информатизации;

 пользоваться нормативными документами по защите информации;

 анализировать и оценивать информационные угрозы объекта ин-форматизации;

 определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.

ВЛАДЕТЬ:

 профессиональной терминологией в области информационной без-опасности;

 навыками безопасного использования технических средств в про-фессиональной деятельности;

 навыками работы с нормативными правовыми актами.

**4. Содержание и структура дисциплины**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Введение в информационную безопасность | Информация. Понятие, свойства, количество информации. Защищаемая информация.  Основные понятия, основные принципы обеспечения информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности РФ. Организационная структура обеспечения информационной безопасности РФ.  Угрозы информационной безопасности, их классификация. Основные механизмы защиты информации. |
| 2 | Введение в правила разграничения доступа | Основные понятия.  Идентификация и аутентификация: способы, формы, системность.  Основные положения системы правил разграничения доступа. |
| 3 | Введение в криптографические методы защиты информации. | Основные понятия.  Стенографические методы защиты.  Методы подстановки. Методы перестановки.  Гаммирование. Симметричные и ассиметричные криптосистемы. Хеширование. |
|  | Принципы построения системы защиты информации | Нормативно-правовая составляющая системы защиты информации.  Организационная составляющая системы защиты информации.  Техническая составляющая системы защиты информации.  Подходы к построению системы защиты информации от угроз конфиденциальности, целостности, доступности. |

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

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

Лекции – 34 час.

Практические занятия – 34 час.

Самостоятельная работа – 31 час.

Форма контроля знаний – зачет.