АННОТАЦИЯ

Дисциплины

«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация выпускника – специалист по защите информации

Специализация – «Информационная безопасность автоматизированных систем на транспорте»

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

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» (Б1.В.ОД.11) относится к вариативной части профессионального цикла и является обязательной для изучения.

**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 и эксплуатационная..

Для достижения поставленной цели решаются следующие задачи:

* 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;
* обучение студентов практическому применению технологий создания систем управления информационной безопасностью;
* изучение управления рисками и инцидентами;
* изучение работы с системами обнаружения и предотвращения вторжений.

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

Изучение дисциплины направлено на формирование следующих компетенций: ОПК-6,   
ПК-6, ПК-7, ПК-8, ПК-9, ПК-23.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

* методики управления рисками и инцидентами;
* архитектуру систем управления информационной безопасности;
* средства администрирования информационной безопасности;
* системы обнаружения вторжения;
* системы предотвращения вторжений;
* системы управления доступом.

УМЕТЬ:

* определять состав информационных активов, подлежащих защите;
* составлять требования к разрабатываемой автоматизированной системе;
* разрабатывать политику информационной безопасности;
* определять оптимальный вариант решения задачи при наличии альтернатив.

ВЛАДЕТЬ:

* навыками разворачивания и настройки систем управления доступом;
* навыками разворачивания и настройки систем обнаружения вторжений;
* навыками разворачивания и настройки систем предотвращения вторжений.

**4. Содержание и структура дисциплины**

1. Система управления информационной безопасностью.
2. Методологическое и техническое обеспечение информационной безопасности.
3. Информационные активы автоматизированной системы.
4. Управление рисками и инцидентами. Анализ рисков в области защиты информации.
5. Создание и реализация политик информационной безопасности.
6. Технологии обнаружения вторжений.
7. Системы управления доступом.
8. Управление и администрирование информационной безопасности.

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

Объем дисциплины – 4 зачетных единиц (144 часа), в том числе:

лекции – 32 часов;

лабораторные работы – 16 часов;

самостоятельная работа – 60 часов;

контроль – 36 часов.

Форма контроля знаний – экзамен, курсовой проект (9 семестр).