

Б1.В.03 Управление информационной безопасностью на объектах транспортной инфраструктуры

Объем дисциплины (модуля) 4 ЗЕТ (144 час)

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.
Приобретение обучаемыми необходимого объема знаний и практических навыков в области управления информационной безопасностью в системах критической информационной инфраструктуры.
Формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ

ПК-3: Способен устанавливать и настраивать средства защиты информации в автоматизированных системах

ПК-3.3: Знает основные меры по защите информации в автоматизированных системах

ПК-3.2: Владеет навыками установки и настройки средств защиты информации в автоматизированных системах

ПК-3.1: Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

ПК-4: Способен проводить работы по техническому обслуживанию защищенных технических средств защиты информации

ПК-4.3: Выполняет техническое обслуживание технических средств обработки информации в защищенном исполнении

ПК-4.2: Знает порядок аттестации объектов информатизации на соответствие требованиям безопасности информации

ПК-4.1: Знает проектную документацию на систему защиты объекта информатизации

ПК-5: Способен проводить мониторинг защищенности информации в автоматизированных системах

ПК-5.3: Анализирует недостатки в функционировании системы защиты информации автоматизированной системы

ПК-5.4: Применяет технические средства контроля эффективности средств защиты информации

ПК-5.1: Проводит мониторинг угроз безопасности информации в автоматизированных системах

ПК-5.2: Принимает меры защиты информации при выявлении новых угроз безопасности информации

ПК-6: Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах

ПК-6.2: Применяет руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

В результате освоения дисциплины обучающийся должен

Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
принципы организации информационных систем в соответствии с требованиями по защите информации в системах критической информационной инфраструктуры;
основные нормативные правовые акты в области информационной безопасности и защиты информации в системах критической информационной инфраструктуры.

Уметь: анализировать и оценивать угрозы информационной безопасности объекта;
применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
пользоваться нормативными документами по защите информации;
формулировать и настраивать политику безопасности распространенных операционных систем, а также вычислительных сетей, построенных на их основе.

Владеть: навыками работы с нормативными правовыми актами;
навыками работы с нормативными документами;
методами и средствами выявления угроз безопасности автоматизированным системам;
методами формирования требований по защите информации;
методами анализа и формализации информационных процессов объекта и связей между ними;
методами организации и управления деятельностью служб защиты информации на предприятии;
методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Теоретические аспекты организации систем управления информационной безопасностью

