АННОТАЦИЯ
производственной практики
«ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»
Квалификация (степень) выпускника – специалист по защите информации
Специализация – «Информационная безопасность автоматизированных систем на транспорте»

1. Место практики в структуре основной профессиональной образовательной программы

Практика «Эксплуатационная» (Б2.П.2) относится к Блоку 2 «Практики, в том числе научно-исследовательская работа (НИР)» и является обязательной.

2. Цель и задачи практики

Целью прохождения практики «Эксплуатационная» является получение обучающимися профессиональных навыков организаторской деятельности в условиях трудового коллектива и приобретение опыта управления производством в сфере обеспечения информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере

Для достижения поставленной цели решаются следующие задачи:

Освоение методов

- анализа безопасности информационных технологий, реализуемых в автоматизированных системах;
- моделирования и исследования защищенных автоматизированных систем, анализа их уязвимостей и эффективности средств и способов защиты;
- контроля работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- инструментального мониторинга защищенности автоматизированных систем;
- контроля реализации политики информационной безопасности;
- мониторинга информационной безопасности автоматизированных систем.

Изучение новых технологий

- для организации работы коллектива, принятия управленческих решений в условиях спектра мнений, определения порядка выполнения работ;
- для их реализации в сфере профессиональной деятельности с использованием защищенных автоматизированных систем.

Приобретение знаний для

- разработки эффективных решений по обеспечению информационной безопасности автоматизированных систем;
- разработки политик информационной безопасности автоматизированных систем;
- разработки защищенных автоматизированных систем по профилю профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;
- выполнения проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- разработки системы управления информационной безопасностью автоматизированных систем;
- разработки предложений по совершенствованию и повышению эффективности принятых мер по обеспечению информационной безопасности автоматизированных систем.

Овладение навыками

- сбора, обработки, анализа и систематизации научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем;

- подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;

- сбора и анализа исходных данных для проектирования систем защиты информации;

- экспериментально-исследовательской работы при сертификации средств защиты автоматизированных систем;

- экспериментально-исследовательской работы при аттестации автоматизированных систем;

- организации работ по выполнению требований защиты информации ограниченного доступа;

организации работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;

администрирования подсистем информационной безопасности автоматизированных систем;

- управления информационной безопасностью автоматизированных систем;

- обеспечения восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.

3. Перечень планируемых результатов прохождения практики

Прохождение практики направлено на формирование следующих компетенций: ОК-5, ОК-8, ОПК-3, ОПК-4, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28.

В результате прохождения практики обучающийся должен:

ЗНАТЬ:

- правила техники безопасности и порядок организации труда на рабочих местах;

- требования режима безопасности и делопроизводства;

- особенности соблюдения специальных правил при работе с оперативно-технической и служебной документацией;

- основные обязанности должностных лиц подразделения по защите информации;

- основные характеристики и возможности используемых в подразделении технических, программных, аппаратных и криптографических средств защиты информации, методы и тактические приемы их применения для решения служебных задач по обеспечению информационной безопасности объекта;

- общие принципы существующего порядка использования технических и программных средств защиты информации;

УМЕТЬ:

- проверять, настраивать и использовать технические и программные средств подразделения по защите информации;

- выполнять основные функциональные обязанности в соответствии с должностью;

- работать с технической и эксплуатационной документацией;

- использовать современные средства разработки программного обеспечения на языках высокого уровня и языках СУБД, библиотеки объектов и классов для решения задач создания и сопровождения автоматизированных систем;

- применять стандартные криптографические решения для защиты информации и квалифицированно оценивать их качество;

- реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

ВЛАДЕТЬ:

- методами системного подхода к обеспечению информационной безопасности в различных сферах деятельности подразделения.

4. Содержание и структура практики

Первая неделя: знакомство со структурой предприятия и изучение локальных нормативных актов, определение рабочего места и руководителя практики от предприятия, подбор литературы по теме задания, анализ и выбор методов решения поставленных задач

Вторая неделя: выполнение индивидуального задания, выданного кафедрой, написание отчета по практике.

5. Объем практики и виды учебной работы

Объем практики– 3 зачетные единицы (108 час.), в том числе:
деятельность на производстве – 60 час.
самостоятельная работа – 48 час.
Форма контроля знаний – экзамен