АННОТАЦИЯ
производственной практики
«ПРЕДДИПЛОМНАЯ 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 «Преддипломная» (Б2.П.3) относится к Блоку 2 «Практики, в том числе научно-исследовательская работа (НИР)» и является обязательной.

2. Цель и задачи практики

Целью преддипломной практики и реального дипломного проектирования по заявкам предприятий является обобщение, систематизация и совершенствование знаний и умений обучающихся по будущей профессии, сбор и подготовка необходимых материалов для выполнения выпускной квалификационной работы.

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-6, ОК-7, ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14, ПК-15, ПК-16, ПК-17, ПК-18, ПК-19, ПК-20, ПК-21, ПК-22, ПК-23, ПК-24, ПК-25, ПК-26, ПК-27, ПК-28, ПСК-10.1, ПСК-10.2, ПСК-10.3, ПСК-10.4, ПСК-10.5.

В результате прохождения практики обучающийся должен:

ЗНАТЬ:

- систему компьютерной и информационной безопасности подразделения и систему противодействия техническим разведкам;

- организацию научной, изобретательской и рационализаторской работы, проводимой подразделением в интересах совершенствования выполнения служебных задач;

- процесс проектирования, производства и эксплуатации средств компьютерной и информационной безопасности;

- организацию служебной и производственной деятельности подразделения;

- структурные и функциональные схемы, используемые в подразделениях компьютерной и информационной безопасности;

- порядок и методы проведения планово-профилактических и ремонтно-восстановительных работ;

- характеристики и возможности диагностического оборудования и измерительных приборов, входящих в состав рабочих мест;

- характеристики технических средств, используемых при разработке, изготовлении и эксплуатации средств компьютерной, информационной безопасности и противодействия техническим разведкам;

- современные методы и средства разработки и оценки модели и политики безопасности.

УМЕТЬ:

- 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.

- выполнять функциональные обязанности в соответствии с должностью специалиста (инженера) по защите информации;

- проводить планово-профилактические и ремонтные работы;

- вести учетно-отчетную документацию;

- проводить занятия с техническим персоналом подразделения;

- выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации;

- решать задачи защиты программ и данных программно-аппаратными средствами и оценивать качество предлагаемых решений.

ВЛАДЕТЬ:

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

- методами планирования и проведения специальных технических мероприятий, направленных на повышение эффективности функционирования системы компьютерной и информационной безопасности подразделения;

- используемыми в подразделении методами определения и измерения параметров опасных сигналов для технических каналов утечки информации;

- методами анализа используемых в подразделении технологий обработки данных в распределенных системах с целью оптимизации их производительности и повышения надежности функционирования.

4. Содержание и структура практики

Первая неделя: Получение темы и состава ВКР и исходных данных. Изучение учебной и нормативной литературы по теме ВКР

Вторая и третья неделя: Изучение и обобщение опыта работы и материалов предприятия по теме ВКР

Четвертая – одиннадцатая недели: Проработка принципиальных технических решений по разделам ВКР.

Двенадцатая неделя: Написание отчета по практике

5. Объем практики и виды учебной работы

Объем практики– 18 зачетных единиц (648 час.), в том числе:
самостоятельная работа – 648 час.
Форма контроля знаний – зачет