АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем»

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Цели прохождения производственной практики:

- закрепление теоретических и практических знаний, полученных в процессе обучения по специальности «Информационная безопасность автоматизированных систем».
- подготовка студента к решению задач, относящихся к обеспечению информационной безопасности.

Задачи прохождения практики:

- овладение профессиональными навыками работы и решение практических задач;
- выбор направления практической работы;
- сбор необходимой для выполнения данной работы информации по месту прохождения практики, а также при изучении литературных и иных источников;
- приобретение опыта работы в коллективе.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

Общая трудоемкость составляет 9 зачетных единиц (324 часа). Продолжительность практики - 6 недель в 10 семестре.

Практика относится к «Блоку 2» части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы специалитета.

Для успешного прохождения практики необходимы компетенции, сформированные в ходе изучения дисциплин «Основы информационной безопасности», «Защита информации от утечки по техническим каналам», «Безопасность открытых информационных систем», «Сети и системы передачи информации», «Организационное и правовое обеспечение информационной безопасности».

Эксплуатационная практика студентов, обучающихся по учебной программе специальности «Информационная безопасность автоматизированных систем», является составной частью основной образовательной программы высшего образования. Практика студента является средством связи теоретического обучения с практической деятельностью, обеспечивающим прикладную направленность и специализацию обучения и направлена на подготовку студентов с учетом их будущей профессиональной деятельности.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ СТУДЕНТОВ, СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В совокупности с дисциплинами базовой и вариативной части ФГОС ВО производственная практика направлена на формирование следующих компетенций по специальности «Информационная безопасность автоматизированных систем»:

Индекс и наименование реализуемой компетенции	**Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций**
1	2
УК-3 - Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	**Знать:** методики формирования команд методы эффективного руководства коллективами основные теории лидерства и стили руководства **Уметь:** разрабатывать план групповых и организационных коммуникаций при подготовке и выполнении проекта сформулировать задачи членам команды для достижения поставленной цели разрабатывать командную стратегию применять эффективные стили руководства командой для достижения поставленной цели **Владеть:** умением анализировать, проектировать и организовывать межличностные, групповые и организационные коммуникации в команде для достижения поставленной цели методами организации и управления коллективом
УК-4 - Способен применять современные коммуникативные технологии, в том числе на иностранном (ых) языке (ах), для академического и профессионального взаимодействия	**Знать:** правила и закономерности личной и деловой устной и письменной коммуникации современные коммуникативные технологии на русском и иностранном языках существующие профессиональные сообщества для профессионального взаимодействия **Уметь:** применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия **Владеть:** методикой межличностного делового общения на русском и иностранном языках с применением языковых форм, средств и современных коммуникативных технологий
УК-8 - Способен создавать и поддерживать в повседневной жизни и в профессиональной де-	**Знать:** классификацию и источники чрезвычайных ситуаций природного и техногенного происхождения причины, признаки и последствия опасностей, способы защиты от чрезвычайных ситуаций

ятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	принципы организации безопасности труда на предприятии, технические средства защиты людей в условиях чрезвычайной ситуации **Уметь:** поддерживать безопасные условия жизнедеятельности выявлять признаки, причины и условия возникновения чрезвычайных ситуаций оценивать вероятность возникновения потенциальной опасности и принимать меры по ее предупреждению **Владеть:** методами прогнозирования возникновения опасных или чрезвычайных ситуаций навыками по применению основных методов защиты в условиях чрезвычайных ситуаций
ПК-1 - Способен организовать работы по выполнению в информационной системе требований защиты информации ограниченного доступа	**Знать:** Источники и классификацию угроз информационной безопасности Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Нормативные правовые акты в области защиты информации **Уметь:** Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты Организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях **Владеть:** Навыками организации применения защищенных протоколов, межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях Навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем
ПК-2 - Способен осуществлять тестирование систем защиты информации автоматизированных систем	**Знает:** Принципы построения и функционирования систем и сетей передачи информации Эталонную модель взаимодействия открытых систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах **Умеет:** Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать безотказное функционирование технических средств защиты информации **Владеет:**

	Навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ПК-3 - Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**Знать:** Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем Принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** Применять действующую нормативную базу в области обеспечения защиты информации Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе **Владеть:** Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-4 - Способен участвовать в разработке программных и программно-аппаратных средств для систем защиты информации автоматизированных систем	**Знает:** Профессиональную и криптографическую терминологию в области безопасности информации Основные информационные технологии, используемые в автоматизированных системах Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации **Умеет:** Проводить комплексное тестирование аппаратных и программных средств Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах

	Владеет: Навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных систем Навыками разработки программного обеспечения, технических средств, баз данных и вычислительных сетей с учетом требований по обеспечению защиты информации
ПК-5 - Способен участвовать в научных и исследовательских работах в сфере разработки средств защиты информации от НСД	**Знать:** Национальные, межгосударственные и международные стандарты, устанавливающие требования к организации и проведению научно-исследовательских, опытно-конструкторских работ, опытной эксплуатации средств и систем защиты информации от НСД Руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты информации от НСД Основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты **Уметь:** Организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности, выработку предложений по вопросам комплексного обеспечения информационной безопасности, разработку моделей угроз НСД Проводить выбор, исследовать эффективность и разрабатывать технико-экономическое обоснование проектных решений средств и систем защиты информации от НСД с целью обеспечения требуемого уровня защищенности **Владеть:** Навыками планирования этапов выполнения НИОКР по созданию средств и систем защиты информации от НСД Навыками организации опытной эксплуатации средств и систем защиты информации от НСД
ПК-6 - Способен проводить контроль защищенности информации от НСД	**Знать:** Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее Методы и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий **Уметь:** Проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий

	Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации **Владеть:** Навыками проведения контроля защищенности информации от несанкционированного доступа и специальных воздействий

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 9 зачетных единиц (324 часа).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На эксплуатационной практике изучаются современные информационные технологии обеспечения информационной безопасности, используемые в технологических производственных процессах предприятия.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Руководитель практики проводит контроль над работами студентов, целью которого является:

- обеспечение высокого качества прохождение студентами практики, ее строго соответствия учебным планам и программам;
- согласование программы и графиков прохождения студентами практики с руководителями практики от предприятий, подготовка и выдача студентам индивидуальных заданий на время практики;
- осуществление регулярного контроля за прохождением студентами практики, за соблюдением студентами правил внутреннего трудового распорядка предприятия;
- проведение консультаций по всем возникающим вопросам;
- проверка отчетов и дневников студентов по завершении практики, участие в работе по приемке защиты отчетов о практике.

По окончании практики студент составляет письменный отчет, оформленный в соответствии с установленными требованиями, сдает его руководителям практики от университета и организации – базе практики для предварительной дифференцированной оценки.

Отчет о практике должен содержать сведения о конкретно выполненной студентом работы в период практики.

По результатам аттестации студенту выставляется итоговая дифференцированная оценка за преддипломную практику («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

Итоги практики подводятся на заседании кафедры. Студент, не выполнивший программу практики, получивший отрицательный отзыв о работе или неудовлетворительную оценку при защите отчета, направляется повторно на практику в период студенческих каникул, либо в свободное от учебы время, либо ставится вопрос об отчислении студента из университета.