АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ПРОИЗВОДСТВЕННАЯ 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 различных проблемам обеспечения информационной безопасности, и к решению отдельных фундаментальных проблем связанных с информационной безопасностью автоматизированных систем.

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 3 зачетных единицы (108 часов). Продолжительность практики - 2 недели в 6 семестре.

Практика относится к «Блоку 2» основной профессиональной образовательной программы специалитета - «Практики, в том числе научно-исследовательская работа (НИР)» и базируется на дисциплинах как базовой, так и вариативной части учебного плана основной профессиональной образовательной программы.

Для успешного прохождения практики необходимы компетенции, сформированные в ходе изучения дисциплин «Основы информационной безопасности», , «Техническая защита информации», «Информационная безопасность открытых систем», «Сети и системы передачи информации».

Производственная 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.

Производственная 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
ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	**Знать:** основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира с древности до наших дней, выдающихся деятелей отечественной истории; различные оценки и периодизации Отечественной истории; **Уметь:** соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; извлекать уроки из исторических событий и на их основе принимать осознанные решения; осуществлять эффективный поиск информации и критику источников; получать, обрабатывать и сохранять источники информации; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории; анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав **Владеть:** представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приемами ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности

1	2
ОК-7 - способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	**Уметь:** осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий) **Владеть:** навыками работы с технической документацией на ЭВМ и вычислительные системы
ОПК-1 – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	**Знать:** основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; основы квантовой физики и физики твёрдого тела; физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации; основные методы управления информационной безопасностью; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах **Уметь:** определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач строить математические модели физических явлений и процессов; решать типовые прикладные физические задачи; анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; применять математические методы исследования моделей шифров основы физической защиты объектов информатизации выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем **Владеть:** навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике, методами линейной алгебры навыками построения дискретных моделей при решении

	профессиональных задач методами теоретического исследования физических явлений и процессов; навыками проведения физического эксперимента и обработки его результатов
ОПК-3 – способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	**Знать:** принципы построения и функционирования, примеры реализаций современных операционных систем; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; основные информационные технологии, используемые в автоматизированных системах; показатели качества программного обеспечения; язык программирования высокого уровня (объектно-ориентированное программирование); возможности, классификацию и область применения макрообработки; способы обработки исключительных ситуаций **Уметь:** создавать объекты базы данных; выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; работать с интегрированной средой разработки программного обеспечения; использовать шаблоны классов и средства макрообработки; использовать динамически подключаемые библиотеки **Владеть:** навыками использования ЭВМ в анализе простейших шифров; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ; навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками поддержания работоспособности, обнаружения

	и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыками проектирования программного обеспечения с использованием средств автоматизации; навыками разработки программной документации
ПК-1 - способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	**Знать:** нормативные и методические документы для разработки технических заданий на создание подсистем информационной безопасности автоматизированных систем **Уметь:** осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности **Владеть:** навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках
ПК-2 - способностью создавать и исследовать модели автоматизированных систем	**Знать:** модели шифров и математические методы их исследования; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации **Уметь:** разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений **Владеть:** навыками математического моделирования в криптографии; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;

	навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	**Знать:** требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; **Уметь:** разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений **Владеть:** навыками математического моделирования в криптографии; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; навыками организации и обеспечения режима секретности
ПК-4 - способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	**Знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах **Уметь:**

	разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; анализировать и оценивать угрозы информационной безопасности объекта **Владеть:** методологией разработки основных угроз безопасности информации и моделей нарушителя в автоматизированных системах
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	**Знать:** требования к шифрам и основные характеристики шифров **Уметь:** анализировать и оценивать угрозы информационной безопасности объекта **Владеть:** методологией анализа рисков информационной безопасности автоматизированной системы
ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**Знать:** Основы эффективного применения автоматизированных систем в сфере профессиональной деятельности **Уметь:** Проводить анализ защищенности автоматизированных систем **Владеть:** Методами формирования требований по защите информации
ПК-7 - способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	**Знать:** принципы построения и функционирования, примеры реализаций современных операционных систем **Уметь:** разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов **Владеть:** навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности
ПК-8 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**Знать:** средства обеспечения безопасности данных; основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации; показатели качества программного обеспечения; методологии и методы проектирования программного

	обеспечения; методы тестирования и отладки ПО; принципы организации документирования разработки, процесса сопровождения программного обеспечения; основные структуры данных и способы их реализации на языке программирования; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности **Уметь:** формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; планировать разработку сложного программного обеспечения; проводить комплексное тестирование и отладку программных систем; проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; работать с интегрированной средой разработки программного обеспечения автоматизированных системах **Владеть:** навыками участия в экспертизе состояния защищенности информации на объекте защиты; навыками проектирования программного обеспечения с использованием средств автоматизации; навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов
ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать:** принципы построения и функционирования, примеры реализаций современных систем управления базами данных; архитектуру систем баз данных; основные модели данных; физическую организацию баз данных; последовательность и содержание этапов проектирования баз данных **Уметь:** разрабатывать и администрировать базы данных; выделять сущности и связи предметной области;

	отображать предметную область на конкретную модель данных; нормализовывать отношения при проектировании реляционной базы данных применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации **Владеть:** навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации
ПК-10 - способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	**Знать:** основную терминологию, определения, понятия и законы электроники и схемотехники; **Уметь:** рассчитывать и измерять параметры и характеристики электронных и электротехнических устройств. **Владеть:** навыками сборки, монтажа и тестирования на лабораторных стендах основных узлов электроники
ПК-11 - способностью разрабатывать политику информационной безопасности автоматизированной системы	**Знать:** основные задачи и понятия криптографии; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; принципы формирования политики информационной безопасности в автоматизированных системах **Уметь:** определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем **Владеть:** навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности

ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	**Уметь:** применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; оценивать информационные риски в автоматизированных системах **Владеть:** навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации; навыками участия в экспертизе состояния защищенности информации на объекте защиты
ПК-13 - способностью участвовать в проектировании средств защиты информации автоматизированной системы	**Знать:** требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах **Уметь:** применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации; эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем **Владеть:** криптографической терминологией; методами формирования требований по защите информации;

	методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; методами и средствами технической защиты информации
ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**Знать:** требования к шифрам и основные характеристики шифров; основные информационные технологии, используемые в автоматизированных системах; **Уметь:** контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем **Владеть:** навыками участия в экспертизе состояния защищенности информации на объекте защиты; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; методами расчета и инструментального контроля показателей технической защиты информации; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков
ПК-15 - способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	**Знать:** Методы сертификации средств защиты информации автоматизированных систем
ПК-16 - способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации	**Знать:** возможности технических средств перехвата информации
ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизи-	**Знать:** технические каналы утечки информации **Уметь:** проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять

рованной системе и выявлять каналы утечки информации	каналы утечки информации **Владеть:** методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-18 - способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	**Знать:** требования и основные характеристики информационной безопасности; **Уметь:** эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах **Владеть:** терминологией теории информационной безопасности
ПК-19 - способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	**Знать:** требования и основные характеристики информационной безопасности; **Уметь:** эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах **Владеть:** терминологией теории информационной безопасности
ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	**Знать:** требования и основные характеристики информационной безопасности; **Уметь:** эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах **Владеть:** терминологией теории информационной безопасности
ПК-21 - способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**Знать:** основные документы, регламентирующие работу по обеспечению информационной безопасности автоматизированных систем **Уметь:** разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем **Владеть:** навыками, эксплуатации и администрирования (в части,

	касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности
ПК-22 - способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**Знать:** требования и основные характеристики информационной безопасности; **Уметь:** эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах **Владеть:** терминологией теории информационной безопасности
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	**Знать:** требования и основные характеристики информационной безопасности; **Уметь:** эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах **Владеть:** терминологией теории информационной безопасности
ПК-24 - способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**Знать:** требования и основные характеристики информационной безопасности; **Уметь:** эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах **Владеть:** терминологией теории информационной безопасности
ПК-25 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	**Знать:** Основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации **Уметь:** Проводить анализ защищенности автоматизирова-нных систем **Владеть:** Методами формирования требований по защите информации
ПК-26 - способностью	**Знать:**

администрировать подсистему информационной безопасности автоматизированной системы	типовые шифры с открытыми ключами; технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования; источники и классификацию угроз информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; современные технологии и методы программирования **Уметь:** планировать политику безопасности операционных систем; применять средства обеспечения безопасности данных; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; администрировать подсистемы информационной безопасности автоматизированных систем **Владеть:** навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ навыками работы с технической документацией на ЭВМ и вычислительные системы; профессиональной терминологией в области информационной безопасности; навыками чтения принципиальных схем, построения вре-

	менных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы навыками разработки программной документации
ПК-27 - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**Знать:** требования и основные характеристики информационной безопасности; **Уметь:** эффективно использовать методы и средства управления информационной безопасностью в автоматизированных системах **Владеть:** терминологией теории информационной безопасности
ПСК-4.1 – способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем	**Знать:** основные методы и средства реализации удаленных сетевых атак на открытые информационные системы; политики безопасности и меры защиты в открытых информационных системах **Уметь:** реализовывать системы защиты информации в открытых информационных системах в соответствии со стандартами по оценке защищенных систем; практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений; осуществлять мониторинг и аудит сетевой безопасности; осуществлять администрирование открытых информационных систем; **Владеть:** терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
ПСК-4.2 – способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных	**Знать:** политики безопасности и меры защиты в открытых информационных системах **Уметь:** проектировать защищенные открытые информационные системы;

систем	определять и устранять основные угрозы информационной безопасности для открытых информационных систем; строить модель нарушителя; **Владеть:** терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах
ПСК - 4.3 – способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы	**Знать:** принципы построения современных виртуальных локальных и частных сетей и направления их развития; виды виртуальных сетей и их преимущества при конкретном применении; политику безопасности для виртуальных сетей **Уметь:** осуществлять управление информационной безопасностью в открытых информационных системах; применять стандартные решения для защиты информации в виртуальных сетях и квалифицированно оценивать их качество **Владеть:** навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
ПСК-4.4 – способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	**Знать:** основные стандарты построения виртуальных сетей; принципы работы сетевых протоколов и технологий передачи данных в виртуальных сетях; подходы к интеграции виртуальных сетей с открытыми информационными системами **Уметь:** обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам; применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество, используя современные методы и средства; разрабатывать и оценивать модели и политику безопасности для открытых информационных систем **Владеть:** навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей

ПСК-4.5 – способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	**Знать:** базовые вопросы построения открытых информационных систем; основные криптографические протоколы и стандарты; основные стандарты построения и взаимодействия открытых систем; политики безопасности и меры защиты в открытых информационных системах **Уметь:** проектировать защищенные открытые информационные системы; определять и устранять основные угрозы информационной безопасности для открытых информационных систем; строить модель нарушителя информационной безопасности для открытых информационных систем; выявлять и устранять уязвимости в основных компонентах открытых информационных систем **Владеть:** терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетных единицы (108 часов).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На преддипломной 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.