

## АННОТАЦИЯ

### Программы преддипломной практики

Направление подготовки: **10.04.01 – Информационная безопасность**

Уровень высшего образования: **магистратура**

Форма обучения: **очная**

**Вид практики** – производственная

#### Цели практики

Целью практики является закрепление знаний и умений, полученных в процессе теоретического обучения, овладение методикой обеспечения информационной безопасности на предприятии (организации), проектирования, внедрения и эксплуатации отдельных задач и подсистем комплексной системы защиты информации предприятия (организации).

Преддипломная практика имеет целью получение практических навыков работы по специальности в профильных подразделениях предприятий (организаций, учреждений). Тема преддипломной практики должна быть логически связана с предполагаемой темой выпускной квалификационной работы. В процессе преддипломной практики студент получает практические, экспериментальные, модельные результаты, используемые при выполнении квалификационной работы. Преддипломную практику проходят студенты 2 курса обучения в соответствии с учебными планами направления 10.04.01 «Информационная безопасность» ВлГУ.

#### Результаты практики

В результате прохождения преддипломной практики обучающийся овладевает компонентами следующих *общекультурных, общепрофессиональных и профессиональных компетенций*:

Коды компетенции	Результаты освоения ООП <i>Содержание компетенций</i>	Перечень планируемых результатов при прохождении практики
ОК-2	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	<b>знать:</b> содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук; основные этапы развития философской мысли, основную проблематику и структуру философского знания. <b>уметь:</b> использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач; анализировать мировоззренческие, социально и личностно значимые философские проблемы; анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности. <b>владеть:</b> основными методами научного познания; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; методами теоретического исследования физических явлений и процессов; навыками проведения физического эксперимента и обработки его результатов; навыками решения типовых математических задач численными методами с использованием средств вычислительной техники.
ОПК-2	способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности	<b>знать:</b> экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности); основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; методы концептуального проектирования технологий обеспечения информационной безопасности. <b>уметь:</b> применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; применять на практике методы физики при исследовании технических каналов утечки информации. <b>владеть:</b> приемами экономического анализа и планирования,

		<p>навыками реализации и контроля результатов управленческого решения по экономическим критериям; методами проведения физического эксперимента при выявлении технических каналов утечки информации.</p>
ПК-1	<p>способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты</p>	<p><b>знать:</b> основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>уметь:</b> самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>владеть:</b> навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов.</p>
ПК-2	<p>способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности</p>	<p><b>Знать:</b> основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; - основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах; - методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>Уметь:</b> - строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных систем;- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; - разрабатывать частные политики информационной безопасности информационных систем; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; - оценивать информационные риски в информационных системах; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; - составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем; применять системы компьютерной математики для решения типовых задач; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>Владеть:</b> методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в</p>

		<p>экспертизе состояния защищенности информации на объекте защиты; методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; - методами организации и управления деятельностью служб защиты информации на предприятии; навыками организации и обеспечения режима секретности навыками управления информационной безопасностью простых объектов.</p>
ПК-3	<p>способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов</p>	<p><b>Знать:</b> цели, задачи и принципы построения системы защиты информации; - требования, предъявляемые к системе защиты информации; - этапы разработки комплексной системы защиты информации; - первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; - перечень вопросов ЗИ, требующих документационного закрепления; - виды контроля функционирования системы защиты информации на предприятии; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>Уметь:</b> определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять системы компьютерной математики для решения типовых задач; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>Владеть:</b> информацией о факторах, определяющие необходимость защиты территории и здания предприятия; - информацией о взаимодействии между субъектами, защищаемыми и использующими информацию ограниченного доступа; информацией о структуре технического задания на создание комплексной системы защиты информации на предприятии; методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; - методикой определения возможностей несанкционированного доступа к защищаемой информации; методикой разработке модели комплексной системы защиты информации; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов</p>
ПК-4	<p>способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности</p>	<p><b>Знать:</b> основные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС; критерии оценки эффективности защищенности; типы и виды программных и программно-аппаратных систем защиты информации; методы идентификация пользователей КС-субъектов доступа к данным; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; физические основы образования технических каналов утечки информации; основные теоретико-числовые методы применительно к задачам защиты информации; основные принципы организации технического, программного и информационного обеспечения</p>

		<p>защищенных информационных систем.</p> <p><b>Уметь:</b> квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфика объекта защиты; применять средства ВТ, средства программирования для эффективной реализации аппаратно-программных комплексов заданного качества и в заданные сроки; проводить испытания объектов профессиональной деятельности; производить установку, настройку и обслуживание программно-аппаратных средств защиты информации; ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>Владеть:</b> навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; навыками сопровождения программно-аппаратных средств защиты информации; навыками консультирования персонала в процессе использования указанных средств; навыками управления информационной безопасностью простых объектов.</p>
ПК-5	<p>способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества</p>	<p><b>Знать:</b> понятийно-категориальный аппарат информационной безопасности; возможности, состояние и перспективы развития информационных технологий; основной инструментарий в виде программного обеспечения для деловых применений при анализе, проектировании и прогнозировании; назначение, принципы работы средств новых информационных технологий; сетевые информационные технологии; качественные и количественные методы описания информационных технологий; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>Уметь:</b> ставить и решать типовые задачи с помощью современных информационных технологий; применять на пользовательском уровне основные средства новых информационных технологий в профессиональной деятельности; использовать информационно-поисковые средства локальных и глобальных вычислительных и информационных сетей; применять системы компьютерной математики для решения типовых задач; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>Владеть:</b> навыками применения современных информационных технологий к текущим реальным ситуациям, основными классификациями информационных систем, навыками развертывания основных программных комплексов и программ, реализующих ту или иную информационную технологию;</p>

		<p>навыками аналитического и численного решения задач математической статистики.</p>
ПК-6	<p>способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок</p>	<p><b>Знать:</b> основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; источники специальной информации; методы оценивания ее достоверности; виды информационных моделей и способы их построения; методы накопления специальной информации; методы подготовки специальной информации; методы выработки и принятия информационного решения; виды отчетно-информационных документов, методы их подготовки; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>Уметь:</b> использовать руководящие, нормативные и методические документы по организации информационно-аналитической работы; - использовать справочную и научную литературу по тематике решаемых информационных задач; оценивать специальную информацию, систематизировать ее, принимать решения о ее дальнейшем использовании; разрабатывать основные виды отчетно-информационных документов; применять средства автоматизации информационно-аналитической работы; использовать разнородные источники сведений, отчетно-информационные документы добывающих органов различных видов, в том числе на иностранном языке; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; применять на практике методы физики при исследовании технических каналов утечки информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>Владеть:</b> Основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации.</p>
ПК-7	<p>способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента</p>	<p><b>знать:</b> основные классификационные признаки экспериментов; основные элементы научно-технического эксперимента; приемы выбора основных факторов эксперимента и технологию построения факторных планов, основные виды регрессионных экспериментов, основные типы оптимальных экспериментов; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>уметь:</b> проводить классификацию экспериментов; выбирать</p>

		<p>необходимые факторы и составлять факторные планы экспериментов различного вида; строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>владеть:</b> методами выбора основных факторов эксперимента; методами подбора эмпирических зависимостей для экспериментальных данных; методами оценки коэффициентов регрессионной модели эксперимента; методами построения оптимальных планов для научных экспериментов; навыками аналитического и численного решения задач; методами проведения физического эксперимента при выявлении технических каналов утечки информации.</p>
<p><i>ПК-8</i></p>	<p>способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи</p>	<p><b>знать:</b> основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; основные отечественные и зарубежные стандарты в области компьютерной безопасности; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; способы измерения свойств объектов предметной области; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; основные типы статистических задач и математические методы их решения; основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации; физические основы функционирования технических средств и систем обработки и передачи информации; физические основы образования технических каналов утечки информации; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>уметь:</b> классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций); готовить проектную документацию на создаваемые специальные АИС; разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования; использовать результаты научно-исследовательских работ в решении задач практики; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; применять теоретико-числовые методы для оценки криптографических свойств</p>

		<p>систем защиты информации; применять системы компьютерной математики для решения типовых задач; использовать физические эффекты для обеспечения технической защиты информации; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>владеть:</b> основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно- процессуальном и финансовом законодательстве; навыками письменного аргументированного изложения собственной точки зрения; навыками публичной речи, аргументации, ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; основными методами научного познания; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации.</p>
<i>ПК-9</i>	<p>способность проводить аудит информационной безопасности информационных систем и объектов информатизации</p>	<p><b>Знать:</b> суть методологии и методы научного познания, методы анализа информационных процессов и систем, средства структурного анализа, математические модели информационных процессов; основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности.</p> <p><b>Уметь:</b> ставить и решать типовые задачи в области структурного анализа информационных процессов и систем, разрабатывать модели предметных областей, проводить исследования характеристик компонентов информационных процессов и информационных систем в целом; осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности.</p> <p><b>Владеть:</b> методами анализа информационных процессов и систем, методами разработки математических моделей информационных процессов; навыками управления информационной безопасностью простых объектов.</p>
<i>ПК-13</i>	<p>способность организовать управление информационной безопасностью</p>	<p><b>Знать:</b> – разновидности и свойства систем управления; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - методологию организационной защиты информации, ее современные проблемы и терминологию; - основные руководящие документы по обеспечению режима и секретности на объекте; - типовую структуру службы безопасности, ее основные задачи и функции</p>

		<p>должностных лиц; - основные документы, регламентирующую организационную безопасность на объекте; - правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; - правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем</p> <p><b>Уметь:</b> – программно реализовывать алгоритмы управления в цифровых системах; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - пользоваться нормативными документами по защите информации; - оценивать состояние организационной защиты информации на объекте; - определять рациональные меры по обеспечению организационной защите на объекте; - организовать работу с персоналом с секретной (конфиденциальной) информацией; - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости; - самостоятельно осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p> <p><b>Владеть:</b> - навыками работы с нормативными правовыми актами; - профессиональной терминологией; навыками формирования методических и нормативных документов, тех. документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; - навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов; – методами анализа и синтеза систем управления; – навыками использования микропроцессоров и микро-ЭВМ в системах управления.</p>
<p><i>ПК-14</i></p>	<p>способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России</p>	<p><b>Знать:</b> – разновидности и свойства систем управления; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - методологию организационной защиты информации, ее современные проблемы и терминологию; - основные руководящие документы по обеспечению режима и секретности на объекте; - типовую структуру службы безопасности, ее основные задачи и функции должностных лиц; - основные документы, регламентирующую организационную безопасность на объекте; - правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; - правовые нормы и стандарты по лицензированию в области обеспечения защиты</p>

		<p>государственной тайны и сертификации средств защиты информации; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем</p> <p><b>Уметь:</b> – программно реализовывать алгоритмы управления в цифровых системах; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - пользоваться нормативными документами по защите информации; - оценивать состояние организационной защиты информации на объекте; - определять рациональные меры по обеспечению организационной защите на объекте; - организовать работу с персоналом с секретной (конфиденциальной) информацией; - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости; - самостоятельно осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности</p> <p><b>Владеть:</b> - навыками работы с нормативными правовыми актами; - профессиональной терминологией; навыками формирования методических и нормативных документов, тех.документации в области обеспечения информационной безопасности; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; - навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы; навыками управления информационной безопасностью простых объектов; – методами анализа и синтеза систем управления; – навыками использования микропроцессоров и микро-ЭВМ в системах управления.</p>
ПК-15	<p>способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности</p>	<p><b>знать:</b> основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; виды контроля функционирования системы защиты информации на предприятии.</p> <p><b>уметь:</b> осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; синтезировать структуру комплексной системы защиты информации; оценивать эффективность системы защиты информации.</p> <p><b>владеть:</b> навыками управления информационной безопасностью простых объектов; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; методикой выявления и оценки</p>

		источников, способов и результатов дестабилизирующего воздействия на информацию; методикой определения возможностей несанкционированного доступа к защищаемой информации.
ПК-16	способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности	<p><b>знать:</b> основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; методы концептуального проектирования технологий обеспечения информационной безопасности; основные нормативные правовые акты в области информационной безопасности и защиты информации; основные понятия, законы, модели и структуры обеспечения организационной безопасности на предприятии; основные понятия, законы и модели прогнозирования принятия решений;</p> <p><b>уметь:</b> - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности; использовать нормативные правовые документы в своей профессиональной деятельности; применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности;</p> <p><b>владеть:</b> навыками управления информационной безопасностью простых объектов; навыками освоения, внедрения и сопровождения документации, в том числе и в команде; навыками нахождения организационно-управленческих решений в нестандартных ситуациях на основе результатов анализа документации и потоков документов; знаниями в области правового обеспечения информационной безопасности и навыками правоприменения нормативного законодательства в данной сфере; навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы</p>

### Задачи практики

В зависимости от тематики задания руководителя практики и тематики выпускной дипломной работы, задачами преддипломной практики являются:

- приобретение практических навыков работы в качестве специалиста (менеджера) информационной безопасности предприятия (организации);
- изучение методов обеспечения безопасности информации, применяемых на предприятии (в организации);
- освоение на практике методов предпроектного обследования объектов информатизации, проведения системного анализа результатов обследования при построении модели комплексной системы защиты информации;
- приобретение практического опыта разработки компонентов комплексной системы защиты информации предприятия (организации);
- сбор и обобщение материалов, необходимых для выполнения выпускной дипломной работы
- изучение технологии регистрации, сбора, передачи и обработки информации о несанкционированных действиях, ознакомление с характеристиками периферийной, терминальной и вычислительной техники и особенностями их эксплуатации в условиях функционирования аппаратно-программных компонентов подсистем комплексной системы защиты информации.
- изучение документации комплексной системы защиты информации предприятия (организации), получение знаний по оформлению технических и рабочих проектов системы защиты информации и порядку внедрения утвержденных решений.
- привитие навыка системного подхода при проектировании комплексной системы защиты информации и отдельных ее подсистем.

• приобретение навыков выбора комплекса технических средств и сопряжения их в единую систему, расчета необходимого числа технических средств, расчета разграничения доступа к ресурсам информационной системы предприятия (организации).

• ознакомление с системной классификацией и кодированием информации, принятой в информационной системе предприятия (организации).

• ознакомление с психологическими аспектами проблемы внедрения и функционирования комплексной системы защиты информации на предприятии (в организации) и в особенности в области применения технических средств (регистраторов, сканеров, дисплеев, графопостроителей, факс-модемов, видеоконтроля и специального оборудования).

• анализ характеристик информационных процессов и формирование исходных данных для проектирования комплексной системы защиты информации предприятия (организации).

• приобретение навыков обслуживания средств ЗИ в ЭВМ, сетях ЭВМ и автоматизированных информационных системах.

• знакомство с методами и средствами обеспечения безопасности информации в документообороте, управлении бизнес-процессами и процессами административного и оперативного руководства.

• подготовка и систематизация необходимых материалов для выполнения выпускной дипломной работы.

В ходе преддипломной практики студент может выполнять следующие виды работ по заданию преподавателя:

• подготовка практических и экспериментальных исследовательских заданий на оборудовании организации (например, установка и конфигурирование необходимого программного обеспечения и оборудования, проработка аналитических задач в интересах предприятия, сбор необходимых материалов);

• подготовка учебно-методических материалов (сбор информации, выполнение обзора современных технологий);

• разработка прикладного (части прикладного) программного обеспечения, в том числе в области автоматизации аналитической деятельности и т.д.

Составитель: доцент кафедры ИЗИ к.т.н. Тельный А.В.  
должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов  
ФИО, подпись

Директор института ИТР А.А. Галкин  
ФИО, подпись

Дата: Печать института (факультета)

