Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

Кафедра информатики и защиты информации

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РАДИОЭЛЕКТРОНИКИ

УТВЕРЖДАЮ

Проректор по ОД
_____ А.А. Панфилов
"31" августа 2019 г.

Программа преддипломной практики

Направление подготовки
10.04.01 «Информационная безопасность»

Профиль (программа) подготовки
Автоматизация информационно-аналитической деятельности

Квалификация (степень) выпускника
магистр

г. Владимир 2019

Вид практики - Производственная

Вид практики - Преддипломная

1. 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.

Тема задания на преддипломную практику должна соответствовать профилю направления и быть увязана с перечнем рекомендованных направлений тем выпускных квалификационных работ, который ежегодно разрабатывается кафедрой в соответствии с профилем ее учебно-методической и научно-исследовательской деятельности. В процессе выполнения преддипломной практики должны быть получены основные практические, экспериментальные, модельные результаты, используемые при выполнении выпускной квалификационной работы, разработаны действующие макеты программно-технических изделий. Тема преддипломной практики предлагается студентом по согласованию с научным руководителем соответствующего направления. В процессе практики проводится изучение автоматизированных средств и систем, реализующих технологии защиты информации, обучаемый студент приобретает навыки исследования и проектирования подсистем обеспечения безопасности информации предприятия (организации).

Целями преддипломной практики являются:

- приобретение практических навыков работы в качестве специалиста (менеджера) ИБ предприятия (организации);
- получение практических, экспериментальных, модельных результатов, используемых при выполнении выпускной дипломной работы;
- сбор сведений об организации прохождения практики, необходимых для выполнения выпускной квалификационной работы;
-получение практических консультаций действующих специалистов предприятий и организаций по вопросам тематики дипломной работы;
- приобретение практического опыта разработки компонентов КСЗИ предприятия (организации);
- приобретение навыка системного подхода при проектировании КСЗИ и отдельных ее подсистем;
- приобретение навыков исследовательской и аналитической работы в области информационной безопасности.

2. Задачи преддипломной практики.

В зависимости от тематики задания руководителя практики и тематики выпускной квалификационной 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 квалификационной 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 квалификационной 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.

3. Способы проведения преддипломной практики – практика может быть стационарной или выездной.

4. Формы проведения преддипломной практики.

Преддипломная практика проводится непрерывно с выделением в учебном графике периода времени по окончании 3 семестра обучения. Форма проведения является заводской

или лабораторной. При прохождении практики на выпускающей кафедре и в научных лабораториях ВлГУ, руководство организационными аспектами преддипломной практики осуществляет преподаватель выпускающей кафедры информатики и защиты информации, назначаемый заведующим кафедрой ИЗИ. Как правило, руководителем практики назначается научный руководитель, руководитель дипломного проектирования студента. При прохождении преддипломной практики на предприятиях и организациях, руководство организационными аспектами практики осуществляет как преподаватель выпускающей кафедры, руководитель дипломного проектирования студента, так и должностное лицо, назначаемое руководителем организации, принимающей студентов на практику (руководитель от предприятия).

В случае прохождения преддипломной практики в сторонней организации сотрудник этой организации может являться консультантом студента. В этом случае на кафедру должно быть представлено письмо, заверенное печатью организации, о согласии принять студента на практику с указанием фамилии, имени, отчества (полностью) и должности консультанта, его контактного телефона и адреса электронной почты. Вместо письма допускается иметь долгосрочный договор с организацией о сотрудничестве и всю информацию о руководителе от предприятия заполнять в дневнике практики.

Преподаватель, руководитель дипломного проектирования студента, осуществляет руководство содержательными аспектами практики, предоставляет студенту информацию по заданию на практику и осуществляет текущий контроль работы студента. Обучаемые студенты получают индивидуальное задание. Тема задания практики должна соответствовать профилю направления обучения и быть увязана с перечнем рекомендованных направлений выпускных квалификационных работ (дипломных работ), который ежегодно разрабатывается кафедрой в соответствии с профилем ее учебно-методической и научно-исследовательской деятельности.

5. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

В результате прохождения преддипломной практики обучающийся должен приобрести следующие практические навыки, умения, общекультурные (универсальные) и профессиональные компетенции:

Коды компетенции	Результаты освоения ООП *Содержание компетенций*	Перечень планируемых результатов при прохождении практики
ОК-2	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения	**знать:** 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. **уметь:** 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. **владеть:** 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	**знать:** экономическое планирование и

	самостоятельному обучению и применению новых методов исследования профессиональной деятельности	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. **уметь:** 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. **владеть:** приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям; методами проведения физического эксперимента при выявлении технических каналов утечки информации.
ПК-1	способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	**знать:** 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. **уметь:** 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. **владеть:** навыками аналитического и численного решения задач математической статистики; методами проведения физического эксперимента при выявлении технических каналов утечки информации; навыками управления информационной безопасностью простых объектов.
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	**Знать:** 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. **Уметь:** - 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. **Владеть:** методами и средствами выявления угроз безопасности автоматизированным системам; навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем; навыками участия в 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.
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов	**Знать:** 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. **Уметь:** 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. **Владеть:** информацией о факторах, определяющие необходимость защиты территории и здания предприятия;-информацией о взаимодействии между субъектами, защищающими 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
ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	**Знать:** 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 защищенных информационных систем. **Уметь:** 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. **Владеть:** 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.
ПК-5	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	**Знать:** 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. **Уметь:** 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. **Владеть:** 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; навыками аналитического и численного решения задач математической статистики.
ПК-6	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	**Знать:** 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. **Уметь:** 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. **Владеть:** 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.
ПК-7	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	**знать:** 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. **уметь:** проводить классификацию экспериментов;

		выбирать 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. **владеть:** 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.
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	**знать:** 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. **уметь:** 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 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. **владеть:** 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.
ПК-9	способность проводить аудит информационной безопасности информационных систем и объектов информатизации	**Знать**: 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. **Уметь:** 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. **Владеть**: методами анализа информационных процессов и систем, методами разработки математических моделей

		информационных процессов; навыками управления информационной безопасностью простых объектов.
ПК-13	способность организовать управление информационной безопасностью	**Знать**: – 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 государственной тайны и сертификации средств защиты информации; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем **Уметь:** – 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 **Владеть:** - 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.
ПК-14	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	**Знать:** – 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 государственной тайны и сертификации средств защиты информации; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем **Уметь:** – 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 **Владеть:** - 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.
ПК-15	способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности	**знать:** 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. **уметь:** 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. **владеть:** 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 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	**знать:** 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; **уметь:** - 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; **владеть:** 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

6. Место преддипломной практики в структуре ОПОП магистратуры

Преддипломная практика магистров магистрантов относится к Блоку Б2 «Практики, в том числе научно-исследовательская работа (НИР)». Настоящая программа практики основывается на требованиях, определённых Федеральным государственным образовательным стандартом высшего образования по направлению 10.04.01 «Информационная безопасность».

Преддипломная практика базируется на основе изучения полного цикла всех дисциплин обучения по программе высшего профессионального образования по направлению 10.04.01 «Информационная безопасность». Практика проводится на 2 курсе, по окончании 3 семестра обучения. Требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки студентов по направлению 10.04.01 «Информационная безопасность».

Преддипломная практика необходима для успешной подготовки выпускной квалификационной работы студента (магистерской диссертации).

7. Место и время проведения преддипломной практики.

Преддипломная практика проводится по окончании 3 семестра обучения. Данная практика является стационарной и проводится в течение 6 недель в сторонних организациях (учреждениях, предприятиях) и структурных подразделениях по профилю направления информационной безопасности или на выпускающей кафедре и в научных лабораториях ВлГУ.

Практика должна проводиться в организациях, оснащенных современной вычислительной техникой, выбранных студентом самостоятельно или предложенных университетом. Проходить практику в предусмотренном объеме можно в России или других странах (в порядке прохождения зарубежных стажировок), непрерывно или с разрывом во времени, набрав необходимое количество часов.

8. Объем практики в зачетных единицах и ее продолжительность в неделях или академических часах

Общая трудоемкость преддипломной практики составляет:

3 семестр распределенная практика:

__9____ зачетных единицы; __324_____ часа.

9. Структура и содержание преддипломной практики

№ п/п	Разделы (этапы) практики	Виды преддипломной работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля
3 семестр распределенная практика			
1	Подготовительный	Получение задания на практику. Ознакомление с заданием, планирование работы. (4 часа)	Собеседование
2	Подготовка теоретических материалов.	Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических указаний и т.д. (12 часов)	Собеседование, консультации
3	Практические работы по теме задания на практику	Проведение практических, экспериментальных, лабораторных и др. занятий (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования и т.д.) (278 часов)	Консультации (в том числе и дистанционно)
4	Отчёт по практике	Составление отчёта по практике (30 часов)	Отчет (в том числе и в электронном виде)
5	Зачёт по практике	Подготовка к зачёту. Зачет по практике (8 часов)	Зачет

10. Формы отчетности по практике

По итогам аттестации преддипломной практики выставляется зачет с оценкой.

В состав отчёта по преддипломной практике должны входить:

• индивидуальное задание на прохождение практики, утверждённое руководителем практики (руководителем дипломной работы);

• дневник практики;

• отчет по практике (материалы с результатами работы и предложениями);

• электронные материалы по практической работе или собранным сведениям;

- оценочный лист сформированности компетенций по итогам преддипломной практики, заполняемый руководителем практики.

Все примеры оформления отчетных документов приведены в методических указаниях по проведению преддипломной практики студентов по направлению 10.04.01 «Информационная безопасность».

Структура и оформление отчетов о преддипломной практике должны соответствовать основным требованиям стандарта ГОСТ 7.32-2001 – «Отчет о научно-исследовательской работе – Структура и правила оформления».

Структурными элементами отчета являются:

- титульный лист;
- лист аннотации;
- содержание;
- определения;
- обозначения и сокращения;
- введение;
- основная часть;
- заключение;
- список использованных источников;

- приложения.

Они включаются в отчет строго в указанном порядке. Остальные структурные элементы включают в отчет по усмотрению исполнителя с учетом настоящих требований и требований ГОСТ 7.32-2001. При оформлении отчетов следует придерживаться следующих правил и рекомендаций.

На титульном листе отчет должен быть подписан автором, консультантом (если есть), научным руководителем, заведующим кафедрой.

Лист аннотации должен содержать:

- сведения об объеме отчета (суммарное количество страниц без учета приложений), количестве иллюстраций, таблиц, приложений, количестве разделов отчета, количестве использованных источников;
- перечень ключевых слов;
- реферат отчета (не более 500 печатных знаков), в котором в краткой форме, удобной для библиотечного поиска, указываются: объект исследования или разработки, цель работы, метод проведения работы, результаты, область применения, значимость работы.

Во введении обязательно должны быть обоснованы актуальность, теоретическая и практическая значимость работы, сформулирована цель работы и перечислены задачи, решаемые для достижения поставленной цели. Объем введения, как правило, не превышает 2 – 2,5 страниц.

Основная часть, как правило, состоит из 3 - 4 самостоятельных разделов, каждый из которых характеризуется логической завершенностью и при необходимости может делиться на подразделы и пункты (заголовок «Основная часть» в отчете не пишется!). Первый раздел, как правило, содержит обзор рассматриваемой предметной области со ссылками на источники информации и постановку задачи работы. Далее следует изложение аналитических, теоретических и прикладных результатов, полученных лично автором в процессе выполнения работы (алгоритмы, протоколы, спецификации, схемы, формулы, расчеты и т.п.). Заключительные разделы содержат практические аспекты работы, описание макетной, экспериментальной части (описание разработанных программных модулей, аппаратных устройств, интерфейсов, графики или таблицы с результатами экспериментов и т.п.), обсуждение возможностей применения полученных результатов в других работах. В конце каждого раздела следует сформулировать краткие выводы (1-2 абзаца) по данному разделу. Разделы основной части должны быть пронумерованы, начиная с первого (введение к отчету и заключение не нумеруются!). Наибольший раздел не должен более, чем в 2 – 3 раза, превышать наименьший.

В заключении формулируется основной результат работы и (по пунктам) выводы по результатам выполненной работы (как правило, 3 – 5 выводов (например, один по каждому разделу)), а также указываются возможные (планируемые) пути и перспективы продолжения работы. Объем заключения, как правило, не превышает 1,5 – 2 страниц.

Отчет должен быть отпечатан шрифтом Times New Roman № 14 через 1,5 интервала на одной стороне белой бумаги формата А4. Размеры полей: сверху, снизу – 20 мм, слева – 30 мм, справа – 10 мм. Листы отчета обязательно должны быть скреплены жестким соединением и пронумерованы сквозной нумерацией, начиная с титульного листа (на котором номер не ставится). Номер страницы проставляют в центре нижней части листа без точки. Рекомендуемый объем отчета о практике (без приложений) составляет 30–40 страниц. По тексту отчета должны содержаться ссылки на источники информации. Ссылки на публикации, приведенные в списке использованных источников, допускаются только цифровые.

11. Фонд оценочных средств для проведения аттестации по преддипломной практике.

По окончании практики студенты сдают зачет, который принимается комиссией в составе преподавателей кафедры (не менее трех доцентов кафедры, один из которых является руководителем практики). Студенты представляют на зачет, полностью оформленный комплект отчетной документации. К отчету могут прилагаться материалы,

разработанные студентом, планы семинарских занятий и другая информация, характеризующая вклад студента в изучение предметной области практики.

Аттестация по результатам прохождения преддипломной практики проводится в течение первых двух недель после окончания практики в форме комиссионной защиты студентом результатов работы по практике. Оценивается отчет студента, выступление на защите практики и отзыв преподавателя, который являлся руководителем практики. Допускается при должном уровне подготовки студентами отчетов по преддипломной практике совмещать отчет по практике с предварительной защитой выпускной квалификационной работы, с выдачей допуска кафедры к защите государственной аттестационной комиссией выпускной квалификационной работе.

Примерные контрольные вопросы и задания по типовым заданиям на преддипломную практику. *(Для конкретного задания студентов на преддипломную практику вопросы и задания могут быть уточнены руководителем практики и членами аттестационной комиссии).*

Примерные вопросы и задания для сбора информации по предприятию прохождения практики

Отметить наличие на предприятии организационно-правовой документации по обеспечению информационной безопасности (Положение о коммерческой тайне на предприятии, Концепция обеспечения информационной безопасности, Политика обеспечения информационной безопасности, другие руководящие документы, положения и инструкции).

Наличие (отсутствие) специального подразделения по ЗИ, его структура, функции, должностные обязанности сотрудников

Привести (по возможности) утвержденный Перечень сведений (или ссылку на него), которые в рамках данного предприятия имеют конфиденциальный характер (составляют служебную или коммерческую тайну), а также названия документов и электронных информационных ресурсов их содержащих.

обследовать объект и его территорию (при необходимости), составить акт обследования состояния инженерно-технической укрепленности объекта и согласно РД.36.003-2002г. По категории объекта определить в каждом помещении соответствуют ли элементы технической конструкции здания (полы, стены, потолки, окна, запорные устройства) требованиям приложений РД.36.003-2002 г.

Привести информацию о структуре защищаемого объекта, назначении помещений.

Привести перечень помещений, оборудованных ОТС.

Отметить наличие (или отсутствие) физической охраны объекта и место расположения поста физической охраны время несения службы.

Отметить наличие (или отсутствие) АРМ ОТС, возможности его комплексирования в интегрированные системы безопасности с подсистемами СОТ, СКУД, АУПС и АСПТ.

Привести информацию об используемых на объекте ПКП и извещателей.

Необходимо оценить правильность проведенных монтажных работ и рациональность размещения охранных извещателей согласно требований РД 78.36.003-2002г. и РД 78-145-93г.

Описать используемую на объекте тактику охраны и рубежность распределения шлейфов сигнализации.

Привести информацию о количестве и распределении ПЦН выходов от ПКП (при наличии договора на централизованную охрану).

Привести сведения об организации обслуживания ТСО.

Оценить структуру распределения шлейфов сигнализации (радиальная, двухпроводная линия и др.) и работоспособность средств ОТС.

Привести структурную схему ОТС и схемы распределения шлейфов сигнализации на поэтажных планах помещений.

Схема расположения защищаемых помещений или зон, размещения проходных,

помещений для расположения АРМ управления.

Наличие физической охраны и их функции по управлению доступом.

Наименование объектов, оснащенных СКУД (количество точек прохода) - административные, производственные, складские, бытовые помещения, производственные площадки или внутренние территории с КПП. Тип прохода по каждой точке прохода (последовательность прохода, двухсторонний или нет, шлюз и др.).

Структура СКУД (сетевая, автономная), наличие АРМ, его функции и используемое программное обеспечение.

Элементы технической укрепленности СКУД (тамбуры, ограждения, турникеты, калитки). Необходимо оценить рациональность выбора установленных исполнительных устройств и режима их работы.

Предполагаемое максимальное количество сотрудников, посетителей, единиц транспорта.

Пропускная способность аппаратуры СКУД и ее соответствие людским потокам.

Тип идентификаторов пользователей (пропуска, магнитные карты, биометрия, дистанционные или контактные).

Краткое описание функциональных возможностей СКУД. Обычно система должна обеспечивать:

- регистрацию и протоколирование тревожных и текущих событий;
- приоритетное отображение тревожных событий;
- управление работой преграждающими устройствами в точках доступа по командам оператора;
- задание временных режимов действия идентификаторов в точках доступа «окна времени» и уровней доступа;
- защиту технических и программных средств от НСД к элементам управления;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
- установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях;
- блокировку прохода по точкам доступа командой с пункта управления.

Оснащенность бюро пропусков комплексом для оперативного изготовления идентификационных удостоверений с фотографиями пользователей, другим специальным оборудованием.

Привести сведения об организации обслуживания СКУД.

Необходимо оценить количество и расположение АРМов для управления СКУД (АРМ-администраторов безопасности, АРМ-службы охраны, АРМ-бюро пропусков, АРМ службы персонала, другие АРМ). Взаимодействие АРМ СКУД с АРМ ОТС, АУПС (интеграция). Наличие сети передачи данных, связывающей объекты (АРМы системы управления доступом должны располагаться в пределах ЛВС). Защищенность АРМов СКУД от НСД.

Составляется структурная схема СКУД и схемы распределения кабельных линий на поэтажных планах помещений. При этом используется условные обозначения согласно РД.78.ВО01.-99

Названия и назначения блоков внутри объекта информатизации (выделенная территория, здание, этаж, группа помещения), в которых функционирует СОТ (административные, производственные, складские, бытовые помещения, производственные площадки, смежные или внутренние территории различного назначения).

Количество отдельных зон, участков, объектов, оснащаемых системой (перечень защищаемых зон, территорий, отдельных зданий, выделенных участков).

Указать на схеме расположение защищаемых помещений или зон, размещения постов наблюдения. Описать по каждой зоне контроля уровень освещенности и условия

видимости, климатические условия.

Цели наблюдения в дневном и ночном режиме (по приоритету) (Например, днем - идентификация личности, определение номера въезжающего автомобиля, ночью - обнаружение автомобиля, человека, и т. д. (с предоставлением планов зон контроля, и прилегающей территории)).

Решаемые системой задачи:

- контроль НСД сотрудников или нарушителей на территорию (или с территории) объекта через проходные и КПП;
- контроль НСД сотрудников или нарушителей на территорию (или с территории) объекта через ограждения или запретные зоны;
- защита людей и материальных ценностей от преступных посягательств в контролируемой зоне охраняемого объекта;
- контроль за ситуационным положением в выделенном помещении или на территории, прилегающей к объекту;
- идентификация личности посетителя или сотрудника объекта при прохождении КПП на основании данных видеотеки;
- идентификация государственного номера автомашины при проезде КПП объекта на основании баз данных службы охраны или бюро пропусков;
- контроль за действиями сотрудников определенных служб на объекте в ходе технологического процесса или исполнения ими своих служебных обязанностей;
- автоматическая фиксация и хранение в течение определенного времени записи противоправных или иных событий по тревожному извещению с защищаемого объекта;
- автоматическая фиксация и хранение в течение определенного времени (указать размер архива) всех событий с охраняемого объекта или территории.

Посты наблюдения и управления комплексом:

- количество независимых постов наблюдения (с указанием мест их размещения на планах);
- возможность видеорегистрации на видеорегистраторы (непрерывно, по усмотрению оператора, по сигналу охранных датчиков);
- возможность одновременного просмотра на одном мониторе всех видеокамер комплекса (всегда или только в режиме непосредственного наблюдения за объектом);
- возможность выполнять охранные функции (детекторы движения);
- возможность моментальной распечатки интересующих кадров на видеопринтере;
- возможность согласованной работы комплекса с персональным компьютером (компьютерами). В этом случае указать количество и расположение АРМов видеонаблюдения, структуру компьютерной сети на объекте.

Описание СОТ

Общие сведения:

- вид системы (цветная, черно-белая, комбинированная);
- срок хранения видеозаписей в архиве (обычно, одна неделя);
- возможность фиксации аудиоинформации с охраняемых объектов;
- наличие и расположение щитов электропитания вблизи мест установки оборудования и на постах наблюдения;
- наличие резервного или дублирующего питания;
- возможность дальнейшего расширения путем добавления новых телекамер и постов наблюдения (охраны);
- описание общей тактики отображения и записи информации, структуры и приоритетности защищаемых зон, порядка и уровня совмещения с взаимодействующими системами.

Технические характеристики системы:

- разрешение видеокамер, видеорегистратора;
- вид ПЗС, фокусное расстояние и параметры вариообъектовов, тип управления диафрагмой и др.

Технические характеристики устройств управления и коммутации видеосигналов:

- разрешение;
- вид входного сигнала извещения о тревоге;
- максимальные коммутируемые напряжения и ток.

Технические характеристики видеомониторов:

- разрешение;
- максимальная яркость изображения;
- геометрические и нелинейные искажения изображения.

Объекты, подлежащие оснащению комплексом защиты корпоративной сети (наименование, характеристика деятельности).

Решаемые комплексом защиты проблемы (как минимум контроль НСД). Общие данные о функционировании информационной системы.

Порядок назначения прав по доступу к критичным ресурсам.

Регламент резервирования и восстановления критичной информации.

Расположение критичной информации.

Информационные потоки критичной информации, относительно рабочих станций, серверов, сегментов.

Наличие систем электронного документооборота.

Наличие критичных для предприятия процессов электронной обработки и передачи данных.

Возможность круглосуточной работы.

Информация о топологии сети, сетевых соединениях и уз-лах

Карта сети:

- количество и тип серверов (платформы, операционные системы, сервисы),
- приложения,
- количество и тип рабочих станций (платформы, ОС, приложения, решаемые задачи),
- используемые сетевые протоколы.

Указать на схеме сегменты и способы их соединения (маршрутизаторы, хабы, мосты и прочее).

Указать вариант организации выхода в Internet:

- подключение выделенного компьютера (способ подключения, авторизации и пр.);
- подключение сети (способ подключения, использование прокси-служб и прочее);
- необходимость контроля трафика и разграничения доступа пользователей;
- наличие внутри предприятия собственного WEB, FTP серверов.

Использование встроенных (приобретенных) средств мониторинга, безопасности и архивации

Защита ПК от НСД (аудит, разграничение доступа), защита и разграничение доступа к ПК при работе на них нескольких пользователей.

Межсетевые экраны - защита от внешних/внутренних атак.

Системы авторизации.

Антивирусная защита.

Средства архивирования, режим их работы.

Системы протоколирования действий пользователей.

Криптографическая защита.

Средства системного аудита.

Системы мониторинга сети.

Защита вычислительной техники от взлома, краж.

Анализаторы протоколов.

Сканеры - сканирование ресурсов сети на возможные уязвимости и выдача рекомендаций для их устранения.

Разделение критичных сегментов сети.

Системы мониторинга безопасности - проверка правильности настройки корпоративных серверов, мониторинг безопасности корпоративной сети в реальном

времени.

Анализ информационных угроз

Определение видов информационных угроз в помещениях и технических каналах.

С проникновением на объект:

- внедрение специальных устройств с целью перехвата информационных сигналов, их преобразования и передачи за пределы зоны безопасности объекта по различным каналам;

- несанкционированная запись информационных сигналов с использованием средств регистрации информации.

Без проникновения на объект:

- прослушивание каналов связи;

- преднамеренный разрыв каналов связи;

- перехват остаточных информационных сигналов и электромагнитных излучений, распространяющихся за пределы зоны безопасности.

Определение видов перехватываемой информации в основных каналах утечки информации:

- акустический канал - речевые и прочие акустические сигналы;

- виброакустический канал - речевые и прочие акустические сигналы;

- утечка по проводному каналу - речевые и прочие акустические сигналы, факсимильная, телеграфная, телетайпная информация, информация, обрабатываемая на ЭВМ, или транслируемая по модемным каналам;

- электромагнитные поля - информация передаваемая по радиотелефону и радиосвязи, информация, передаваемая по радиомодему;

- ПЭМИН - информация, обрабатываемая на ЭВМ, ПЭМИН прочего офисного оборудования, промодулированный полезным акустическим сигналом;

- оптический - скрытая фото, кино и видеосъемка, видеонаблюдение из вне зоны охраны.

Оценка оперативно-тактических возможностей нарушителя. Формирование модели нарушителя, его возможностей по:

- перехвату информации в непосредственной близости от территории объекта,

- легальному проникновению на территорию объекта, например, иметь статус сотрудника родственного предприятия или клиента,

- временному использованию или стационарной установке технических средств промышленного шпионажа,

- получению априорных данных, которые могут облегчить планирование и проведение операций по перехвату информации.

К таким данным относятся, например:

- тематика перехватываемой информации,

- сведения о перечне решаемых вопросов,

- технические средства хранения, обработки и передачи информации, общие параметры сигналов, несущих полезную информацию,

- расположение помещений,

- организация и техническая оснащенность службы безопасности,

- распорядок работы объекта,

- психологическая обстановка в коллективе.

Оценка технического оснащения нарушителя по следующим группам технических средств перехвата и регистрации информации:

- радиомикрофоны (перехват акустической информации);

- телефонные радиопередатчики (перехват телефонной информации);

- системы кабельных микрофонов (перехват акустической информации;

- системы с передачей информации по сетям электропитания и телефонным линиям (перехват акустической информации).

- направленные микрофоны (перехват акустической информации;

- комплексы для перехвата информации с монитора ЭВМ в реальном времени;

- стетоскопы (перехват акустической информации);

- аппаратура для перехвата остаточных информативных сигналов в линиях питания и заземления;

- аппаратура для перехвата радиоэфирной информации и ПЭМИН офисного оборудования;

- звукозаписывающая аппаратура (перехват акустической информации).

Оценка технических возможностей потенциального нарушителя с учетом его финансового положения и целесообразности вложения средств в конкретную операцию по перехвату информации. Обычно количество вложенных средств пропорционально стоимости интересующей нарушителя информации.

Функции специального оборудования.

Защита от утечек информации по акустическому каналу, за счет: ПЭМИН средств ВТ и звукоусилительной аппаратуры, по цепям питания и заземления, по каналу визуального наблюдения, виброакустическому каналу.

Защита от утечек по проводному каналу - речевые и прочие акустические сигналы, факсимильная, телеграфная, телетайпная информация, информация, обрабатываемая на ЭВМ, или транслируемая по модемным каналам.

Защита от утечек через электромагнитные поля - информация передаваемая по радиотелефону и радиосвязи, информация, передаваемая по радиомодему.

Защита от утечек через ПЭМИН - информация, обрабатываемая на ЭВМ, ПЭМИН прочего офисного оборудования, промодулированный полезным акустическим сигналом;

Защита от утечек через оптический канал - скрытая фото, кино и видеосъемка, видеонаблюдение из вне зоны охраны.

Технология работы СПЭШ

Система защиты информации (СЗИ) должна обеспечивать оперативное и незаметное для окружающих выявление активных радиомикрофонов, занесенных в помещение, имеющих традиционные каналы передачи информации.

Аппаратура СЗИ по акустическому и виброакустичекому каналу должна включаться в работу по команде оператора.

Включение аппаратуры защиты информации от съема с использованием записывающих устройств должно управляться оператором.

СЗИ должна обеспечивать противодействие перехвату информации, передаваемой по телефонной линии (на участке до АТС).

Функциональные возможностям СПЭШ

Система должна обеспечивать защиту информации от утечек:

- по акустическому каналу с использованием различной звукозаписывающей аппаратуры, внесенной на объект;

- по акустическому каналу в виде мембранного переноса речевых сигналов через перегородки за счет малой массы и слабого затухания сигналов;

- по акустическому каналу за счет слабой акустической изоляции (щели у стояков системы отопления, вентиляция);

- по виброакустическому каналу за счет продольных колебаний ограждающих конструкций и арматуры систем отопления;

- по проводному каналу от съема информации с телефонной линии (городская и внутренняя телефонная сеть, факсимильная связь, переговорные устройства, системы конференц-связи и оповещения, системы охранной и пожарной сигнализации, сети электропитания и заземления);

- по каналу электромагнитных полей основного спектра сигнала за счет использования различных радиомикрофонов, телефонных радиопередатчиков;

- по оптическому каналу за счет визуального наблюдения за объектом с использованием технических средств;

- по каналу ПЭМИН за счет модуляции полезным сигналом электромагнитных полей, образующихся при работе бытовой техники;

- по каналу ПЭМИН при обработке информации на ПЭВМ за счет паразитных излучений компьютера.

Стационарные средства защиты информации

Определение стационарных средств защиты информации в выделенном помещении для проведения переговоров и совещаний. Обычно используются следующие виды технических средств:

- система, блокирующая передачу информации по сети питания,
- средство блокировки виброканала,
- обнаружитель работающих диктофонов,
- подавитель радиомикрофонов и диктофонов,
- генераторы акустического шума,
- стационарный детектор электромагнитного поля.

Определение стационарных средств защиты информации в кабинетах руководства и помещениях, в которых проводятся переговоры и совещания. Обычно используются следующие виды технических средств:

- комплексный генератор шума,
- система вибродатчиков,
- обнаружитель работающих диктофонов,
- подавитель радиомикрофонов и диктофонов,
- генераторы акустического шума,
- стационарный индикатор электромагнитного поля,
- фильтры для проводных линий.

Определение стационарных средств защиты информации в прочих технологических помещениях, в которых циркулирует информация, предназначенная для служебного пользования. Обычно используются следующие виды технических средств:

- фильтры для проводных линий,
- при наличии в помещениях ПЭВМ должны быть установлены генераторы радиоэлектронного шума (в варианте защиты рабочего места).

Определение стационарных средств защиты информации в выделенных каналах связи для передачи:

- секретной информации,
- конфиденциальной информации,
- информации для служебного пользования.

Описание показателей и критериев оценивания компетенций, а также шкал оценивания по результатам преддипломной практики:

Характеристика работы		Баллы	
1. Оценка работы по формальным критериям			
1.1.	Использование литературы (достаточное количество актуальных источников, достаточность цитирования, использование нормативных документов, научной и справочной литературы)	0-5	
1.2.	Соответствие отчета требованиям нормоконтроля и методическим указаниям кафедры	0-5	
	ВСЕГО БАЛЛОВ	0-10	
2. Оценка отчета по содержанию			
2.1.	Корректность и точность технического описания выполненной практической работы.	0-5	
2.2.	Соответствие выполненной практической работы заданию на практику. Качество функционирования выполненной разработки.	0-10	

2.3.	Оптимальность выполненной разработки, наличие недочетов и ошибок.	0-25	
2.4.	Оригинальность и практическая значимость предложений и рекомендаций в работе	0-5	
	ВСЕГО БАЛЛОВ	0-45	
3. Оценка защиты отчета по практике			
3.1.	Качество доклада (структурированность, полнота раскрытия, аргументированность выводов)	0-5	
3.2.	Качество и использование презентационного материала (информативность, соответствие содержанию доклада, наглядность, достаточность).	0-5	
3.3.	Ответы на вопросы комиссии (полнота, глубина, оригинальность мышления).	0-15	
	ВСЕГО БАЛЛОВ	0-25	
4. Отзыв руководителя практики		0-20	
	СУММА БАЛЛОВ	**100**	

Шкала соотнесения баллов и оценок

Оценка	**Количество баллов**
«2» неудовлетворительно	0-60
«3» удовлетворительно	61-73
«4» хорошо	74-90
«5» отлично	91-100

Члены комиссии оценивают отчет и работу студента на практике, исходя из соответствия выполненной работы заданию, самостоятельности разработки задания, обоснованности выводов и предложений, а также исходя из уровня сформированности компетенций студента, который оценивают руководитель практики студента члены комиссии. Результаты определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценки:

«Отлично»:

- доклад структурирован, раскрывает выполнение задания, цель и задачи работы, освещены вопросы практического применения и внедрения результатов работы в практику;
- отчет по практике отвечает предъявляемым требованиям и оформлена в соответствии со стандартом;
- представленный демонстрационный материал высокого качества в части оформления и полностью соответствует содержанию отчета;
- ответы на вопросы членов комиссии показывают глубокое знание исследуемой темы, подкрепляются ссылками на соответствующие литературные источники, выводами и расчетами (при необходимости), демонстрируют самостоятельность и глубину изучения материалов студентом;
- выводы в отзыве руководителя по отчету не содержат замечаний;
- результат оценки уровня сформированности компетенций (в соответствии с оценкой руководителя) составляет от 15 до 20 баллов.

«Хорошо»:

Доклад структурирован, допускаются одна-две неточности, но эти неточности устраняются при ответах на дополнительные уточняющие вопросы.

- отчет по практике выполнен в соответствии с целевой установкой, отвечает предъявляемым требованиям и оформлена в соответствии со стандартом.

- представленный демонстрационный материал хорошего качества в части оформления и соответствует содержанию отчета и доклада;

- ответы на вопросы членов комиссии показывают хорошее владение материалом, подкрепляются выводами и расчетами (при необходимости), показывают самостоятельность и глубину изучения проблемы студентом;

- выводы в отзыве руководителя без замечаний или содержат незначительные замечания, которые не влияют на качество работы;

- результат оценки уровня сформированности компетенций (в соответствии с оценкой руководителя) составляет от 12 до 17 баллов.

«Удовлетворительно»:

- доклад структурирован, допускаются неточности, но эти неточности устраняются в ответах на дополнительные вопросы;

- отчет по практике выполнен в соответствии с целевой установкой, но не в полной мере отвечает предъявляемым требованиям;

- представленный демонстрационный материал удовлетворительного качества в части оформления и в целом соответствует содержанию отчета и доклада;

- ответы на вопросы членов комиссии носят не достаточно полный и аргументированный характер, не раскрывают до конца сущности вопроса, слабо подкрепляются выводами, показывают недостаточную самостоятельность и глубину изучения проблемы студентом;

- выводы в отзыве руководителя содержат замечания, указывают на недостатки, которые не позволили студенту в полной мере выполнить задание по практике;

- результат оценки уровня сформированности компетенций (в соответствии с оценкой руководителя) составляет от 8 до 14 баллов.

«Неудовлетворительно»:

- доклад недостаточно структурирован, допускаются существенные неточности или явные технические ошибки и эти неточности не устраняются в ответах на дополнительные вопросы;

- отчет по практике не отвечает предъявляемым требованиям;

- представленный демонстрационный материал низкого качества в части оформления и не соответствует содержанию выполнения работы и доклада;

- ответы на вопросы членов комиссии носят неполный характер, не раскрывают сущности вопроса, не подкрепляются материалами отчета, показывают недостаточную самостоятельность и глубину изучения проблемы студентом;

- задание на практику осталось не выполненным или ответы на вопросы членов комиссии показывают не самостоятельность выполнения задания студентом;

- выводы в отзыве руководителя содержат существенные замечания, указывают на недостатки, которые не позволили студенту выполнить задание на практику;

- результат оценки уровня сформированности компетенций (в соответствии с оценкой руководителя) составляет менее 8 баллов.

12. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем.

В процессе организации и проведения преддипломной практики применяются современные образовательные и научно-исследовательские технологии.

Образовательные технологии: семинары в диалоговом режиме с элементами дискуссии, лабораторный практикум (в зависимости от задания практики), выступления с докладами, разбор конкретных ситуаций.

Научно-исследовательские технологии, структурно-логические технологии, представляющие собой поэтапную организацию постановки дидактических задач, выбора способа их решения, диагностики и оценки полученных результатов.

Проектные технологии, направленные на формирование критического и творческого мышления, умения работать с информацией и реализовывать собственные проекты в рамках формирования компетенций студента.

Мультимедийные технологии: ознакомительные материалы (в т.ч. лекции), инструктажи студентов во время практики проводятся в помещениях, оборудованных экраном, видеопроектором, персональными компьютерами. Это позволяет экономить время, затрачиваемое на изложение необходимого материала и увеличить его объем.

Компьютерные технологии и программные продукты: применяются для сбора и систематизации информации, разработки планов, проведения требуемых программой преддипломной практики.

Использование сети Интернет (Интернет-технологий): способствует индивидуализации учебного процесса и обращению к принципиально новым познавательным средствам.

В качестве обеспечения преддипломной практики выступают:

- учебно-методические комплексы по дисциплинам курсов обучения;
- организационно-распорядительная и справочная документация места проведения практики (по согласованию с организацией проведения практики);
- кафедральная документация, методические пособия, учебники, отчеты по НИР, публикации научно-технических конференций и т.д.

Ко времени окончания практики представляется отчет о практике, подписанный руководителем практики. По итогам аттестации практики выставляется зачет с оценкой.

13. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

Информационно – библиотечное обеспечение – представлено в рабочих программах учебных курсов в разрезе каждой дисциплины учебной программы, а также в карте обеспеченности литературой учебной дисциплины. Конкретный список рекомендованной литературы определяется руководителем практики индивидуально для каждого обучаемого в зависимости от индивидуального задания практики.

а) Основная литература:

1. Тельный, А.В. Технические средства охраны : практикум для вузов / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова — Владимир:2012 —139с. ISBN 978-5-9984-00300-2

2. Тельный, А.В.. Инженерно-техническая защита информации. Системы охранного телевидения : учебное пособие / А. В. Тельный ; Владимирский государственный университет (ВлГУ) ; под ред. М. Ю. Монахова .— Владимир 2013 .— 143 с.

3. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-01378-6,

4. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.

5. Региональная и национальная безопасность: Учебное пособие / А.Б. Логунов. - 3-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ ИНФРА-М, 2014. - 457 с.: ISBN 978-5-9558-0310-4,

6. Кнауб, Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2012. - 160 с.

7. Каратунова, Н. Г. Защита информации. Курс лекций : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с.

8. "Вычислительные системы, сети и телекоммуникации: учебник / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко; под ред. А.П. Пятибратова. - 4-е изд., перераб. и доп. - М. : Финансы и статистика, 2014." - http://www.studentlibrary.ru/book/ISBN9785279032853.html 736 с.

9. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ISBN 978-5-8199-0331-5,

б) Дополнительная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2, /

2. Соколов, А.И. Технические средства защиты информации : технические каналы утечки информации : учебное пособие / А. И. Соколов, М. Ю. Монахов ; ВлГУ .— Владимир:, 2007 .— 71 с.

3. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. ISBN 978-5-369-01450-9.

4. Бугаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бугаков, А. В. Тельный ; Владимирский государственный университет (ВлГУ) .— Владимир : 2007 .— 147 с. :

5. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.:

6. Файман, О.И. Правовое обеспечение информационной безопасности : учебное пособие / О. И. Файман, В. А. Граник, М. Ю. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2010 .— 86 с. ISBN 978-5-9984-0020-9

7. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857

8. Кнауб, Л. В. Теоретико-численные методы в криптографии : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - http://www.studentlibrary.ru/book/ISBN5980030026.html 256 с. ISBN 5-98003-002-6.

9. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М. : СОЛОН-ПРЕСС, 2009. http://www.studentlibrary.ru/book/ISBN5980030115.html 272 с.

10. Воронин А.А. Вычислительные сети : учебное пособие / А. А. Воронин ; Владимирский государственный университет (ВлГУ) .— Владимир : 2011 .— 87 с. ISBN 978-5-9984-0179-A

11. Основы информационных и телекоммуникационных технологий. Сетевые информационные технологии : учеб. пособие / В.Б. Попов. - М. : Финансы и статистика, 2015. - http://www.studentlibrary.ru/book/ISBN5279030139.html 224 с.

12. Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие / С.В. Никифоров.- 2-е изд. - М. : Финансы и статистика, 2007. - http://www.studentlibrary.ru/book/ISBN9785279032808.html 224 с.

в) Периодические издания

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;

2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.

3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.

г) Программное обеспечение и Интернет-ресурсы:

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru

2. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

14. Материально-техническое обеспечение преддипломной практики

При прохождении преддипломной практики на кафедре ИЗИ ВлГУ имеется следующая материально-техническая база:

- Лекционная аудитория 408-2 на 40 мест. Перечень оборудования: переносной проектор, маркерная доска, переносной ноутбук.

- Компьютерный класс 427а-2 на 12 персональных рабочих мест с доступом в Интернет, переносной проектор, маркерная и интерактивная доски, переносной ноутбук.

- Компьютерный класс 427б-2 на 7 персональных рабочих мест с доступом в Интернет, стационарный проектор, маркерная доска, переносной ноутбук.

При кафедре ИЗИ создан учебно-научный центр «Комплексная защита объектов информатизации», который укомплектован необходимым специальным оборудованием: - Генератор сигналов специальной формы Г6-31, -Многофункциональный поисковый прибор ST-031P «Пиранья-Р» - обнаружение и локализация специальных технических средств негласного добывания информации; -Прибор «Улан-2» - проверка проводных коммуникаций на наличие гальванически подключенных к ним цепей устройств съема и передачи информации; - Устройство защиты телефонных переговоров от прослушивания «Прокруст-2000»; -Комплекс «Соната АВ. Модель 1М» - защита помещения от прослушивания по акустическому и вибрационному каналу; -Нелинейный локатор «Родник-2К» - обнаружение включенных и выключенных устройств, содержащих радиоэлектронные нелинейные элементы; -Имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник»; -Анализатор спектра «GoodWill GSP-827» - исследование сигналов в телекоммуникационных диапазонах частот до 2,7 ГГц; -Индикатор поля «SEL SP-75 Black Hunter» -поиск и обнаружение в ближней зоне любых радиопередатчиков и работающих сотовых телефонов всех стандартов; - Программно-аппаратный комплекс проведения акустических и виброакустических измерений «Спрут-мини-А»; - Сканирующий приемник «Icom IC-R1500»; -Устройство блокирования работы систем мобильной связи «Мозаика-3»; -Шумогенератор Гном-3 (средство защиты от ПЭМИН); -Анализатор сетей Wi-Fi Fluke AirCheck с активной антенной; -Цифровой видеорегистратор BestDVR-404L на 4 канала; - Извещатели средств охранной сигнализации.

Все компьютеры кафедры объединены в кафедральную компьютерную сеть и имеет выход в корпоративную сеть ВлГУ и, соответственно, в Интернет. Все рабочие станции оборудованы лицензионным программным обеспечением: MS Windows XP Professional SP3, Ubuntu 10.04, MS Office 2007, OpenOffice, Visual Studio 2008, Eclipse, Oracle VirtualBox, VMware Player, MySQL Server, Apache, AnyLogic, GPSS World.

На кафедре ИЗИ имеется специализированное ПО: - ПО Мобильный криминалист; - ПО радиообъектовой системы охранной сигнализации «Стрелец»; -Программа расчета показателей защищенности конфиденциальной информации «ГРОЗА-К»; - Cisco Packet Tracer 5.3.3.0019; - MathCad 14.0.0.163; MathLAB 6.5; Microsoft Visual Studio. NET; AnyLogic 6.0 Professional. Сетевое оборудование: Коммутаторы 3Com 3C16475BS ME 24 Port, Оборудование для передачи информации ограниченного доступа Cisco WS CE500 24TT; Межсетевые экраны CiscoSystems VPN Edition w/10SSL users; 50FW Users и др.

При прохождении преддипломной практики на сторонних предприятиях (организациях), необходимое лабораторное, экспериментальное и компьютерное оборудование, а также программное обеспечение определяются руководителем практики от кафедры ИЗИ согласно специфике выданного задания для прохождения практики.

15. Практика для обучающихся с ограниченными возможностями здоровья и инвалидов проводится с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность»

Программу преддипломной практики составил доцент кафедры ИЗИ к.т.н. Тельный А.В.
(ФИО, подпись)

Рецензент
(представитель работодателя) ГАОУ ДПО ВО ВИРО, зав. каф. ЦиОИБ, к.т.н. Д.В. Мишин

(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 26.08.2019 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.04.01 «Информационная безопасность»

Протокол № 1 от 26.08.2019 года

Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ

Программа одобрена на 2020/2021 учебный год

Протокол заседания кафедры № 1 от 31.08.20 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)