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
«__» _____ 20__ г.

Программа технологической практики

Специальность
10.05.04 «Информационно-аналитические системы безопасности»

Специализация подготовки
Автоматизация информационно-аналитической деятельности

Квалификация (степень) выпускника
Специалист

г. Владимир 2010

Вид практики - Производственная

Тип практики - Технологическая

1. Цели практики.

Целью практики является закрепление знаний и умений, полученных в процессе теоретического обучения, овладение методикой обеспечения информационной безопасности предприятия (организации), проектирования, внедрения и эксплуатации отдельных задач и подсистем комплексной системы защиты информации предприятия (организации). В процессе практики проводится изучение автоматизированных средств и систем, реализующих технологии защиты информации, обучаемый приобретает навыки исследования и проектирования подсистем обеспечения безопасности информации предприятия (организации).

Целями технологической практики являются:

- приобретение практических навыков работы в качестве специалиста (менеджера) ИБ предприятия (организации);
- приобретение навыков обслуживания средств ЗИ в ЭВМ, сетях ЭВМ и автоматизированных информационных системах;
- приобретение практического опыта разработки компонентов КСЗИ предприятия (организации);
- подготовка и систематизация необходимых материалов для построения комплексной системы защиты информации на предприятии (для выполнения курсовых работ по учебному плану);
- приобретение навыка системного подхода при проектировании КСЗИ и отдельных ее подсистем;
- приобретение навыков исследовательской и аналитической работы в области информационной безопасности.

2. Задачи технологической практики.

В зависимости от тематики задания руководителя практики, задачами технологической 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).
- 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 курсового проекта (работы) по изучаемым дисциплинам и сбор материалов по выполнению выпускной квалификационной работы.

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

• подготовка практических и лабораторных занятий по дисциплине (например, установка и конфигурирование необходимого программного обеспечения и оборудования, проработка задач, решаемых на занятии, сбор необходимых материалов для проведения занятия);

• подготовка учебно-методических материалов (сбор информации, выполнение обзора современных технологий, помощь в написании отдельных разделов);

• разработка прикладного (части прикладного) программного обеспечения, в том числе разработка сайтов (части сайта) и т.д.

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

4. Формы проведения технологической практики.

Технологическая практика проводится как непрерывно с выделением в учебном графике периода времени по окончании шестого семестра обучения, так и непрерывно от обучения в шестом семестре. Форма проведения является заводской или лабораторной. При прохождении практики на выпускающей кафедре и в научных лабораториях ВлГУ, руководство организационными аспектами технологической практики осуществляет преподаватель выпускающей кафедры информатики и защиты информации, назначаемый заведующим кафедрой ИЗИ. При прохождении практики на предприятиях и организациях, руководство организационными аспектами технологической практики осуществляет как преподаватель выпускающей кафедры, так и должностное лицо, назначаемое руководителем организации, принимающей студентов на практику (руководитель от предприятия).

В случае прохождения технологической 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 осуществляет руководство содержательными аспектами практики, предоставляет студенту информацию по заданию на практику и осуществляет текущий контроль работы студента. Обучаемые 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. Тема задания технологической практики предлагается студентом по согласованию с научным руководителем соответствующего направления. Научным руководителем технологической практики может быть только преподаватель выпускающей кафедры.

Кроме индивидуального задания и в зависимости от тематики задания руководителя практики, при прохождении технологической практики студент должен:

Изучить:

- организацию и управление деятельностью по защите информации в организации;
- вопросы производимой, разрабатываемой или используемой техники, формы и методы сбыта продукции или предоставления услуг;
- действующие стандарты, технические условия, должностные обязанности, положения и инструкции по обеспечению информационной безопасности в организации, используемое оборудование по обеспечению защиты информации, в том числе периферийное и связное оборудование, программы испытаний технических средств, правила оформления технической документации;
- правила эксплуатации ТСЗИ и средств ВТ, исследовательских установок, измерительных приборов или технологического оборудования по ЗИ, имеющихся в подразделении, а также их обслуживание;
- вопросы обеспечения безопасности жизнедеятельности и экологии.

Освоить:

- методы анализа технического уровня обеспечения ИБ организации, аппаратного и программного обеспечения средств ЗИ для определения их соответствия действующим техническим условиям и стандартам;
- методики применения ТСЗИ, измерительной техники для контроля и изучения эффективности использования ТСЗИ и методики эксплуатации ТСЗИ;
- отдельные пакеты программных средств компьютерного обеспечения ЗИ объектов профессиональной деятельности;
- порядок пользования периодическими, реферативными и справочно-информационными изданиями по профилю направления подготовки.

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

В результате прохождения 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 НИР
ОК-7	способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	**знать:** - лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке. **уметь:** - читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи. **владеть:** - иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке, навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.
ОК-8	способность к самоорганизации и самообразованию	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.
ОПК-3	способность применять в профессиональной деятельности современные средства вычислительной техники и программное обеспечение, достижения информационных технологий для поиска и обработки информации по профилю профессиональной деятельности	**знать:** - формы и способы представления данных в персональном компьютере; состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; классификацию современных компьютерных систем; язык программирования высокого уровня (объектно-ориентированное программирование); основные сведения о базовых структурах данных; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. **уметь:** - применять персональные компьютеры для обработки различных видов информации; работать с интегрированной средой разработки программного обеспечения; реализовывать на языке программирования высокого уровня алгоритмы решения профессиональных задач, использовать известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. **владеть:** - навыками решения типовых математических задач численными методами с использованием средств вычислительной техники; навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных задач; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками анализа программных реализаций.
ОПК-4	способность применять в профессиональной деятельности языки и системы программирования, инструментальные средства разработки программного обеспечения, современные методы и технологии программирования	**знать:** - классификацию современных компьютерных систем; - типовые структуры и принципы организации компьютерных сетей; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; - основные стандарты в области инфокоммуникационных систем и технологий; основные модели данных и модели представления знаний и программные средства работы с ними; **уметь:** - пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; использовать модели данных и знаний для решения стандартных задач автоматизации; решать задачи построения и эксплуатации распределенных автоматизированных

		систем обработки данных; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно-аналитической деятельности; устанавливать корреспондентские отношения с источниками информации, включая взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях. **владеть:** - навыками поиска и обмена информацией в глобальной информационной сети Интернет; навыками безопасного использования технических средств в профессиональной деятельности; профессиональной терминологией в области информационной безопасности; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками формализации знаний предметного эксперта с использованием моделей представления знаний; - навыками работы с инструментальными средствами построения систем представления знаний;
ОПК-5	способностью использовать нормативные правовые акты в своей профессиональной деятельности	**знать:** основы права и законодательства России, основы конституционного строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации; основные стандарты в области инфокоммуникационных систем и технологий; основные положения гражданского, гражданско- процессуального, административного, уголовного, уголовно- процессуального и финансового законодательства. **уметь:** использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; использовать результаты научно-исследовательских работ в решении задач практики, готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем, - 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, разработки и оценки защищенности компьютерных систем; осуществлять правовую оценку информации, используемой в профессиональной деятельности. **владеть:** навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; профессиональной терминологией в области информационной безопасности; основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно-процессуальном и финансовом законодательстве.
ОПК-7	способностью применять методы и средства обеспечения информационной безопасности специальных ИАС	**знать:** - источники и классификацию угроз информационной безопасности; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений;

		основные отечественные и зарубежные стандарты в области компьютерной безопасности; сущность и понятие информации, информационной безопасности и характеристику ее составляющих; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные стандарты в области инфокоммуникационных систем и технологий; основные методы организационного обеспечения информационной безопасности специальных АИС; методологические основы, методы и средства моделирования предметной области специальных АИС; методологические основы, методы и средства моделирования специальных АИС; методологические основы, методы и средства построения распределенных специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; методологические основы информационно- аналитической деятельности; задачи, методы и средства; основные принципы организации информационно- аналитической деятельности; **уметь:** - применять средства антивирусной защиты и обнаружения вторжений; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; пользоваться средствами защиты, предоставляемыми системами управления базами данных; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; формализовать предметную область с целью создания баз данных и экспертных систем; использовать модели данных и знаний для решения стандартных задач автоматизации; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно-аналитической деятельности; формализовывать предметную область с целью создания специальных АИС; разрабатывать технические задания на разработку специальных АИС; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; пользоваться средствами защиты, предоставляемыми системами управления базами данных; **владеть:** - навыками разработки алгоритмов решения типовых профессиональных задач; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных, навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; - методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками разработки концептуальной модели предметной области; навыками формализации знаний предметного эксперта с использованием моделей

		представления знаний; навыками работы с инструментальными средствами построения систем представления знаний; навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов; навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС; навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС; навыками выбора и обоснования критериев эффективности функционирования специальных АИС
ПК-1	способность анализировать и формализовывать поставленные задачи, выдвигать гипотезы, устанавливать границы их применения и подтверждать или опровергать их на практике	**знать:** основные понятия, задачи и методы вычислительной математики; постановки типовых математических задач, численные методы и алгоритмы их решения; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; основные принципы организации информационно- аналитической деятельности; - основные понятия и методы теории вероятностей, математической статистики, теории случайных процессов; основные понятия и методы дискретной математики; задачи и методы вычислительной математики; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности; **уметь:** - применять персональные компьютеры для обработки различных видов информации; строить математические модели физических явлений и процессов; применять современные численные методы решения типовых математических задач (нелинейные уравнения, среднеквадратичное приближение и асимптотические методы); формализовать предметную область с целью создания баз данных и экспертных систем; использовать модели данных и знаний для решения стандартных задач автоматизации; применять общенаучные методики, использовать результаты научно-исследовательских работ в решении задач практики; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; - применять стандартные методы и модели к решению типовых теоретико- вероятностных и статистических задач; пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; строить математические модели физических явлений и процессов; применять современные численные методы решения типовых математических задач (нелинейные уравнения, среднеквадратичное приближение и асимптотические методы); использовать известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; **владеть:** - навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; методами проведения научных исследований, постановки и решения специальных задач по профилю будущей

		деятельности; навыками решения типовых математических задач численными методами с использованием средств вычислительной техники; навыками разработки алгоритмов решения типовых профессиональных задач; навыками разработки концептуальной модели предметной области; навыками формализации знаний предметного эксперта с использованием моделей представления знаний; - навыками описания базы знаний средствами логических исчислений; навыками работы с инструментальными средствами построения систем представления знаний.
ПК-2	способность применять методы анализа массивов данных и интерпретировать профессиональный смысл получаемых формальных результатов	**знать:** - методологические основы математического программирования, классификацию и основные подходы к решению оптимизационных задач; конкретные методы решения оптимизационных задач различных классов, с учетом особенностей компьютерной реализации алгоритмов и анализа алгоритмической сложности; средства и методы хранения и передачи информации; основные сведения о базовых структурах данных; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности; основные модели данных и модели представления знаний и программные средства работы с ними; области применения экспертных систем и этапы их проектирования; методологические основы: - основные понятия и методы теории вероятностей, математической статистики, теории случайных процессов; основные понятия и методы дискретной математики; основные понятия, задачи и методы вычислительной математики; постановки типовых математических задач, численные методы и алгоритмы их решения; основные модели данных и модели представления знаний и программные средства работы с ними; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации; способы формирования описаний объектов и классов объектов предметной области. **уметь:** - использовать модели данных и знаний для решения стандартных задач автоматизации; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно- аналитической деятельности; пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; применять персональные компьютеры для обработки различных видов информации; решать основные типы оптимизационных задач, включая задачи линейного программирования; - применять стандартные методы и модели к решению типовых теоретико- вероятностных и статистических задач; - строить математические модели физических явлений и процессов; применять современные численные методы решения типовых математических задач (нелинейные уравнения, среднеквадратичное приближение и асимптотические методы); решать основные задачи векторной алгебры и аналитической геометрии; применять стандартные методы дискретной математики для решения профессиональных задач; анализировать и применять физические явления и эффекты для решения практических задач обеспечения

		информационной безопасности; использовать результаты научно-исследовательских работ в решении задач практики. **владеть:** - навыками пользования библиотеками прикладных программ и пакетами программ для решения прикладных математических задач; навыками решения оптимизационных задач с использованием средств вычислительной техники; навыками постановки и решения задач оптимизации при различного рода ограничениях на целевую функцию и ее параметры; навыками решения задач оптимизации с использованием средств вычислительной техники; - навыками описания базы знаний средствами логических исчислений; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками решения задач линейной алгебры и аналитической геометрии; методами теоретического исследования физических явлений и процессов; методами проведения научных исследований, постановки и решения специальных задач по профилю будущей деятельности; навыками решения типовых математических задач численными методами с использованием средств вычислительной техники; навыками разработки алгоритмов решения типовых профессиональных задач.
ПК-3	способность осуществлять сбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности	**знать:** - основные понятия и принципы делопроизводства и электронного документооборота; принципы функционирования автоматизированных систем поддержки документооборота и их безопасность; средства и методы хранения и передачи информации; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; основные принципы организации информационно- аналитической деятельности; способы формирования описаний объектов и классов объектов предметной области. **уметь:** - разрабатывать технические задания на разработку специальных АИС; пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности. **владеть:** - профессиональной терминологией в области информационной безопасности; основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно- процессуальном и финансовом законодательстве; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками поиска и обмена информацией в глобальной информационной сети Интернет.
ПК-4	способность применять современные методы научных исследований с использованием	**знать:** формы и способы представления данных в персональном компьютере; классификацию современных компьютерных систем; конкретные методы

	компьютерных технологий, в том числе в работе над междисциплинарными проектами	решения оптимизационных задач различных классов, с учетом особенностей компьютерной реализации алгоритмов и анализа алгоритмической сложности; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; методы планирования и оптимизации компьютерных экспериментов с моделями специальных АИС. **уметь:** - пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач; применять персональные компьютеры для обработки различных видов информации; строить математические модели физических явлений и процессов, использовать известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; проектировать и сопровождать типовые специальные АИС, локальные сети. **владеть:** - навыками пользования библиотеками прикладных программ и пакетами программ для решения прикладных математических задач; навыками решения оптимизационных задач с использованием средств вычислительной техники; навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов); навыками поиска и обмена информацией в глобальной информационной сети Интернет; навыками решения задач оптимизации с использованием средств вычислительной техники; навыками решения типовых математических задач численными методами с использованием средств вычислительной техники; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств, навыками настройки межсетевых экранов; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений; навыками анализа программных реализаций; методами и средствами выявления угроз безопасности компьютерным системам; методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах; основами маршрутизации и управления потоками в сетях передачи информации.
ПК-5	способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности	**знать:** - методологические основы математического программирования, классификацию и основные подходы к решению оптимизационных задач; конкретные методы решения оптимизационных задач различных классов, с учетом особенностей компьютерной реализации алгоритмов и анализа алгоритмической сложности; основные понятия, задачи и методы вычислительной математики; постановки типовых математических задач, численные методы и алгоритмы их решения; методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации.

		уметь: - применять персональные компьютеры для обработки различных видов информации; строить математические модели физических явлений и процессов; анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; решать основные типы оптимизационных задач, включая задачи линейного программирования; применять современные численные методы решения типовых математических задач (нелинейные уравнения, среднеквадратичное приближение и асимптотические методы); использовать результаты научно-исследовательских работ в решении задач практики. **владеть:** - навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками решения оптимизационных задач с использованием средств вычислительной техники; навыками постановки и решения задач оптимизации при различного рода ограничениях на целевую функцию и ее параметры; навыками решения задач оптимизации с использованием средств вычислительной техники; навыками решения типовых математических задач численными методами с использованием средств вычислительной техники; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов; навыками выбора и обоснования критериев эффективности функционирования специальных АИС.
ПК-6	способность готовить научно-технические отчеты, обзоры, публикации, доклады по результатам выполненных исследований	**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; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; методологические основы информационно-аналитической деятельности: задачи, методы и средства; основные принципы организации информационно-аналитической деятельности. **уметь:** - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; 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, разработки и оценки защищенности компьютерных систем; использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности. **владеть:** - профессиональной терминологией в области информационной безопасности; навыками разработки, документирования, тестирования и отладки программ;

		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.
ПК-7	способность проводить предпроектное обследование профессиональной деятельности и информационных потребностей автоматизируемых подразделений	**знать:** основные стандарты в области инфокоммуникационных систем и технологий: методологические основы, методы и средства моделирования специальных АИС; методологические основы, методы и средства построения распределенных специальных АИС; системы распределенной обработки данных, используемые в специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; методы проектирования АИС; - средства и методы хранения и передачи информации; основные стандарты в области инфокоммуникационных систем и технологий; основные модели данных и модели представления знаний и программные средства работы с ними; **уметь:** решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно-аналитической деятельности; разрабатывать технические задания на разработку специальных АИС; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС; - применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС; **владеть:** методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС; навыками выбора и обоснования критериев эффективности функционирования специальных АИС; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации; навыками проектирования и сопровождения специальных АИС; - навыками разработки алгоритмов решения типовых профессиональных задач; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС.
ПК-8	способность разрабатывать и исследовать модели технологических процессов обработки информации в специальных ИАС	**знать:** - источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; основные модели данных и модели представления знаний и программные средства

		работы с ними; логико-лингвистические основы обработки данных и знаний в специальных АИС; методологические основы, методы и средства моделирования предметной области специальных АИС; методологические основы, методы и средства моделирования специальных АИС; методы построения и исследования математических моделей специальных АИС; методы планирования и оптимизации компьютерных экспериментов с моделями специальных АИС; методологические основы, методы и средства построения распределенных специальных АИС; системы распределенной обработки данных, используемые в специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; назначение и классификацию информационных и аналитических систем, систем управления; структуру функциональной и обеспечивающих частей специальных АИС; методы проектирования АИС; принципы эксплуатации и сопровождения АИС; 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, роль и место информационно- аналитической деятельности в системах организационного управления; методологические основы информационно-аналитической деятельности: задачи, методы и средства; основные принципы организации информационно-аналитической деятельности. **уметь:** - использовать модели данных и знаний для решения стандартных задач автоматизации; решать задачи исследования специальных АИС методами моделирования; применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно-аналитической деятельности; проектировать и сопровождать типовые специальные АИС, локальные сети; устанавливать корреспондентские отношения с источниками информации, включая взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях; проводить обследование подразделений в целях определения их информационных потребностей; формализовывать предметную область с целью создания специальных АИС; разрабатывать технические задания на разработку специальных АИС; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач. **владеть:** - профессиональной терминологией в области информационной безопасности; навыками разработки концептуальной модели предметной области; навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов; навыками исследования математических моделей

		технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС; навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС; навыками выбора и обоснования критериев эффективности функционирования специальных АИС; навыками проектирования и сопровождения специальных АИС.
ПК-9	способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	**знать:** - источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; механизмы реализации атак в компьютерных сетях; - защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений; основные отечественные и зарубежные стандарты в области компьютерной безопасности. **уметь:** - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; применять средства антивирусной защиты и обнаружения вторжений; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; пользоваться средствами защиты, предоставляемыми системами управления базами данных; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; 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, разработки и оценки защищенности компьютерных систем. **владеть:** - навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений; навыками анализа программных реализаций; методами и средствами выявления угроз безопасности компьютерным системам; методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах; основами маршрутизации и управления потоками в сетях передачи информации; простейшими методами криптографического анализа; простейшими методами анализа безопасности криптографических протоколов.
ПК-10	способность осуществлять выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности	**знать:** - эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; методологические основы, методы и средства моделирования специальных АИС; методологические основы, методы и средства построения распределенных

	создаваемых специальных ИАС	специальных АИС; системы распределенной обработки данных, используемые в специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; методы проектирования АИС; **уметь:** - решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно-аналитической деятельности; разрабатывать технические задания на разработку специальных АИС; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС. **владеть:** - методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС; навыками выбора и обоснования критериев эффективности функционирования специальных АИС; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации; навыками проектирования и сопровождения специальных АИС.
ПК-11	способность разрабатывать проектные документы на создаваемые специальные ИАС, в том числе средства обеспечения их информационной безопасности	**знать:** - основные стандарты в области инфокоммуникационных систем и технологий; основные модели данных и модели представления знаний и программные средства работы с ними; методологические основы, методы и средства моделирования предметной области специальных АИС; методологические основы, методы и средства моделирования специальных АИС; методологические основы, методы и средства построения распределенных специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; методы проектирования АИС; принципы эксплуатации и сопровождения АИС. **уметь:** - применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; разрабатывать технические задания на разработку специальных АИС; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС. **владеть:** - навыками разработки алгоритмов решения типовых профессиональных задач; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС; навыками выбора и обоснования критериев эффективности функционирования специальных АИС; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации; навыками

		проектирования и сопровождения специальных АИС.
ПК-12	способность разрабатывать программное и иные виды обеспечения специальных ИАС	**знать:** - определение, свойства аксиоматических систем и приёмы работы с ними; определение и классы машин Тьюринга и их роль в теории алгоритмов; основные классы формальных грамматик и автоматов, способы задания формальных языков; средства и методы хранения и передачи информации; принципы построения и основные виды симметричных и асимметричных криптографических алгоритмов; базовые криптографические протоколы и основные требования к ним; общие принципы построения и использования современных языков и программирования высокого уровня; язык программирования высокого уровня (объектно-ориентированное программирование); основные сведения о базовых структурах данных; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; основные модели данных и модели представления знаний и программные средства работы с ними; логико-лингвистические основы обработки данных и знаний в специальных АИС; принципы проектирования реляционных баз данных. **уметь:** - формулировать задачи логического характера в рамках исчисления высказываний и исчисления предикатов; описывать базы знаний средствами логических исчислений; формулировать и решать задачи, пользуясь соответствующими классами машин Тьюринга; строить формальные грамматики для простых формальных языков; работать с интегрированной средой разработки программного обеспечения; реализовывать на языке программирования высокого уровня алгоритмы решения профессиональных задач; использовать известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; использовать модели данных и знаний для решения стандартных задач автоматизации; - проектировать простые базы данных и экспертные системы и реализовывать их с использованием стандартных систем управления базами данных и инструментальных средств создания экспертных систем; использовать результаты научно-исследовательских работ в решении задач практики; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач. **владеть:** - навыками описания базы знаний средствами логических исчислений; навыками синтаксического анализа формальных языков; навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных задач; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками работы с инструментальными средствами построения систем представления знаний.
ПК-13	способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их	**знать:** - основные стандарты в области инфокоммуникационных систем и технологий; основные модели данных и модели представления знаний и программные средства работы с ними;

	информационной безопасности	методологические основы, методы и средства моделирования предметной области специальных АИС; методологические основы, методы и средства моделирования специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; назначение и классификацию информационных и аналитических систем, систем управления; структуру функциональной и обеспечивающих частей специальных АИС; методы проектирования АИС; принципы эксплуатации и сопровождения АИС; 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. **уметь:** - применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно-аналитической деятельности; готовить проектную документацию на создаваемые специальные АИС; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач. **владеть:** - методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов; навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС; навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС; навыками выбора и обоснования критериев эффективности функционирования специальных АИС; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации.
ПК-14	способность использовать специальные АИС для решения задач в сфере профессиональной деятельности	**знать:** - основные методы организационного обеспечения информационной безопасности специальных АИС; логико-лингвистические основы обработки данных и знаний в специальных АИС; методологические основы, методы и средства моделирования предметной области специальных АИС; методологические основы, методы и средства моделирования специальных АИС; методы построения и исследования математических моделей специальных АИС; методы планирования и оптимизации компьютерных экспериментов с моделями специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; назначение и классификацию информационных и аналитических систем, систем управления; структуру функциональной и обеспечивающих частей специальных АИС; методы проектирования АИС; принципы эксплуатации и сопровождения АИС; методологические основы теории

		принятия решений, теории измерений, теории прогнозирования и планирования; роль и место информационно- аналитической деятельности в системах организационного управления, методологические основы информационно-аналитической деятельности: задачи, методы и средства; основные принципы организации информационно-аналитической деятельности. **уметь:** - использовать модели данных и знаний для решения стандартных задач автоматизации; проектировать простые базы данных и экспертные системы и реализовывать их с использованием стандартных систем управления базами данных и инструментальных средств создания экспертных систем; решать задачи исследования специальных АИС методами моделирования; применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно- аналитической деятельности; устанавливать корреспондентские отношения с источниками информации, включая взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях; использовать результаты научно-исследовательских работ в решении задач практики; проводить обследование подразделений в целях определения их информационных потребностей; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач. **владеть:** - навыками разработки алгоритмов решения типовых профессиональных задач; навыками разработки концептуальной модели предметной области; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками работы с инструментальными средствами построения систем представления знаний; навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов; навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС; навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС.
ПК-15	способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях	**знать:** - основные стандарты в области инфокоммуникационных систем и технологий; принципы построения защищенных телекоммуникационных систем; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; основные модели данных и модели представления знаний и программные средства работы с ними; логико-лингвистические основы обработки данных и знаний в специальных АИС; методологические основы, методы и средства моделирования предметной области специальных АИС; методы планирования и

		оптимизации компьютерных экспериментов с моделями специальных АИС; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; структуру функциональной и обеспечивающих частей специальных АИС; методы проектирования АИС; принципы эксплуатации и сопровождения АИС; основные принципы организации информационно- аналитической деятельности; способы формирования описаний объектов и классов объектов предметной области. **уметь:** - работать с интегрированной средой разработки программного обеспечения; реализовывать на языке программирования высокого уровня алгоритмы решения профессиональных задач; использовать известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; решать задачи исследования специальных АИС методами моделирования; применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; проектировать и сопровождать типовые специальные АИС, локальные сети; устанавливать корреспондентские отношения с источниками информации, включая взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; пользоваться средствами защиты, предоставляемыми системами управления базами данных. **владеть:** - навыками разработки алгоритмов решения типовых профессиональных задач; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками работы с инструментальными средствами построения систем представления знаний; навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС; навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС; навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений; навыками анализа программных реализаций; методами и средствами выявления угроз безопасности компьютерным системам; методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах.
ПК-16	способность разрабатывать	**знать:** - источники и классификацию угроз

	проекты нормативных, методических, организационно-распорядительных документов, регламентирующих функционирование специальных ИАС и средств обеспечения их информационной безопасности	информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; 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; основные методы организационного обеспечения информационной безопасности специальных АИС; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; области применения экспертных систем и этапы их проектирования; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; методы проектирования АИС; принципы эксплуатации и сопровождения АИС; основные положения гражданского, гражданско-процессуального, административного, уголовного, уголовно- процессуального и финансового законодательства. **уметь:** - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; проектировать и сопровождать типовые специальные АИС, локальные сети; устанавливать корреспондентские отношения с источниками информации, включая взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; - 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, разработки и оценки защищенности компьютерных систем. **владеть:** - профессиональной терминологией в области информационной безопасности; методами и средствами разработки прикладных систем поддержки баз данных и знаний; навыками применения стандартного программного обеспечения для решения прикладных задач с использованием баз данных; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации; навыками проектирования и сопровождения специальных АИС; основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно- процессуальном и финансовом законодательстве.
ПК-17	способность организовывать работу малых коллективов исполнителей, принимать и реализовывать управленческие	знать: - методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности); научные основы, цели, принципы, методы и технологии управленческой

	решения в сфере профессиональной деятельности	деятельности; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; роль и место информационно-аналитической деятельности в системах организационного управления; методологические основы информационно-аналитической деятельности; задачи, методы и средства; основные принципы организации информационно-аналитической деятельности; основные положения гражданского, гражданско-процессуального, административного, уголовного, уголовно-процессуального и финансового законодательств. **уметь:** - использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности; - работать в коллективе, принимать управленческие решения и оценивать их эффективность; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; применять общенаучные методики, характерные для теории распределенных систем, к решению конкретных задач информационно-аналитической деятельности; использовать результаты научно-исследовательских работ в решении задач практики; проводить обследование подразделений в целях определения их информационных потребностей; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. **владеть:** - навыками письменного аргументированного изложения собственной точки зрения; навыками публичной речи, аргументации, ведения дискуссии и полемики; профессиональной терминологией в области информационной безопасности; навыками разработки алгоритмов решения типовых профессиональных задач; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации; навыками проектирования и сопровождения специальных АИС; основной юридической терминологией, используемой в гражданском, гражданско-процессуальном, административном, уголовном, уголовно-процессуальном и финансовом законодательстве;
ПК-18	способность выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные	**знать:** - источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; средства и методы хранения и передачи информации; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений; основные отечественные и зарубежные стандарты в области компьютерной безопасности; основные методы организационного обеспечения информационной безопасности специальных АИС; требования, методы и средства информационной безопасности в технологиях платежных систем.

		уметь: - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; применять средства антивирусной защиты и обнаружения вторжений; готовить проекты нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; пользоваться средствами защиты, предоставляемыми системами управления базами данных; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; 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, разработки и оценки защищенности компьютерных систем. **владеть:** - профессиональной терминологией в области информационной безопасности; навыками разработки алгоритмов решения типовых профессиональных задач; навыками проектирования и сопровождения специальных АИС; навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений; методами и средствами выявления угроз безопасности компьютерным системам; методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах; - простейшими методами криптографического анализа; простейшими методами анализа безопасности криптографических протоколов.
ПК-19	способность обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей	**знать:** - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; - принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; - средства и методы предотвращения и обнаружения вторжений; основные отечественные и зарубежные стандарты в области компьютерной безопасности; основные методы организационного обеспечения информационной безопасности специальных АИС; нормативную базу,

		регламентирующую создание и эксплуатацию специальных АИС; назначение и классификацию информационных и аналитических систем, систем управления; методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования; методологические основы информационно- аналитической деятельности: задачи, методы и средства, основные принципы организации информационно- аналитической деятельности; основные положения гражданского, гражданско- процессуального, административного, уголовного, уголовно-процессуального и финансового законодательства; требования, методы и средства информационной безопасности в технологиях платежных систем. **уметь:** - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации, проектировать и сопровождать типовые специальные АИС, локальные сети; устанавливать корреспондентские отношения с источниками информации, включая взаимодействие с вычислительными системами и базами данных в телекоммуникационном режиме и работу в глобальных компьютерных сетях; проводить обследование подразделений в целях определения их информационных потребностей; разрабатывать технические задания на разработку специальных АИС; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; 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, разработки и оценки защищенности компьютерных систем; осуществлять правовую оценку информации, используемой в профессиональной деятельности. **владеть:** - профессиональной терминологией в области информационной безопасности; навыками разработки, документирования, тестирования и отладки программ; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации; навыками проектирования и сопровождения специальных АИС; основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно-процессуальном и финансовом законодательстве.
ПК-20	способность анализировать правоотношения, являющиеся объектами профессиональной деятельности, юридически правильно квалифицировать факты, события и обстоятельства	**знать:** - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные понятия и принципы делопроизводства и электронного документооборота; основные стандарты в области инфокоммуникационных систем и технологий; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой

		безопасности; средства и методы предотвращения и обнаружения вторжений; основные отечественные и зарубежные стандарты в области компьютерной безопасности; нормативную базу, регламентирующую создание и эксплуатацию специальных АИС; основные принципы организации информационно- аналитической деятельности; основные положения гражданского, гражданско- процессуального, административного, уголовного, уголовно- процессуального и финансового законодательства; требования, методы и средства информационной безопасности в технологиях платежных систем. **уметь:** - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; готовить проекты нормативно- распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации специальных АИС; готовить проектную документацию на создаваемые специальные АИС; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; - 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, разработки и оценки защищенности компьютерных систем; осуществлять правовую оценку информации, используемой в профессиональной деятельности. **владеть:** - навыками разработки, документирования, тестирования и отладки программ; навыками проведения предпроектного обследования и постановки новых задач автоматизации и информатизации; навыками проектирования и сопровождения специальных АИС; основной юридической терминологией, используемой в гражданском, гражданско- процессуальном, административном, уголовном, уголовно-процессуальном и финансовом законодательстве; основными методами научного познания; навыками публичной речи, аргументации, ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности
ПСК-1.1	способность разрабатывать, анализировать и применять формализованные модели и методы решения аналитических задач	**знать:** понятие и классификацию информационных языков АИС, свойства информационных языков различных классов; основные свойства естественного языка как знаковой системы; структуру естественно-языкового текста как объекта компьютерной обработки; ограничения, накладываемые свойствами русского естественно языкового текста на процедуры обработки; основные типы задач по обработке текстов и основные виды автоматизированных систем, решающих эти задачи; прикладные методы, модели и алгоритмы, применяемые в системах компьютерной обработки естественно-языковых текстов; теоретические основы построения и использования информационно-поисковых тезаурусов; - классификацию, методы, алгоритмы морфологического анализа; основные классы формальных грамматик и автоматов, способы задания формальных языков; **уметь:** ставить и решать практические задачи анализа

		данных в условиях различной полноты исходной информации; проводить комплексный анализ данных с использованием базовых параметрических и непараметрических моделей; проводить оценку качества и осуществлять выбор автоматизированной технологии семантической обработки текстов в конкретных условиях решения прикладных информационно-аналитических задач; применять современные автоматизированные технологии семантической обработки текстов при решении прикладных информационно- аналитических задач; использовать современные средства автоматизации при подготовке выходных аналитических документов; - описывать базы знаний средствами логических исчислений; строить формальные грамматики для простых формальных языков; **владеть:** навыками решения формализованных математических задач анализа данных с помощью пакетов прикладных программ; навыками работы с программными системами, реализующими автоматизированные технологии семантической обработки текстов; навыками самостоятельного освоения, оценки и внедрения автоматизированных технологий семантической обработки текстов; навыками использования информационных языков для задания информационных запросов; - навыками синтеза гуманитарного и технического знания при решении конкретных проблем автоматизации обработки текстов; - навыками описания базы знаний средствами логических исчислений; навыками синтаксического анализа формальных языков.
ПСК-1.2	способность разрабатывать и применять автоматизированные технологии обработки естественно-языковых текстов и формализованных данных при решении информационно-аналитических задач	**знать:** - понятие и классификацию информационных языков АИС, свойства информационных языков различных классов; основные свойства естественного языка как знаковой системы; структуру естественно-языкового текста как объекта компьютерной обработки, ограничения, накладываемые свойствами русского естественно языкового текста на процедуры обработки; классификацию, методы, алгоритмы морфологического анализа; основные типы задач по обработке текстов и основные виды автоматизированных систем, решающих эти задачи; прикладные методы, модели и алгоритмы, применяемые в системах компьютерной обработки естественно-языковых текстов. **уметь:** - проводить оценку качества и осуществлять выбор автоматизированной технологии семантической обработки текстов в конкретных условиях решения прикладных информационно- аналитических задач; применять современные автоматизированные технологии семантической обработки текстов при решении прикладных информационно- аналитических задач; использовать современные средства автоматизации при подготовке выходных аналитических документов; определять тип информационного языка по его описанию, структуре, словарному составу. **владеть:** - навыками работы с программными системами, реализующими автоматизированные технологии семантической обработки текстов; навыками самостоятельного освоения, оценки и внедрения автоматизированных технологий семантической обработки текстов; методами поиска, выбора и обработки массивов документов по конкретным направлениям служебной деятельности; навыками синтеза гуманитарного и технического знания при

		решении конкретных проблем автоматизации обработки текстов; навыками использования информационных языков для задания информационных запросов.
ПСК-1.3	способность решать задачи анализа данных больших объемов	**знать:** - методологические основы анализа данных: методы статистического анализа случайных последовательностей; методы снижения размерности многомерных данных; методы распознавания объектов; понятие и классификацию знаковых систем; понятие и классификацию информационных языков АИС, свойства информационных языков различных классов; основные свойства естественного языка как знаковой системы; структуру естественно-языкового текста как объекта компьютерной обработки; ограничения, накладываемые свойствами русского естественно языкового текста на процедуры обработки; основные типы задач по обработке текстов и основные виды автоматизированных систем, решающих эти задачи. **уметь:** - ставить и решать практические задачи анализа данных в условиях различной полноты исходной информации; проводить комплексный анализ данных с использованием базовых параметрических и непараметрических моделей, проводить оценку качества и осуществлять выбор автоматизированной технологии семантической обработки текстов в конкретных условиях решения прикладных информационно-аналитических задач; применять современные автоматизированные технологии семантической обработки текстов при решении прикладных информационно- аналитических задач. **владеть:** - навыками решения формализованных математических задач анализа данных с помошью пакетов прикладных программ; навыками работы с программными системами, реализующими автоматизированные технологии семантической обработки текстов; навыками синтеза гуманитарного и технического знания при решении конкретных проблем автоматизации обработки текстов.

6. Место технологической практики в структуре ОПОП специалитета

Практика специалистов относится к циклу «Учебная и производственная практики, научно-исследовательская работа». Настоящая программа практики основывается на требованиях, определённых Федеральным государственным образовательным стандартом высшего образования по специальности 10.05.04 «Информационно-аналитические системы безопасности».

Технологическая практика базируется на основе изучения следующих **(или аналогичных)** дисциплин:

Базовая часть

- Математика
- Информатика
- Физика
- Статистические методы в информационной безопасности
- Основы информационной безопасности
- Программно-аппаратные средства защиты информации
- Криптографические методы защиты информации
- Техническая защита информации
- Безопасность информационных и аналитических систем
- Безопасность операционных систем
- Базы данных и экспертные системы

- Технологии и методы программирования
- Языки программирования
- Система защиты информации на предприятии
- Принципы построения, проектирования и эксплуатации информационно-аналитических систем
- Экономика

Вариативная часть

- Теория информации
- Физические процессы в информационной безопасности
- Аппаратные средства вычислительной техники
- Организационное и правовое обеспечение информационной безопасности
- Сети и системы передачи информации
- Структуры данных
- Информационные технологии
- Алгоритмы на графах и сетях
- Методы формализации и моделирования объектов информатизации
- Системное программное обеспечение
- Теория автоматов и формальных языков
- Электроника и схемотехника
- Политики информационной безопасности в корпоративных ИС

Практика проводится на 3 курсе, по окончании и во время 6 семестра обучения.

Требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки студентов специальности 10.05.04 «Информационно-аналитические системы безопасности» по курсам «Математика», «Информатика», «Технологии и методы программирования», «Структуры данных», «Сети и системы передачи информации», «Методы формализации и моделирования объектов информатизации» и др.

Технологическая практика необходима для успешного изучения таких дисциплин как «Техническая защита информации», «Организационное и правовое обеспечение информационной безопасности», «Криптографические методы защиты информации», «Система защиты информации на предприятии», «Корпоративные информационные систем» и т.д.

7. Место и время проведения технологической практики.

Технологическая практика проводится в два этапа во время обучения согласно графику учебного процесса.

1. Технологическая практика во время 6 семестра обучения. Данная практика является распределенной, параллельно с учебным процессом, стационарной и проводится в течение 1 и 1/3 недельи на выпускающей кафедре и в научных лабораториях ВлГУ.

2. Технологическая практика по окончании 6 семестра обучения. Данная практика является стационарной и проводится в течение 2 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, 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 технологической практики составляет:
6 семестр распределенная практика:
__2__ зачетных единицы; __72__ часа.

6 семестр не распределенная практика:
__3__ зачетных единицы; __108__ часов.

9. Структура и содержание технологической практики

№ п/п	Разделы (этапы) практики	Виды технологической работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля
6 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. (10 часов)	Собеседование, консультации
3	Практические работы по теме задания на практику	Проведение практических занятий (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования и т.д.) (58 часов)	Консультации (в том числе и дистанционно)
6 семестр не распределенная практика			
1	Подготовительный	Проведение организационного собрания. Получение задания на практику. Ознакомление с заданием, планирование работы. Проведение инструктажа по ОТ и ТБ на рабочем месте. (8 часов)	Собеседование
2	Подготовка теоретических материалов.	Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических указаний и т.д. (20 часов)	Собеседование, консультации
3	Практические работы по теме задания на практику	Проведение практических работ (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования и т.д.) (68 часов)	Консультации (в том числе и дистанционно)
4	Отчёт по практике	Составление отчёта по практике (12 часов)	Отчет (в том числе и в электронном виде)
5	Зачёт по практике	Подготовка к зачёту. Зачет по практике (8 часов)	Зачет

Примечание: Отчет по распределенной практике в течение 6 семестра и отчет по распределенной практике по окончании 6 семестра делается совместно по одному выданному (уточненному) заданию. Защита отчета проводится после прохождения технологической практике распределенной практике по окончании 6 семестра.

10. Формы отчетности по практике

По итогам аттестации практики выставляется зачет с оценкой.

В состав отчёта по технологической практике должны входить:

• индивидуальное задание на прохождение практики, утверждённое руководителем практики;

• дневник практики для учебной практики не составляется (только для технологической практики);

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

• электронные материалы по практической работе.

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

Все примеры оформления отчетных документов приведены в методических указаниях по проведению технологической практики студентов по специальности 10.05.04 «Информационно-аналитические системы безопасности».

Структура и оформление отчетов о технологической 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. Обязательные структурные элементы выделены полужирным шрифтом. 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.

Титульный лист должен соответствовать форме, приведенной в Приложении. 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 технологической 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 технологической практики проводится в течение первых двух недель начала следующего семестра в форме комиссионной защиты студентом результатов работы по практике. Оценивается отчет студента, выступление на защите практики и отзыв преподавателя, который являлся руководителем практики.

Примерные контрольные вопросы и задания по типовым заданиям на технологическую практику. *(Для конкретного задания студентов на технологическую 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 кар-ты, 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.В001.-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 посяга-тельств 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 рас-положение 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 вариообъективов, 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 поль-зователей;
- наличие внутри предприятия собственного WEB, FTP серверов.

Использование встроенных (приобретенных) средств мони-торинга, 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 ис-пользованием 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 террито-рии 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 плани-рование 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 информа-ции, 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 ин-формация, 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 виброакустическому 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 технологической 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 технологической 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 технологической практики.

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

В качестве обеспечения технологической 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. Баньлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Баньлы, 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. Бутаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бутаков, 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.

9. 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.

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

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

12. 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.

13. 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 технологической практики

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

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств

нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокрест 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

При прохождении технологической 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 специальности 10.05.04 «Информационно-аналитические системы безопасности», специализация «Автоматизация информационно-аналитической деятельности»

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

Рецензент
(представитель работодателя) ГАОУ ДПО ВО ВИРО, зав. каф. ЦЦИБ к.т.н. Д.Р. 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 по специальности 10.05.04 «Информационно-аналитические системы безопасности», специализация «Автоматизация информационно-аналитической деятельности»

Протокол № 1 от 26.08.2019 года

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

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ

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)

Программа одобрена на _____ учебный год

Протокол заседания кафедры № _____ от _____ года

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