Министерство образования и науки 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
(Наименование института, факультета)

УТВЕРЖДАЮ

Проректор по образовательной деятельности
_____ А.А. Панфилов

"29" 12 2016 г.

Программа производственной практики
(Наименование практики)

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль (программа) подготовки
_____

Квалификация (степень) выпускника
Бакалавр

г. Владимир 2016

Вид практики - Производственная

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 производственной 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 производственной практики.

В зависимости от тематики задания руководителя практики, задачами производственной 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 производственной практики бакалавр 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 производственной практики.

Производственная практика проводится в три этапа во время обучения.

1. Производственная практика по окончании 4 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 может быть выездной, если между кафедрой и организацией, принимающей студентов на практику заключен договор о направлении студентов на практику, решены все вопросы финансового обеспечения прохождения практики (в т.ч. расходы на проживание и проезд до места проведения практики). Кроме того, предприятие (организация) должна иметь достаточную материально-техническую базу, соответствующий профиль деятельности и квалифицированных специалистов в области защиты информации.

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

3. Производственная практика по окончании 6 семестра обучения. Данная практика является стационарной и проводится в течение 2 и 2/3 недели в сторонних организациях (учреждениях, предприятиях) и структурных подразделениях по профилю направления информационной безопасности или на выпускающей кафедре и в научных лабораториях ВлГУ.

4. Формы проведения производственной практики.

Производственная практика проводится как непрерывно с выделением в учебном графике периода времени по окончании четвертого и шестого семестра обучения, так и во время обучения в шестом семестре. Форма проведения является заводской или лабораторной. При прохождении практики на выпускающей кафедре и в научных лабораториях ВлГУ, руководство организационными аспектами производственной практики

осуществляет преподаватель выпускающей кафедры информатики и защиты информации, назначаемый заведующим кафедрой ИЗИ. При прохождении практики на предприятиях и организациях, руководство организационными аспектами производственной практики осуществляет как преподаватель выпускающей кафедры, так и должностное лицо, назначаемое руководителем организации, принимающей студентов на практику (руководитель от предприятия).

В случае прохождения производственной 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 бакалавру информацию по заданию на практику и осуществляет текущий контроль работы бакалавра. 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 производственной практики предлагается студентом по согласованию с научным руководителем соответствующего направления. Научным руководителем производственной практики может быть только преподаватель выпускающей кафедры.

Кроме индивидуального задания и в зависимости от тематики задания руководителя практики, при прохождении производственной 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, используемой 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 производственной практики обучающийся должен приобрести следующие практические навыки, умения, общекультурные (универсальные) и профессиональные компетенции:

Коды компетенции	Результаты освоения ООП *Содержание компетенций*	Перечень планируемых результатов при прохождении практики
ОК-8	способность к самоорганизации и самообразованию	**знать:** различные формы и методы научно-исследовательской работы. **уметь:** анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результата этого анализа. **владеть:** навыками освоения и внедрения новых систем защиты, сопровождения систем защиты; осуществлять поиск наиболее эффективных путей обработки информации, принципами и методами защиты информации.
ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач	**знать:** - суть научного метода, его основные характеристики, современную естественнонаучную картину мира; - основные законы и принципы, которым подчиняется поведение разнообразных физических моделей, а также, вытекающие из этих законов следствия и возможность их применения на практике; - теоретические методы построения решения разнообразных задач по физике; -методы и принципы постановки экспериментов в физике; -основные методы компьютерной физики; -основные принципы связи физики с другими науками; **уметь:** - проводить физический анализ практических задач; - приобретать новые научные и практические знания, опираясь на методы физики; - решать разнообразные задачи по физике; - широко использовать научную, справочную литературу, интернет-информацию в области физики в проектно-конструкторской, производственно-технологической, научно-исследовательской деятельности; - формировать системный подход к принятию управленческих решений; - анализировать и формализовать задачи своей профессиональной деятельности (научно-исследовательские, экспертно-аналитические, организационно-управленческие и др.) и выбирать адекватные пути и методы для их решения; квалифицированно применять имеющийся математический аппарат; использовать математические методы и модели для решения прикладных задач; применять основные законы физики при решении прикладных задач; **владеть:** - теоретическими методами курса общей физики; - -математическим аппаратом соответствующим теоретическим методам курса общей физики; - -методами анализа и решения задач по физике; - -методами использования компьютера, интернет-технологий при решении задач по физике;- методикой постановки и проведения физического эксперимента; - методикой анализа и обработки результатов физического эксперимента; - методами математического описания физических явлений и процессов, методами обработки информации, представленной в различном виде; - навыками поиска нормативной и технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов работы.

ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	**знать:** - суть научного метода, его основные характеристики, современную естественнонаучную картину мира, - основные понятия математики, в том числе математического анализа, линейной алгебры, интегрального и дифференциального исчисления, рядов, теории вероятности и математической статистики, дискретной математики; - математические методы обработки экспериментальных данных. **уметь:** формировать системный подход к принятию управленческих решений, анализировать альтернативные варианты; - использовать математические методы и модели для решения прикладных задач **владеть:** методами математического описания физических явлений и процессов, методами обработки информации, представленной в различном виде; - математическим аппаратом, навыками алгоритмизации и решения основных задач в профессиональной области; - математической символикой, для выражения количественных и качественных соотношений объектов.
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	**знать:** историю возникновения направления "Информационная безопасность", развитие направления "Информационная безопасность". ОСНОВНУЮ терминологию. Основы законодательства в области информационной безопасности, основные разделы направления "Информационная безопасность", типы угроз информационной безопасности и способы их упреждения, источники угроз информационной безопасности; - теоретические основы оценки рисков и угроз, предпосылки для управления информационными рисками и угрозами, основные требования по управлению информационными рисками и угрозами, порядок оценки рисков и угроз информационной безопасности, порядок обработки рисков и угроз. **уметь:** анализировать механизмы реализации методов зашиты конкретных объектов и процессов для решения профессиональных задач, применять штатные средства зашиты и специализированные продукты для решения типовых задач, квалифицированно оценивать область применения конкретных механизмов зашиты, грамотно использовать аппаратные средства зашиты при решении практических задач; - определять источники угрозы информационной безопасности; - применять отечественные и зарубежные стандарты в области безопасности для проектирования, разработки и оценки эффективности подсистем охраны **владеть:** методами анализа и формализации информационных процессов объекта и связей между ними; профессиональной терминологией, навыками внедрение и эксплуатации современных средств охраны, методами и средствами выявления угроз безопасности, методиками проверки защищенности с требованиями нормативных документов.
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	**знать:** основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные нормативные правовые акты в области информационной безопасности и защиты информации, а так же нормативные и методические документы Федеральной службы безопасности по техническому и экспортному контролю в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию

		в области обеспечения защиты государственной тайны основные принципы и сертификации средств защиты информации. **уметь:** использовать в практической деятельности правовые знания, анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав. **владеть:** навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	**знать:** теоретические основы оценки рисков и угроз, предпосылки для управления информационными рисками и угрозами, основные требования по управлению информационными рисками и угрозами, порядок оценки рисков и угроз информационной безопасности, порядок обработки рисков и угроз. **уметь:** определять источники угрозы информационной безопасности, организовывать предпроектное обследование, разрабатывать меры защиты от выявленных угроз, выбирать и устанавливать технические средства охраны, оценивать эффективность и надежность технической охраны, применять отечественные и зарубежные стандарты в области безопасности для проектирования, разработки и оценки эффективности подсистемы технической охраны. **владеть:** профессиональной терминологией, навыками внедрение и эксплуатации современных средств технической охраны, методами и средствами выявления угроз безопасности, методиками проверки защищенности с требованиями нормативных документов.
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	**Знать:** методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; современные средства разработки и анализа программного обеспечения на языках высокого уровня; аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; сигналы электросвязи, принципы построения систем и средств связи; принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них; основы схемотехники; **Уметь:** выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; **Владеть:** методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; методами расчета и инструментального контроля показателей технической защиты информации; навыками чтения электронных схем; методиками проверки защищенности объектов информатизации на соответствие

		требованиям нормативных документов; профессиональной терминологией.
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать:** основные понятия и методы администрирования Unix (Linux) в объеме, необходимом для практического использования операционной системы как серверной платформы основных сетевых служб (tftp, ftp, samba, http), платформы для создания АРМ разработки программного обеспечения на популярных языках высокого уровня, платформы для создания типового АРМ офисного сотрудника; - стандартные и пользовательские типы данных и методы их обработки; - принципы структурного и модульного программирования; - принципы разработки сложных программных систем, в том числе правила разработки интерфейса; - основные методы разработки машинных алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов; - определение, свойства, операции и правила использования указателей на переменные и функции в программе на языке высокого уровня; **Уметь:** устанавливать операционные системы Debian GNU/Linux, CentOS, Fedora, Ubuntu, FreeBSD, OpenSolaris; устанавливать дополнительное программное обеспечение как из исходных текстов, так и из официальных репозиториев дистрибутивов; писать простейшие сценарии (sh скрипты), упрощающие рутинные задачи администратора; - использовать методы абстрагирования и управления современных языков программирования для описания и решения конкретных прикладных задач; - строить формальную модель системы (подсистемы) по ее описанию в терминах предметной области; - разработать структуры информационных объектов, функционирующих в программной системе, и соответствующие им структуры данных (в том числе абстрактные); - разработать алгоритм и реализовать программу, выбрав наиболее подходящий метод и язык программирования; - разработать модульную структуру программной системы, обеспечивающие ее функциональную наполненность, и дружественный интерфейс пользователя; - использовать оптимальные методы поиска и сортировки данных; - создавать и использовать абстрактные типы данных, экспериментально (с помощью компьютера) исследовать эффективность алгоритма и программы; - индексировать данные; - хешировать данные; - анализировать существующие структуры данных на предмет оптимальности применения в конкретной задаче. **Владеть:** навыками использования пакетов систем управления виртуальными машинами (Oracle VirtualBox, VMWare); основными приемами работы с командными интерпритаторами Unix (Linux); навыками установки и базовой настройки операционных систем; - методами программирования, разработки эффективных алгоритмов решения прикладных задач; - основными методами разработки машинных алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов; - разработкой алгоритмов, используя общие схемы, методы и приемы построения алгоритмов; - технологией представления разнородных данных в виде алгоритмических структур.
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	**Знать:** аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления базами данных; принципы построения

		информационных систем; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; **Уметь:** формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; **Владеть:** методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз безопасности автоматизированным системам; методами расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; профессиональной терминологией
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Знать:** - основы администрирования вычислительных сетей; принципы построения информационных систем; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; методы и средства контроля эффективности технической защиты информации; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы организации информационных систем в соответствии с требованиями по защите информации; - эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы; - возможные действия противника, направленные на нарушение политики безопасности информации, наиболее уязвимые для атак противника элементы компьютерных систем, механизмы решения типовых задач защиты информации **Уметь:** - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;- пользоваться нормативными документами по защите информации; - охарактеризовать возможности методов обработки информации, границ их применения, оценивать точность и достоверность полученной информации, устанавливать влияние факторов на достоверность полученной информации, определять объемы хранимой информации,

		анализировать и оценивать угрозы информационной безопасности. **Владеть:** - методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; - методами и средствами выявления угроз безопасности автоматизированным системам; - методами технической защиты информации; - методами формирования требований по защите информации; - методами расчета и инструментального контроля показателей технической защиты информации; - методами организации и управления деятельностью служб защиты информации на предприятии; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - профессиональной терминологией. - основными методами определения затрат на информационную безопасность, структуру интеллектуальной собственности предприятий, классификацию и способы минимизации предпринимательских рисков.
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**знать:** -основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; - основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России. Знать понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации; международные стандарты информационной безопасности. **уметь:** - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну; уметь проводить процедуры аттестации, категорирования объектов информатизации; уметь пользоваться научно- технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме. **владеть:** навыками анализа методов и средств передачи, хранения и обработки данных, навыками применения средств охраны от негативных воздействий, навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; - типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования; :- навыками анализа информационной инфраструктуры информационной системы и ее безопасности; пользоваться нормативными документами

		по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать:** основные понятия и методы в области управления службой безопасности предприятия; содержание управленческой работы руководителя подразделения службы безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России; - основные средства и способы обеспечения информационной безопасности компьютерных систем; требования к защищенным АС;- критерии оценки эффективности защищенности; типы и виды программных и программно-аппаратных систем защиты информации. **Уметь:** - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов информационных систем; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем; - квалифицированно оценивать область применения программно-аппаратного средства защиты с учетом специфика объекта защиты; применять средства ВТ, средства программирования для эффективной реализации аппаратно-программных комплексов заданного качества и в заданные сроки; проводить испытания объектов профессиональной деятельности; - производить установку, настройку и обслуживание программно-аппаратных средств защиты информации; - ставить и решать задачи, возникающие в процессе проектирования, отладки, испытаний и эксплуатации системных программных средств. **Владеть:** - навыками анализа информационной инфраструктуры информационной системы и ее безопасности; - методами выявления угроз информационной безопасности информационных систем; -пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; -применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; - навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; - навыками сопровождения программно-аппаратных

		средств защиты информации; - навыками консультирования персонала в процессе использования указанных средств.
ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**знать:** технические средства реализации информационных процессов, основные законодательные и нормативные документы по защите информации техническими средствами, правовые основы деятельности подразделений охраны, основные демаскирующие признаки объектов охраны, методы и способы технической охраны объектов информатизации и методы оценки их эффективности, основные методы исследования и диагностики технических средств охраны объектов информатизации; – состав, порядок формирования и методы оценки эффективности использования ресурсов для обеспечения информационной безопасности; – показатели и методы оценки эффективности (рентабельности) деятельности структурных подразделений обеспечения информационной безопасности предприятий (организаций);– сущность, структуру и значение экономических потерь от реализации угроз информационной безопасности, а также методы и способы оценки стоимости защищаемых информационных ресурсов; – о методах технико-экономического анализа и обоснования выбора проектных решений по оснащению объектов системами защиты информации и оптимизации инженерных решений. **уметь:** - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; выбирать оптимальный метод для численной реализации, эффективно применять ЭВМ для решения прикладных задач, анализировать численные результаты решения задачи; – формулировать цели и задачи по экономической оценке инженерно-технических решений в области обеспечения информационной безопасности;– проводить экономические расчеты и оценивать экономическую эффективность мероприятий по обеспечению защиты информации на предприятии (организации); – определять расходы по статьям сметы затрат на содержание структурных подразделений обеспечения информационной безопасности предприятий (организаций) **владеть:** методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; методами количественного анализа процессов обработки, поиска и передачи информации; – навыками определения экономической эффективности в области обеспечения информационной безопасности.
ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**знать:** структуру систем документационного обеспечения. **уметь:** пользоваться нормативными документами по защите информации. **владеть:** типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования.
ПК-9	способность осуществлять подбор, изучение и обобщение научно- технической литературы,	**Знать:** - базовый понятийный аппарат в области ИБ; - виды и состав угроз информационной безопасности; - принципы и общие методы обеспечения информационной

	нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	безопасности; - основные положения государственной политики обеспечения информационной безопасности; - критерии, условия и принципы отнесения информации к защищаемой; - виды носителей защищаемой информации; - виды тайн конфиденциальной информации; - виды уязвимости защищаемой информации; - источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; - каналы и методы несанкционированного доступа к конфиденциальной информации; - классификацию видов, методов и средств защиты информации; принципы и методы организационной защиты информации. **Уметь:** - выявлять угрозы информационной безопасности применительно к объектам защиты; - определять состав конфиденциальной информации применительно к видам тайны; - выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия; - выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации; - определять направления и виды защиты информации с учетом характера информации и задач по ее защите; - выполнять поиск, сбор, обработку, анализ и систематизацию информации по теме исследования; - производить выбор методов и средств решения задач исследования, разрабатывать инструментарий для проведения исследований, применять современные информационные технологии. **Владеть:** - основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации; информацией о современных и перспективных системах автоматизации информационно-аналитической работы; навыками использования современных программных и аппаратных средств при проведении научно-исследовательской работы.
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	**знать:** основные способы представления информации с использованием математических средств, этапы метода математического моделирования, возможности применения основных математических моделей в прикладных задачах. **уметь:** использовать методы передачи, хранения и защиты информации для исследования различных явлений и процессов, в том числе: методы теории кодирования для решения задач передачи информации по каналам связи с шумами, криптографические методы защиты информации от несанкционированного доступа для передачи информации с использованием как криптосистем с секретными ключами, так и криптосистем с открытыми ключами, знать методы теории информации для решения задач передачи информации по каналам связи без шума. **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам.
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	**Знать:** - основные математические методы исследования случайных процессов; - основные теоретико-числовые методы применительно к задачам защиты информации; - основные классификационные признаки экспериментов; - основные элементы научно-технического эксперимента; - приемы выбора основных факторов эксперимента и технологию построения факторных планов; - основные виды регрессионных экспериментов; - основные типы оптимальных экспериментов.

		Уметь: - самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач; - применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; - проводить классификацию экспериментов; - выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; - строить системы базисных функций, делать точечные оценки параметров регрессионной модели; - анализировать свойства оценок параметров регрессионной модели; - выполнять оптимальное планирование экспериментов с использованием различных критериев. **Владеть:** - методами выбора основных факторов эксперимента и построения факторных планов; - методами подбора эмпирических зависимостей для экспериментальных данных; - методами оценки коэффициентов регрессионной модели эксперимента; - методами построения оптимальных планов для научно-технических экспериментов; - навыками аналитического и численного решения задач математической статистики; - методами проведения физического эксперимента при выявлении технических каналов утечки информации.
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	**Знать:** - базовые способы оценки и повышения защищенности информационных ресурсов в корпоративных информационных системах, - способы инвентаризации программных сервисов и информационных ресурсов; - ключевые точки приложения информационных атак в типовой структуре корпоративных ИС; - методы и алгоритмы реструктуризации и реинжиниринга информационных процессов в рамках корпоративной информационной инфраструктуры; - основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем **Уметь:** - ставить и решать типовые задачи в области оценки и повышения защищенности корпоративных ИС; - подбирать и использовать адекватные методы и средства защиты информации; – оценивать эффективность методов защиты информационных процессов экспертным путем; - осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; **Владеть:** - навыками аудита информационной безопасности с использованием современных программно-технических средств; - навыками проведения экспертной оценки уровня безопасности систем; - приемами тестирования уязвимостей корпоративных программно-технических сервисов, типовыми атаками на ИС предприятий; - современным аппаратом для количественной и качественной оценки результатов аудита, комплексами средств защиты информации; - навыками управления информационной безопасностью простых объектов.
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	**Знать:** - особенности предприятия как сложного экономического объекта управления; - задачи, решаемые с использованием КИС на различных уровнях управления; - компоненты корпоративной информационной системы; - современные технологии построения КИС; - пути достижения максимальной эффективности от внедрения КИС; - принципы

		построения информационных систем; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; - принципы организации информационных систем в соответствии с требованиями по защите информации; - цели, задачи и принципы построения системы защиты информации; - требования, предъявляемые к системе защиты информации; - этапы разработки комплексной системы защиты информации; - первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; - перечень вопросов ЗИ, требующих документационного закрепления; - виды контроля функционирования системы защиты информации на предприятии. **Уметь:** - анализировать процессы управления на различных уровнях корпоративных систем; - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации. **Владеть:** - методами и средствами выявления угроз безопасности автоматизированным системам; - методами анализа и формализации информационных процессов объекта и связей между ними; - информацией о факторах, определяющие необходимость защиты территории и здания предприятия; -информацией о взаимодействии между субъектами, защищающими и использующими информацию ограниченного доступа; - методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; - методикой определения возможностей несанкционированного доступа к защищаемой информации; -методикой разработке модели комплексной системы защиты информации.
ПК-14	способность организовывать работу малого коллектива исполнителей в профессиональной деятельности	**Знать:** основные понятия и методы в области управления службой безопасности предприятия; содержание управленческой работы руководителя подразделения службы безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России; - этапы разработки комплексной системы защиты информации; - первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; - перечень вопросов ЗИ, требующих документационного закрепления; - виды контроля функционирования системы защиты информации на предприятии; - основные понятия, законы и модели прогнозирования принятия решений; методологию принятия управленческих решений; - параметры и

		условия обеспечения качества и эффективности управленческих решений в условиях рисков и неопределенностей; - особенности принятия управленческих решений для обеспечения информационной безопасности. **Уметь:** - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов информационных систем; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации; - применять основные закономерности принятия управленческих решений и управления коллективом при решении прикладных задач обеспечения информационной безопасности. **Владеть:-** навыками анализа информационной инфраструктуры информационной системы и ее безопасности; - пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; -применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; - информацией о структуре технического задания на создание комплексной системы защиты информации на предприятии; - методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; -методикой разработке модели комплексной системы защиты информации.
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знать:** - компоненты корпоративной информационной системы; - современные технологии построения КИС; современные средства проектирования и создания КИС; - пути достижения максимальной эффективности от внедрения КИС; - основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; - принципы организации информационных систем в соответствии с требованиями по защите информации. **Уметь:** - анализировать процессы управления на различных уровнях корпоративных систем; анализировать специфику процессов управления предприятием; - анализировать и оценивать угрозы информационной безопасности объекта; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. **Владеть:** - методами и средствами выявления угроз безопасности автоматизированным системам; - методами анализа и формализации информационных процессов объекта и связей между ними; - профессиональной терминологией.
ПСК-3.1	способность проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств, с целью	**Знать:** - принципы и методы организационной защиты информации; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы

	определения возможных источников информационных угроз, их вероятных целей и тактики	противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - теоретические основы оценки рисков и угроз, предпосылки для управления информационными рисками и угрозами, основные требования по управлению информационными рисками и угрозами, порядок оценки рисков и угроз информационной безопасности, порядок обработки рисков и угроз; - возможные действия противника, направленные на нарушение политики безопасности информации, наиболее уязвимые для атак противника элементы компьютерных систем. **Уметь:** - формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; - определять источники угрозы информационной безопасности; - разрабатывать меры защиты от выявленных угроз, выбирать и устанавливать технические средства охраны, оценивать эффективность и надежность технической охраны; - анализировать и оценивать угрозы информационной безопасности, определять размер целесообразных затрат на обеспечение информационной безопасности, проводить экономическую оценку объектов интеллектуальной собственности, а также анализ и оценку предпринимательских рисков. **Владеть:** - навыками организации и обеспечения режима секретности; - методами технической защиты информации; - методами формирования требований по защите информации; - методами расчета и инструментального контроля показателей технической защиты информации; - методами организации и управления деятельностью служб защиты информации на предприятии; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; - методами и средствами выявления угроз безопасности, методиками проверки защищенности с требованиями нормативных документов.
ПСК-3.2	способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объектов и локализации защищаемых элементов	**знать:** технические средства реализации информационных процессов, основные законодательные и нормативные документы по защите информации техническими средствами, правовые основы деятельности подразделений охраны, основные демаскирующие признаки объектов охраны, методы и способы технической охраны объектов информатизации и методы оценки их эффективности, основные методы исследования и диагностики технических средств охраны объектов информатизации. **уметь:** применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. **владеть:** методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
ПСК-3.3	способность разработать комплекс организационных и	**Знать:** - принципы и методы организационной защиты информации, создания систем охранно-тревожной

	технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	сигнализации, систем контроля и управления доступом, охранного телевидения; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - современные компьютерные технологии и программное обеспечение для решения задач, связанных с процедурами обработки аналитической информации и поиском информации; - этапы разработки комплексной системы защиты информации; - первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; - перечень вопросов ЗИ, требующих документационного закрепления; - виды контроля функционирования системы защиты информации на предприятии. **Уметь:** - анализировать и формализовать задачи своей профессиональной деятельности (научно-исследовательские, экспертно-аналитические, организационно-управленческие и др.) и выбирать адекватные пути и методы для их решения; квалифицированно применять полученные знания; - анализировать и оценивать угрозы информационной безопасности объекта, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; - формировать комплекс мер по информационной безопасности с учетом его технической обоснованности и реализуемости; - осуществлять изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации **Владеть:** -методами и средствами выявления угроз безопасности автоматизированным системам; - навыками организации и обеспечения режима секретности; - методами технической защиты информации; - методами формирования требований по защите информации; - методами расчета и инструментального контроля показателей технической защиты информации; - профессиональной терминологией; -навыками безопасного использования технических средств в профессиональной деятельности; -навыками поиска технической информации, необходимой для профессиональной деятельности, обоснования, выбора, реализации и контроля результатов в профессиональной деятельности; - квалифицированно использовать сетевые ресурсы с целью организации интерактивного взаимодействия, а также поиска и передачи информации в локальных и глобальных информационных сетях.
ПСК-3.4	способность организовать и сопровождать аттестацию объектов информатизации в соответствии с нормативными документами	**знать:** - принципы и методы организационной защиты информации, создания систем охранно-тревожной сигнализации, систем контроля и управления доступом, охранного телевидения; - технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; - принципы и методы противодействия несанкционированному

		информационному воздействию на вычислительные системы и системы передачи информации; - современные компьютерные технологии и программное обеспечение для решения задач, связанных с процедурами обработки аналитической информации и поиском информации; - основные принципы обеспечения информационной безопасности и защиты информации; структуру систем документационного обеспечения; - основные понятия и методы в области управления службой безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России. **уметь:** -, оценивать и разрабатывать мероприятия по повышению уровня технической защиты информации; - формировать комплекс мер по информационной безопасности с учетом его технической обоснованности и реализуемости; - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности сведений, составляющих государственную и коммерческую тайну; уметь проводить процедуры аттестации, категорирования объектов информатизации; уметь пользоваться научно- технической и справочной литературой для решения прикладных задач; **владеть:** навыками оценки защищенности объектов информатизации, навыками организации охраны на объектах информатизации, навыками применения технических средств защиты информации; - навыками анализа информационной инфраструктуры информационной системы и ее безопасности; пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения безопасности сведений, составляющих государственную и коммерческую тайну; владеть методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях для обеспечения защиты сведений, составляющих государственную и коммерческую тайну; -методами и средствами выявления угроз безопасности автоматизированным системам; - навыками организации и обеспечения режима секретности; - методами технической защиты информации; - методами формирования требований по защите информации; -методами расчета и инструментального контроля показателей технической защиты информации

6. Место производственной практики в структуре ООП бакалавриата

Практика бакалавров относится к Блоку Б2 «Практики». Настоящая программа практики основывается на требованиях, определённых Федеральным государственным образовательным стандартом высшего образования по направлению 10.03.01 «Информационная безопасность».

Производственная практика базируется на основе изучения следующих дисциплин:
Базовой части программы:

- математика;
- • основы информационной безопасности;
- физические процессы ы информационной безопасности;
- физика;
- информатика;
- электротехника;
- технологии и методы программирования;
- сети и системы передачи информации;

Вариативной части программы:

- аппаратные средства вычислительной техники
- математическое моделирование;
- структуры данных;
- администрирование сетей
- теория информации
- методы формализации и моделирования объектов информатизации

Практика проводится на 2 курсе и 3 курсе, по окончании 4 и 6 семестра обучения.

Требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки студентов направления 10.03.01 «Информационная безопасность» по курсам «Математика», «Информатика», «Технологии и методы программирования», «Структуры данных»; «Сети и системы передачи информации»; «Методы формализации и моделирования объектов информатизации».

Производственная 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 производственной практики.

Производственная практика проводится в три этапа во время обучения согласно графику учебного процесса.

1. Производственная практика по окончании 4 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.

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

3. Производственная практика по окончании 6 семестра обучения. Данная практика является стационарной и проводится в течение 2 и 2/3 недели 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 производственной практики составляет:

4 семестр не распределенная практика:

___3(три)_____ зачетных единицы; __108_____ часов (недель).

6 семестр распределенная практика:

___2(две)_____ зачетных единицы; __72_____ часа (недель).

6 семестр не распределенная практика:

___4(четыре)_____ зачетных единицы; __144_____ часа (недель).

9. Структура и содержание производственной практики

№ п/п	Разделы (этапы) практики	Виды производственной работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля
4 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
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	Консультации (в том числе и дистанционно)

		программного обеспечения и оборудования и т.д.) (58 часов)	
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 производственной практике распределенной практике по окончании 6 семестра.

10. Формы отчетности по практике

По итогам аттестации практики выставляется зачет с оценкой.

В состав отчёта по производственной практике должны входить:

• индивидуальное задание на прохождение практики, утверждённое руководителем практики;

• дневник практики для учебной практики не составляется (только для производственной 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 производственной практики бакалавров по направлению 10.03.01 «Информационная безопасность».

Структура и оформление отчетов о производственной 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 производственной 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 бакалавром, планы семинарских занятий и другая информация, характеризующая вклад бакалавра в изучение предметной области практики.

Аттестация по результатам прохождения производственной 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 производственную практику. *(Для конкретного задания студентов на производственную 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.ВО01.-99

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

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

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

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

Решаемые системой задачи:

- контроль НСД сотрудников или нарушителей на территорию (или с территории) объекта через проходные и КПП;
- контроль НСД сотрудников или нарушителей на территорию (или с территории) объекта через ограждения или запретные зоны;
- защита людей и материальных ценностей от преступных 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 вариообъектовов, тип управления диафрагмой и др.

Технические характеристики устройств управления и коммутации видеосигналов:

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

Технические характеристики видеомониторов:

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

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

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

Порядок назначения прав по доступу к критичным ресурсам.

Регламент резервирования и восстановления критичной информации.

Расположение критичной информации.

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

Наличие систем электронного документооборота.

Наличие критичных для предприятия процессов электронной обработки и передачи данных.

Возможность круглосуточной работы.

Информация о топологии сети, сетевых соединениях и уз-лах

Карта сети:

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

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

Указать вариант организации выхода в Internet:

- подключение выделенного компьютера (способ подключения, авторизации и пр.);
- подключение сети (способ подключения, использование прокси-служб и прочее);
- необходимость контроля трафика и разграничения доступа 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 вибро-акустичекому 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 вы-деленном 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 производственной 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 производственной 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 бакалавра.

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 производственной практики.

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

В качестве обеспечения производственной 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 бакалаврской 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:

- 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
- 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.
- 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 Режим доступа: http://znanium.com/
- 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, Режим доступа: http://znanium.com/
- Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.
- 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, Режим доступа: http://znanium.com/
- 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. Режим доступа: http://znanium.com/
- Каратунова, Н. Г. Защита информации. Курс лекций : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://www.znanium.comРежим доступа: http://znanium.com/
- Мишин Д.В. Анализ защищенности распределенных информационных систем.

Идентификация ресурсов корпоративной сети передачи данных : практикум для вузов по направлению "Информационная безопасность" / Д. В. Мишин, Ю. М. Монахов ; Владимирский государственный университет (ВлГУ) .— Владимир : 2012 .— 94 с. ISBN 978-5-9984-0295-1.

- "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.
- 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, Режим доступа: http://znanium.com/

б) Дополнительная литература:

- Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2, Режим доступа: http://znanium.com/
- Соколов, А.И. Технические средства защиты информации : технические каналы утечки информации : учебное пособие / А. И. Соколов, М. Ю. Монахов ; ВлГУ .— Владимир:, 2007 .— 71 с.
- 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. Режим доступа: http://znanium.com/
- Бугаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бугаков, А. В. Тельный ; Владимирский государственный университет (ВлГУ) .— Владимир : 2007 .— 147 с. :
- Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2016 - 120 с.: Режим доступа: http://znanium.com/
- 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
- 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.Режим доступа: http://znanium.com/
- 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.
- Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М. : СОЛОН-ПРЕСС, 2009. http://www.studentlibrary.ru/book/ISBN5980030115.html 272 с.
- Воронин А.А. Вычислительные сети : учебное пособие / А. А. Воронин ; Владимирский государственный университет (ВлГУ) .— Владимир : 2011 .— 87 с. ISBN 978-5-9984-0179-A
- 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.
- 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 производственной практики

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

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

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

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

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»

к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № 7 от 28.12.16 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»
Протокол № 4 от 28.12.16 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ

Рабочая программа одобрена на 2017/18 учебный год
Протокол заседания кафедры № 1 от 30.08.17 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)