Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

ЭКСПЛУАТАЦИОННАЯ ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ ПРОИЗВОДСТВЕННАЯ ПРАКТИКА

Направление подготовки «(10.03.01) Информационная безопасность»
Направленность «Организация и технология защиты информации»

Квалификация (степень) выпускника: Бакалавр

Кострома

Программа производственной практики разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

Разработал: _____ Виноградова Г.Л.. доцент кафедры защиты информации, к.т.н., доцент

подпись

Рецензент: _____ Алексеев Д.С., доцент кафедры защиты информации, к.т.н.

подпись

УТВЕРЖДЕНО:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11__ от _30.05.2019__ г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_ г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

1. Цели и задачи практики

Цель 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 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.

Задачи практики:

В зависимости от тематики задания руководителя практики, задачами производственной практики являются:

•приобретение практических навыков работы в качестве специалиста 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.

Тип практики: производственная.

Вид практики: эксплуатационная, проектно-технологическая, преддипломная.

Форма проведения: стационарная, дискретная, распределенная

Производственная практика проводится как непрерывно с выделением в учебном графике периода времени по окончании четвертого и шестого семестра обучения. Форма проведения является проводимой в организации или подразделениях КГУ. При прохождении практики на выпускающей кафедре и в научных лабораториях КГУ, руководство организационными аспектами производственной практики осуществляет преподаватель выпускающей кафедры защиты информации, назначаемый заведующим кафедрой ЗИ. 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 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 ТСМ и методики эксплуатации ТСМ;
- отдельные пакеты программных средств компьютерного обеспечения ЗИ объектов профессиональной деятельности;
- порядок пользования периодическими, реферативными и справочно-информационными изданиями по профилю направления подготовки.

2. Планируемые результаты прохождения практики

В результате прохождения практики обучающийся должен:

знать:

- 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 ТСМ и методики эксплуатации ТСМ;
- отдельные пакеты программных средств компьютерного обеспечения ЗИ объектов профессиональной деятельности;

- порядок пользования периодическими, реферативными и справочно-информационными изданиями по профилю направления подготовки;

уметь:

- 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;
- выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических_ и технических средств защиты информации;
- применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования в области защиты информации;
- администрировать подсистемы информационной безопасности объекта защиты;
- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности;
- принимать участие в формирование, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;
- разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение;

владеть:

- навыками участия в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- навыками участия в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- навыками оформления рабочей технической документации с учетом действующих нормативных и методических документов;
- навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
- навыками проведения экспериментов по заданной методике, обработку, оценку погрешности и достоверности результатов;
- навыками организации работы малого коллектива в области информационной безопасности;
- навыками организации технологического процесса 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;
- навыками формирования предложений по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов;

- навыками организации контроля защищенности объекта в соответствии с нормативными документами.

освоить компетенции:

- способность к самоорганизации и самообразованию ОК-8,
- способность анализировать физические явления и процессы для решения профессиональных задач (ОПК-1);
- способность применять соответствующий математический аппарат для решения профессиональных задач ОПК-2,
– способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4).
- способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5);
- 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 (ОПК-7);
- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических_ и технических средств защиты информации (ПК-1),
- способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2),
- способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3),
- способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4),
- способность применять участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ПК-5,
- способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);
- способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);
- способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);
- способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);
- способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10),
- способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности результатов (ПК-11);
- способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

- способностью принимать участие в формирование, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);
- способность организовывать работу малого коллектива в профессиональной деятельности (ПК-14);
– 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 (ПК-15);
- способностью проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК-2.1);
– способность формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК-2.2);
– способностью разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-2.3);
- способностью организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК-2.4).

3. Место учебной/производственной практики в структуре ОП

Практика относится к вариативной части учебного плана. Практика проводится в 4,6,8 семестре(ах) обучения. Практика проводится с отрывом от учебы. Способ проведения практики стационарная.

Прохождение практики основывается на ранее освоенных дисциплинах/практиках:

Производственная (эксплуатационная) (4 семестр) на учебной практике, математике, физике, основам информационной безопасности, основы программирования и алгоритмизации, информационные технологии, алгоритмы и структуры данных.

Производственная (проектно-технологическая) (6 семестр) на эксплуатационной практике, электроника и схемотехника, базы данных, теоретические основы информационных процессов, теории информации и кодирования, базы данных, криптографические методы защиты информации, техническая защита информации, сети и системы передачи информации, защита информационных процессов в компьютерных системах, безопасность телекоммуникационных систем, безопасность компьютерных сетей, методы и средства защиты программного обеспечения, защита и обработка конфиденциальных документов.

Производственная (преддипломная) (8 семестр) на эксплуатационной, проектно-технологической практиках, организационное и правовое обеспечение информационной безопасности, программно-аппаратные средства защиты информации, основы управления информационной безопасностью, комплексные системы защиты информации на предприятии, управление информационными ресурсами и проектами, стандартизация, лицензирование и сертификация, информационный менеджмент, организация и управление службой защиты информации на предприятии, защита государственных интересов, методы и средства защиты программного обеспечения, аудит защищенности объектов информатизации, технические средства охраны и видеонаблюдения.

Прохождение практики является основой для освоения последующих дисциплин/практик:

Производственная (эксплуатационная) (4 семестр) - производственная (проектно-технологическая) (6 семестр), электроника и схемотехника, базы данных, теоретические основы информационных процессов, теории информации и кодирования, базы данных, криптографические методы защиты информации, техническая защита информации, сети и системы передачи информации, защита информационных процессов в компьютерных системах, безопасность телекоммуникационных систем, безопасность компьютерных сетей, методы и средства защиты программного обеспечения, защита и обработка конфиденциальных документов.

Производственная (проектно-технологическая) (6 семестр) - производственная (преддипломная) практика, организационное и правовое обеспечение информационной безопасности, программно-аппаратные средства защиты информации, основы управления информационной безопасностью, комплексные системы защиты информации на предприятии, управление информационными ресурсами и проектами, стандартизация, лицензирование и сертификация, информационный менеджмент, организация и управление службой защиты информации на предприятии, защита государственных интересов, методы и средства защиты программного обеспечения, аудит защищенности объектов информатизации, технические средства охраны и видеонаблюдения.

Производственная (преддипломная) (8 семестр) – для написания квалификационной выпускной работы.

Трудоемкость практики составляет:
Производственная (эксплуатационная) (4 семестр) 108 часов, 2 недели, 3 зачетных единиц.
Производственная (проектно-технологическая) (6 семестр) 216 часов, 4 недели, 6 зачетных единиц.
Производственная (преддипломная) (8 семестр) 216 часов, 4 недели, 6 зачетных единиц.

4. База проведения практики

Практика может проводиться как в структурных подразделениях университета, так и на предприятиях, в учреждениях и организациях, деятельность которых соответствуют профессиональным компетенциям, осваиваемым в рамках ОП, на основе договоров. При недостаточном количестве в регионе организаций, деятельность которых соответствуют профессиональным компетенциям, для проведения практик могут использоваться рабочие места индивидуальных предпринимателей.

Для лиц, с ограниченными возможностями здоровья выбор мест прохождения практик должен учитывать состояние здоровья и требования по доступности.

Организации и учреждения:

1. Территориальный фонд обязательного медицинского страхования
2. ООО «ММТР»
3. ЗАО "БДКО" "Безопасные дороги Костромской области"
4. Управление федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Костромской области
5. ООО "Аргус-Сервис"
6. ПАО ВТБ24
7. Администрация Костромской области
8. Управление МЧС по Костромской области
9. Обособленное подразделение ЗАО "Калуга Астрал" в городе Костроме
10. АО "Газпром газораспределение Кострома"
11. Областное государственное казенное учреждение «Многофункциональный центр предоставления государственных и муниципальных услуг»

5. Структура и содержание учебной/производственной практики

№ п/п	Этапы прохождения практики	Содержание работ на практике	Задания, умения и навыки, получаемые обучающимися	Формы текущего контроля
Производственная (эксплуатационная) (4 семестр)				
1	Подготовительный	Проведение организационного собрания. Получение задания на практику. Ознакомление с заданием, планирование работы. Проведение инструктажа по ОТ и ТБ на рабочем месте		Собеседование
2	Подготовка теоретических материалов	Сбор, обработка и систематизация фактического и литературного материала, в т,ч. лекций, практических занятий, методических казаний и т.д.		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.		Консультации (в том числе и дистанционно)
4	Отчёт по практике	Составление отчёта по практике		Отчет (в том числе и в электронном виде
5	Зачёт по практике	Подготовка к зачёту. Зачет по практике		Зачет
Производственная (проектно-технологическая) (6 семестр)				
1	Подготовительный	Получение задания на практику. Ознакомление с заданием, планирование аботы.		Собеседование
2	Подготовка теоретических материалов,	Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических казаний и т.д.		Собеседование, консультации
3	Практические работы по теме задания на практику	Проведение практических занятий (например, разработка программных средств, информационных систем, установка необходимого		Консультации (в том числе и дистанционно)
Производственная (преддипломная) (8 семестр)				
1	Подготовитель	Проведение организационного		Собеседов

	ный	собрания. Получение задания на практику. Ознакомление с заданием, планирование работы. Проведение инструктажа по ОТ и ТБ на рабочем месте.		ание
2	Подготовка теоретических материалов.	Сбор, обработка и систематизация фактического и литературного материала, в т.ч. лекций, практических занятий, методических азаний и т.д.		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.		Консультации (в том числе и дистанционно)
4	Отчёт по практике	Составление отчёта по практике		Отчет (в том числе и в электронном виде
5	Зачёт по практике	Подготовка к зачёту. Зачет по практике		Зачет

6. Методические материалы для обучающихся по прохождению практики

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».

Оформление отчета осуществляется согласно установленным требованиям:

Правила оформления текстовых документов : руководящий документ пооформлению рефератов, отчетов о лабораторных работах, практиках, пояснительных записок к курсовым проектам и выпускным квалификационным работам / А.В. Басова, С.В. Боженко, Т.Н. Вахнина, И.Б. Горланова, И.А. Делекторская, Р.Г. Евтушенко, А.А. Титунин, О.В. Тройченко, С.А. Угрюмов, С.Г. Шарабарина ; под общ.ред. О. В.

Тройченко. – 2-е изд., перераб. и доп. – Кострома : Изд-во Костром.гос. ун-та, 2017. – 47 с. / (https://sdo.freshdesk.com/helpdesk/attachments/26001068088)

Структурными элементами отчета являются:

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

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 З - 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 — З раза, превышать наименьший.

В заключении формулируется основной результат работы и фо пунктам) выводы по результатам выполненной работы (как правило, З — 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 10—20 страниц. По тексту отчета должны содержаться ссылки на источники информации. Ссылки на публикации, приведенные в списке использованных источников, допускаются только цифровые.

7. Перечень основной и дополнительной литературы, необходимой для освоения практики

а) основная

1. **Информационная безопасность конструкций ЭВМ и систем** : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — М. : ИНФРА-М, 2018. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — **http://znanium.com/catalog.php?bookinfo=925825**
2. **Информационная безопасность и защита информации**: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). — h**ttp://znanium.com/catalog.php?bookinfo=763644**
3. **Загинайлов, Ю.Н.** Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
4. **Нестеров, С.А**. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
5. **Информационная безопасность и защита информации** : учеб. пособие для вузов / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2010. - 384 с.: рис. - ISBN 978-5-94178-216-1 : 590.00.
6. **Бабаш, Александр Владимирович .** Информационная безопасность : Лабор. практикум+CD: учеб. пособие / Бабаш, Александр Владимирович . - 2-изд., стер. - Москва : КноРус, 2013. - 136 с.: рис. - (Бакалавриат). - СД. - осн. - ISBN 978-5-406-02760-8 : 303.00.
7. Правила оформления текстовых документов : руководящий документ пооформлению рефератов, отчетов о лабораторных работах, практиках, пояснительных записок к курсовым проектам и выпускным квалификационным работам / А.В. Басова, С.В. Боженко, Т.Н. Вахнина, И.Б. Горланова, И.А. Делекторская, Р.Г. Евтушенко, А.А. Титунин, О.В. Тройченко, С.А. Угрюмов, С.Г. Шарабарина ; под общ.ред. О. В. Тройченко. – 2-е изд., перераб. и доп. – Кострома : Изд-во Костром.гос. ун-та, 2017. – 47 с. / (https://sdo.freshdesk.com/helpdesk/attachments/26001068088)

8.

б) дополнительная

1. **Информационная безопасность предприятия** : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). **http://znanium.com/catalog.php?bookinfo=612572**
2. **Информационная система предприятия**: Учебное пособие/Вдовенко Л. А., 2-е изд., перераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с.: 60x90 1/16 (Переплёт 7БЦ) ISBN 978-5-9558-0329-6, 500 экз. **http://znanium.com/catalog.php?bookinfo=501089**
3. **Артемов, А.В**. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605
4. **Золотарев, В. В**. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. **http://znanium.com/catalog.php?bookinfo=463037**
5. **Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности** [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. **http://znanium.com/catalog.php?bookinfo=463061**
6. **Бабаш, Александр Владимирович.** Информационная безопасность : лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - М. : КНОРУС, 2012. - 131 с. + 1 опт. диск. - Библиогр.: с. 131. - ISBN 978-5-406-01170-6 : 250.00.
7. **Мельников, Владимир Павлович.** Информационная безопасность и защита информации : учеб. пособие для вузов спец. 230201 "Информац. системы и технологии" / Мельников Владимир Павлович, С. А. Клейменов, А. М. Петраков ; под ред. Клейменова С.А. - 3-е изд., стер. - Москва : Академия, 2008. - 336 с. - (Высш. проф. образов. Информат. и выч. техн.). - УМО. - ЕН, ОПД, СД. - ISBN 978-5-7695-4884-0 : 165.66.
8. **Партыка, Татьяна Леонидовна.** Информационная безопасность : Учеб. пособие для сред. проф. образования, спец. информатики и выч. техники / Партыка Татьяна Леонидовна, Попов Игорь Иванович. - 2-е изд., испр. и доп. - Москва : ФОРУМ - ИЕФРА-М, 2007. - 368 с.: ил. - (Профессиональное образование). - МО РФ . - ОПД, СД. - ISBN 5-91134-095-X; 5-16-002849-8 : 288.00.
9. **Филин, Сергей Александрович.** Информационная безопасность : учеб. пособие / Филин Сергей Александрович. - Москва : Альфа-Пресс, 2006. - 412 с. - ОПД, СД. - ISBN 5-94280-163-0 : 200.00.
10. **Малюк, А. А.** Информационная безопасность: концептуальные и методологические основы защиты информации : Учеб. пособие для студ. высш. учеб. заведений / А. А. Малюк. - М. : Горячая линия-Телеком , 2004. - 280 с. : ил. - Библиогр.: с. 276-278. - ISBN 5-93517-197-X : 99.00. В прил.: Гос. образовательный стандарт высшего профессионального образования. - Допущено МО РФ
11. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, ОМ. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ МОР: НИЦ ИНФРА-М, 2015. - 392 с. ISBN 978-5-369-013786 Режим доступа: http://znanium.com/
12. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/booWlSBN9785940746478.html. 474 с.

13. 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 978-59558-0310-4, Режим доступа: http://znanium.com/
14. Каратунова, Н. Г. Защита информации. Курс лекций : Учебное пособие / Н. Г, Каратунова. Краснодар: КСЭИ, 2014. 188 с. Режим доступа: http://www.znanium.comPe-.k14M доступа: http://znanium.com/
15. Информационная безопасность компьютерных систем и сетей: Учебное пособие /
16. ВО. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: 1SBN 978-5-8199-0331-5, Режим доступа: http://znanium.com/
17. 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/
18. Соколов, А.И. Технические средства защиты информации : технические каналы утечки информации : учебное пособие / А. И. Соколов, М, Ю. Монахов ; ВлГУ, Владимир:, 2007 .—71 с.
19. Информационная безопасность и защита информации: Учебное пособие Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ МОР, НИЦ ИНФРА-М, 2016. - 322 с. ISBN 978-5-36901450-9. Режим доступа: http://znanium.com/
20. Бутаков, В.П. Технические средства охраны : системы контроля и управления доступом : учебное пособие / В. П. Бутаков, А. В. Тельный ; Владимирский государственный университет (ВлГУ) .— Владимир : 2007 147 с.:
21. 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/
22. 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. lSBN 978-5-9984-0020-9
23. Кнауб, Л. В. Теоретико-численные методы в криптографии : Учеб. пособие / Л. В.
24. 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/
25. Практическая криптография: алгоритмы и их программирование / Аграновский А.В,, Хади Р.А.м. СОЛОН-ПРЕСС, 2009. ht1p://mw.studentlibrary.ru/booWlSBN5980030026.html 256 с, ISBN 5-98003-002-6.
26. Цифровая стеганография / ВГ. Грибунин, И.Н. Оков, ИВ. Туринцев - М. : СОЛОН-ПРЕСС, 2009. http://№vw.studentlibrary.ru/book/ISBN5980030115.html 272 с.
27. Воронин А.А. Вычислительные сети : учебное пособие / А. А. Воронин :Владимирский государственный университет (ВлГУ) .— Владимир : 2011 — 87 с. ISBN 978-5-9984-0179-А

в) Периодические издания

1. Журнал «Вопросы защиты информации». Режим доступа: http://ivimi.ru/editions/detail.php?SECTION 0=155';
2. Журнал ”Information» 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:

4. ИНТУИТ. Национальный открытый университет.— Режим доступа: http://wy»w.intuit.ru/

Электронные библиотечные системы:
1. ЭБС «Лань»
2. ЭБС «Университетская библиотека online»
3. ЭБС «Znanium»

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики

Электронные библиотечные системы:
1. ЭБС «Лань»
2. ЭБС «Университетская библиотека online»
3. ЭБС «Znanium»

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по практике

При прохождении производственной практики на кафедре защиты информации КГУ имеется следующая материально-техническая база:

1. Многофункциональный поисковый прибор ST 031 “Пиранья»
2. Портативный обнаружитель полупроводниковых элементов «Лорнет»
3. Детектор поля ST 107
4. Оптико-электронный обнаружитель микровидеокамер «Чистильщик»
5. Имитатор многофункциональный "ИМФ-2"
6. Устройство защиты объектов информатизации от утечки информации за счёт ПЭМИН "Соната-Р2"
7. Анализатор спектра «Тритон»
8. Автоматизированная измерительная система «Талис-НЧ-Лайт»
9. Цифровой запоминающий осциллограф «АКИП-4115/6А
10. Генератор-усилитель тестового акустического сигнала «Шорох 2МИ
11. Акустическая колонка для системы «Шорох 2МИ»
12. Комплект СЗИ НСД Scarlet Net v 7.0 + Secret Net Card
13. Генератор электромагнитного шума «Салют 2000Б»
14. Устройство для быстрого уничтожения информации на НЖМД «Стек НС1в»
15. Программный комплекс защиты от НСД «Zecurion Lock»
16. Программный комплекс защиты от НСД «Dallas Lock 8.0-K»
17. Программно-аппаратный комплекс защиты от НСД «Соболь»
18. Аппаратный модуль доверенной загрузки «Аккорд ФМДЗ»
19. Комплекс СЗИ НСД «Страж NT»
20. Стол поворотный диэлектрический для проведения стендовых испытаний
21. Комплекс обнаружения ПЭМИН «Сигурд – Р19»
22. Учебный стенд технических средств охраны и видеонаблюдения «Наружное видеонаблюдение»
23. Учебный стенд технических средств охраны и видеонаблюдения «Внутреннее видеонаблюдение»
24. Учебный стенд технических средств охраны и видеонаблюдения «Интеллектуальное видеонаблюдение»
25. Учебный стенд технических средств охраны и видеонаблюдения «Системы контроля и управления доступом»

При прохождении практики в сторонни организациях и предприятиях, необходимое лабораторное, экспериментальное и компьютерное оборудование, а так же программное обеспечение определяются руководителем практики от кафедры ЗИ КГУ согласно выданного задания для прохождения практики.

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