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

Институт информационных технологий и радиоэлектроники
(Наименование института)

УТВЕРЖДАЮ:
Директор института
_____/А.А. Галкин/
«24» 06 2021 г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Производственная (технологическая)
(наименование типа практики)

направление подготовки / специальность

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки)

направленность (профиль) подготовки

**Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)**
(направленность (профиль) подготовки))

г. Владимир

2021 год

Вид практики - __ПРОИЗВОДСТВЕННАЯ_____
(учебная, производственная)

1. Цели практики

Проведение производственной (технологической) практики направлено на 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 (технологической) практики являются:

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

2. Задачи производственной (технологической) практики

Задачами производственной (технологической) практики являются:

• приобретение практических навыков работы в качестве специалиста (менеджера) информационной безопасности предприятия (организации);

• изучение методов обеспечения безопасности информации, применяемых на предприятии (в организации);

• освоение на практике методов предпроектного обследования объектов информатизации, проведения системного анализа результатов обследования при построении модели комплексной системы защиты информации;

• приобретение практического опыта разработки компонентов комплексной системы защиты информации предприятия (организации).

• изучение технологии регистрации, сбора, передачи и обработки информации о несанкционированных действиях, ознакомление с характеристиками периферийной, терминальной и вычислительной техники и особенностями их эксплуатации в условиях функционирования аппаратно-программных компонентов подсистем комплексной системы защиты информации.

• изучение документации комплексной системы защиты информации предприятия (организации), получение знаний по оформлению технических и рабочих проектов системы защиты информации и порядку внедрения утвержденных решений.

• привитие навыка системного подхода при проектировании комплексной системы защиты информации и отдельных ее подсистем.

• приобретение навыков выбора комплекса технических средств и сопряжения их в

единую систему, расчета необходимого числа технических средств, расчета разграничения доступа к ресурсам информационной системы предприятия (организации).

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

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

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

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

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

• подготовка и систематизация необходимых материалов для выполнения курсового проекта (работы) по изучаемым дисциплинам и сбор материалов по выполнению выпускной квалификационной работы.

В ходе 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 _стационарная_

(стационарная, выездная и т.д.)

4. Формы проведения производственной практики

Производственная практика проводится в два этапа во время обучения.

1. Распределенная производственная практика во время 6 семестра обучения. Данная практика является распределенной, параллельно с учебным процессом, стационарной и проводится в течение не менее 6 недель на выпускающей кафедре и в учебных лабораториях кафедры ИЗИ ВлГУ. Форма проведения является лабораторной. Руководство организационными аспектами распределенной производственной практики осуществляет преподаватель выпускающей кафедры информатики и защиты информации, назначаемый заведующим кафедрой ИЗИ.

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

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.

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 от кафедры ИЗИ, являющийся научным руководителем студента 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. 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 КЗИ, 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 установленными в образовательной программе индикаторами достижения компетенций

Код компетенции/ индикатора достижения компетенции	Результаты освоения ОПОП (содержание компетенции / индикатора достижения компетенции)	Перечень планируемых результатов при прохождении практики
ПК-1 Способен осуществлять анализ уязвимостей внедряемой системы защиты информации	ПК-1.1.1 Знает основные методы и средства криптографической защиты информации	Знания методы и средства криптографической защиты информации; способы защиты информации от «утечки» по техническим каналам; руководящие и методические документы государственных регуляторов; организационные меры по ЗИ на предприятии; содержание эксплуатационной документации автоматизированной системы
	ПК-1.1.2 Знает способы защиты информации от «утечки» по техническим каналам	
	ПК-1.1.3 Знает нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	
	ПК-1.1.4 Знает организационные меры по защите информации	
	ПК-1.1.5 Знает содержание эксплуатационной документации автоматизированной системы	
	ПК-1.2.1 Умеет классифицировать и оценивать угрозы безопасности информации автоматизированной системы	Умения классифицировать и оценивать угрозы безопасности АИС; разрабатывать предложения по совершенствованию системы управления ЗИ АИС; проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе ЗИ АИС;
	ПК-1.2.2 Умеет разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы	
	ПК-1.2.3 Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств	
	ПК-1.3.1 Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем	Навыки выбора и обоснования критериев эффективности функционирования средств ЗИ в АИС; анализа уязвимости программных и программно- аппаратных средств СЗИ АИС
	ПК-1.3.2 Владеет навыками анализа уязвимости программных и программно- аппаратных средств системы защиты информации автоматизированной системы	
ПК-2 Способен осуществлять управление защитой информации в автоматизированных системах	ПК-2.1.1. Знает Нормативные правовые акты в области защиты информации. Национальные, межгосударственные и международные стандарты в области защиты информации; руководящие и методические документы уполномо-	Знания - правовые акты в области защиты информации. Национальные, межгосударственные и международные стандарты в области защиты информации; руководящие и методические документы

	ченных федеральных органов исполнительной власти по защите информации	действующие на предприятии; 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 на предприятии;
	ПК-2.1.2. Знает 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	
	ПК-2.2.1. Умеет организовывать процесс применения отечественных и зарубежных стандартов в области защиты информации для проектирования, разработки и оценки защищенности компьютерных систем	Умения организовывать процесс применения отечественных и зарубежных стандартов в области защиты информации на предприятии; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации на предприятии; классифицировать и оценивать угрозы безопасности информации на предприятии
	ПК-2.2.2. Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации	
	ПК-2.2.3. Умеет анализировать и использовать в практической деятельности нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа	
	ПК-2.2.4. Умеет классифицировать и оценивать угрозы безопасности информации; определять подлежащие защите информационные ресурсы автоматизированных систем	
	ПК-2.3.1. Владеет навыками анализа информационной инфраструктуры информационной системы и ее безопасности на предмет соответствия действующим стандартам нормативно-правовым документам	Навыки анализа информационной инфраструктуры информационной системы и ее безопасности на предмет соответствия действующим стандартам нормативно-правовым документам на предприятии; внесения изменений в эксплуатационную документацию и организационно-распорядительные документы СЗИ АИС на предприятии
	ПК-2.3.2. Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы	
ПК-3 Способен осуществлять аудит защищенности информации в автоматизированных системах	ПК-3.1.1 Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	Знания криптографические методы, алгоритмы, протоколы, используемые для ЗИ в АИС на предприятии; способы защиты информации от «утечки» по техническим каналам; методы контроля эффективности защиты информации от «утечки» по
	ПК-3.1.2 Знает способы защиты информации от «утечки» по техническим каналам; методы кон-	

	троля эффективности защиты информации от «утечки» по техническим каналам; принципы построения систем защиты информации	техническим каналам на предприятии; нормативные правовые акты в области защиты информации; руководящие и методические документы госрегуляторов, действующие на предприятии; Знает организационные меры по защите информации в АИС на предприятии
	ПК-3.1.3 Знает нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	
	ПК-3.1.4 Знает организационные меры по защите информации	
	ПК-3.2.1 Умеет классифицировать и оценивать угрозы безопасности информации для объекта информатизации	Умения классифицировать и оценивать угрозы безопасности информации на предприятии; разрабатывать предложения по совершенствованию системы управления ИБ АИС на предприятии; разрабатывать политики безопасности информации автоматизированных систем; применять инструментальные средства контроля защищенности информации для АИС предприятия
	ПК-3.2.2 Умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	
	ПК-3.2.3 Умеет разрабатывать политики безопасности информации автоматизированных систем	
	ПК-3.2.4 Умеет применять инструментальные средства контроля защищенности информации в автоматизированных системах	
	ПК-3.3.1 Владеет навыками Оценки информационных рисков	Навыки Оценки информационных рисков для ИР АИС предприятия; обоснования и контроля результатов управленческих решений в области безопасности информации АИС на предприятии; оценки состояния защищенности информации в АИС предприятия
	ПК-3.3.2 Владеет навыками обоснования и контроля результатов управленческих решений в области безопасности информации автоматизированных систем; навыками оценки состояния защищенности информации автоматизированных систем	
ПК-4 Способен разрабатывать организационно-распорядительных документы по защите информации в автоматизированных системах	ПК-4.1.1 Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	Знания порядок деятельности персонала по эксплуатации защищенных АИС и СЗИ на предприятии; основные угрозы безопасности информации и модели нарушителя в АИС на предприятии; нормативные правовые акты в области защиты информации; - руководящие и методические документы государственных регуляторов, действующие на предприятии
	ПК-4.1.2 Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	
	ПК-4.1.3 Знает нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	
	ПК-4.2.1 Умеет классифицировать и оценивать угрозы информационной безопасности	Умения классифицировать и оценивать угрозы информационной безопасности на предприятии; контролировать эффективность принятых мер по ЗИ в АИС на предприятии;
	ПК-4.2.2 Умеет контролировать эффективность принятых мер по защите информации в автоматизи-	

	рованных системах	
	ПК-4.3.1 Владеет навыками определения правил и процедур управления системой защиты информации автоматизированной системы	Навыки определения правил и процедур управления ЗСИ в АИС на предприятии; определения правил и процедур выявления инцидентов в АИС на предприятии; навыками определения правил и процедур мониторинга обеспечения уровня защищенности информации в АИС на предприятии; навыками определения правил и процедур реагирования на инциденты в АИС на предприятии
	ПК-4.3.2 Владеет навыками определения правил и процедур выявления инцидентов	
	ПК-4.3.3 Владеет навыками определения правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы	
	ПК-4.3.4 Владеет навыками определения правил и процедур реагирования на инциденты	

6. Место практики в структуре ОПОП, объем и продолжительность практики

Производственная (технологическая) практика относится к части, формируемой участниками образовательных отношений Блока 2. «Практики» в соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационая безопасность».

Объем производственной (технологической) практики составляет:

6 семестр распределенная практика параллельно с учебным процессом 9(девять) зачетных единиц (324 часа), продолжительность – _не менее 6__ недель;

6 семестр не распределенная практика 3(три) зачетных единиц (108 часов), продолжительность – _2__ недели;

Общая трудоемкость производственной практики в 6 семестре составляет 12(двенадцать) зачетных единиц (432 часа);

7. Структура и содержание производственной (технологической) практики

№ п/п	Разделы (этапы) практики	Виды учебной работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля
6 семестр распределенная практика параллельно с учебным процессом			
1	Подготовительный	Получение задания на практику. Ознакомление с заданием, планирование работы. (10 часов)	Собеседование
2	Информационный (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	Аналитический (разработка новых методик, алгоритмов и т.д.)	Информационно-аналитическая работа по совершенствованию или формированию новых методик, алгоритмов, теоретических положений и т.д. (40 часов)	Собеседование, консультации
4	Исследовательский (практические работы по теме задания на практику)	Проведение практических занятий (например, разработка программных средств, информационных систем, установка и конфигурирование необходимого программного обеспечения и оборудования, проведение экспериментов и т.д.) (254 часа)	Консультации (в том числе и дистанционно)

6 семестр не распределенная практика			
1	Подготовительный	Проведение организационного собрания. Получение задания на практику. Ознакомление с заданием, планирование работы. Проведение инструктажа по ОТ и ТБ на рабочем месте. (10 часов)	Собеседование
2	Информационный (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	Исследовательский (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.) (58 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 с оценкой

Примечание:

Отчет по распределенной практике в течение 6 семестра параллельно с учебным процессом и отчет по не распределенной практике по окончании 6 семестра делается совместно по одному выданному (уточненному) заданию от научного руководителя студента. Защита отчета проводится после прохождения производственной практике распределенной практике по окончании 6 семестра.

8. 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 научным руководителем студента;
- дневник прохождения практики (форма представлена на сайте учебно-методического управления ВлГУ (http://uu.vlsu.ru/) в разделе «документы/практика»);
- отчет по практике (материалы с результатами работы, выводами и предложениями) в распечатанном, бумажном виде;
- отчет по практике в электронном виде и дополнительные материалы, программы, расчеты, таблицы и пр. (при необходимости) в электронном виде;
- 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. При оформлении отчетов следует придерживаться следующих правил и рекомендаций.

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

Лист аннотации должен содержать:

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

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

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

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

Отчет должен быть отпечатан шрифтом Times New Roman № 14 через 1,5 интервала на одной стороне белой бумаги формата А4. Размеры полей: сверху, снизу – 20 мм, слева – 30 мм, справа – 10 мм. В таблицах, сносках, подписях рисунков допускается использовать шрифт 10-12pt. 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 в квадратных скобках. Нумерация ссылок на используемые источники производится по мере их упоминания в тексте работы. Ссылки на публикации, приведенные в списке использованных источников, допускаются только цифровые. Рекомендуемой количество используемых источников литера-

туры не менее 25.

Разрешается использовать компьютерные возможности, применяя шрифты разной гарнитуры для акцентирования внимания на определенных терминах, формулах, теоремах и т.п. Отчет распечатывается на принтере листы формата А4 в одном экземпляре. К отчету прилагается диск CD-R/RW, DVD-R/RW, содержащий все электронные материалы по работе. Допускается вместо дисков CD-R/RW, DVD-R/RW сдавать отчет в электронном виде на любом носителе или пересылать преподавателю по электронной почте или размещать в сети с использованием облачных технологий. При этом отчет не должен содержать конфиденциальной информации и персональных данных третьих лиц и преподавателей. Переплет бумажного варианта отчета может быть произвольным, но должен исключать рассыпание листов.

Защита результатов практики с предоставлением настоящего отчета и других документов проходит в форме собеседования с членами специальной комиссии из преподавателей кафедры и оценки результатов практики в виде дифференцированного зачета.

Студенты, без уважительных причин не выполнившие программу практики, а также получившие не удовлетворительную оценку при защите отчета, отчисляются из университета как имеющие академическую задолженность.

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

При подготовке отчётной документации и представлении результатов проделанной работы используется Microsoft Office – офисный пакет приложений для операционных систем Microsoft Windows (академическая лицензия для студентов и преподавателей ВлГУ).

При прохождении практики используются следующие образовательные, научно-исследовательские и профессионально-ориентированные технологии:

– интерактивные и проектные технологии обучения;

– использование современных интернет и компьютерных технологий (как на основном этапе проведения практики, так и на этапе обработки полученной информации, подготовки отчета по практике);

– по результатам проведения практики проводится публичная защита отчета, где студенты имеют возможность обсудить полученные результаты, произвести обмен впечатлениями и опытом.

Наряду с традиционными образовательными технологиями, при организации и прохождении практики могут использоваться технологии электронного обучения и дистанционные образовательные технологий в электронной информационно-образовательной среде ВлГУ. Контактная работа обучающихся с руководителем практики может проводиться с использованием платформ Microsoft Teams, Cisco, Moodle, Zoom, общения по электронной почте, WhatsApp, Viber и др., что позволяет обеспечить онлайн и офлайн взаимодействие руководителя практики с обучающимися.

Основными методами контроля являются электронный учёт и контроль учебных достижений студентов (использование средств сервиса информационно-образовательной среды ВлГУ).

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

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронной библиотеке ВлГУ (дата обращения)
Основная литература*		
1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. ISBN 978-5-4475-3946-7. – DOI 10.23681/276557.	2015	https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 257.08.2021)
2. Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие : [16+] / Е. А. Басыня. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил. ISBN 978-5-7782-3484-0.	2018	https://biblioclub.ru/index.php?page=book&id=575325 (дата обращения: 25.08.2021).
3. Брюхомицкий, Ю. А. Безопасность информационных технологий : учебное пособие : в 2 частях : Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – Ч. 1. – 171 с. ISBN 978-5-9275-3571-2 (Ч. 1). - ISBN 978-5-9275-3526-2	2020	https://biblioclub.ru/index.php?page=book&id=612167 (дата обращения: 25.08.2021)
4. Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с ISBN 978-5-8265-1737-6.	2017	https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 25.08.2021)
5. Котов, Ю. А. Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом : [16+] / Ю. А. Котов. – Новосибирск : Новосибирский государственный технический университет, 2017. – 67 с. ISBN 978-5-7782-3411-6	2017	https://biblioclub.ru/index.php?page=book&id=574782 (дата обращения: 07.08.2021)
Дополнительная литература		
1. Илюхин Л. К. Преддипломная научно-творческая производственная практика / Л.К. Илюхин - Астрахань: Астраханский инженерно-строительный институт, 2010. - 28с.	2010	http://biblioclub.ru/index.php?page=book&id=438925 (дата обращения 25.08.2021)
2. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] /	2021	https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.08.2021)

А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988.		
3. Абденов, А. Современные системы управления информационной безопасностью : учебное пособие : [16+] / А. Абденов, Г. Дронова, В. Трушин ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2017. – 48 с. – ISBN 978-5-7782-3236-5	2017	https://biblioclub.ru/index.php?page=book&id=574594 (дата обращения: 07.08.2021)
4. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С. И. Козьминых ; Финансовый университет при Правительстве Российской Федерации. – Москва : Юнити-Дана, 2020. – 544 с.– ISBN 978-5-238-03200-9	2020	https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 25.08.2021)
5. Долозов, Н. Л. Программные средства защиты информации: конспект лекций / Н. Л. Долозов, Т. А. Гультяева ; Новосибирский государственный технический университет 2015. – 63 с. – ISBN 978-5-7782-2753-8	2015	https://biblioclub.ru/index.php?page=book&id=438307 (дата обращения: 25.08.2021)

11. Материально-техническое обеспечение производственной (технологической) практики

Материально-техническое обеспечение производственной (технологической) практики предоставляется организациями, принявшими студента на практику, на основе договоров с организациями, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках подготовки бакалавров направления 10.03.01 «Информационная безопасность» в соответствии с основной образовательной программой. При этом должны использоваться современная компьютерная техника, программные и технические средства, предоставляемые на предприятии (организации), где проходит производственная (технологическая) практика. Для самостоятельных занятий студент использует нормативно-техническую документацию организации. Рабочее место практиканта на предприятии прохождения производственной (технологической) практики должно соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-исследовательских работ.

Для проведения консультаций с научным руководителем практики от ВлГУ или прохождении практики на кафедре ИЗИ или в структурных подразделениях ВлГУ, используются лаборатории кафедры ИЗИ, с выходом в Интернет. Практиканту выделяется рабочее места в лаборатории кафедры, соответствующее действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-исследовательских работ. При прохождении практики в университете, используется оборудование следующих учебных аудиторий. Лекционная аудитория 408-2. Перечень оборудования: переносной проектор, маркерная доска, переносной ноутбук. Компьютерный класс 427а-2 на 12 персональных рабочих мест с доступом в Интернет, переносной проектор, маркерная и интерактивная доски, переносной ноутбук. Компьютерный

противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-исследовательских работ. При прохождении практики в университете, используется оборудование следующих учебных аудиторий. Лекционная аудитория 408-2. Перечень оборудования: переносной проектор, маркерная доска, переносной ноутбук. Компьютерный класс 427а-2 на 12 персональных рабочих мест с доступом в Интернет, переносной проектор, маркерная и интерактивная доски, переносной ноутбук. Компьютерный класс 427б-2 на 7 персональных рабочих мест с доступом в Интернет, стационарный проектор, маркерная доска, переносной ноутбук.

Необходимое лабораторное, экспериментальное и компьютерное оборудование, а также программное обеспечение определяются руководителем практики от кафедры ИЗИ.

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

Рабочую программу составил
доцент кафедры ИЗИ, к.т.н., доцент _____/А.В. Т[illegible]ный/
(ФИО, должность, подпись)

Рецензент:
_Заведующий кафедрой цифрового образования и информационной безопасности (ЦОИБ) ГАОУ ДПО _ Владимирского института развития образования имени Л.И.Новиковой, к.т.н._

_____/Д.В. Мишин /
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 26.08.21 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»

Протокол № 1 от 26.08.21 года
Председатель УМК направления 10.03.01 д.т.н, профессор_____/М.Ю. Монахов/
код направления И.О. Фамилия

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой_____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
в рабочую программу практики
НАИМЕНОВАНИЕ
образовательной программы направления подготовки *код и наименование ОП*,
направленность: *наименование (указать уровень подготовки*)

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/ _____

Подпись *ФИО*