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 (преддипломная)
(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 (преддипломной) 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). Преддипломная практика имеет целью получение практических навыков работы по специальности в профильных подразделениях предприятий (организаций, учреждений). Тема преддипломной практики должна быть логически связана с предполагаемой темой выпускной квалификационной работы. В процессе преддипломной практики студент получает практические, экспериментальные, модельные результаты, используемые при выполнении выпускной квалификационной работы. Преддипломную практику проходят студенты 4 курса обучения в соответствии с учебными планами направления 10.03.01 «Информационная безопасность» ВлГУ.

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

Целями производственной (преддипломной) практики являются:

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

2. Задачи производственной (преддипломной) практики

В зависимости от тематики задания руководителя практики и тематики выпускной квалификационной работы, задачами преддипломной практики являются:

- приобретение практических навыков работы в качестве специалиста (менеджера) информационной безопасности предприятия (организации);
- изучение методов обеспечения безопасности информации, применяемых на предприятии (в организации);
- освоение на практике методов предпроектного обследования объектов

информатизации, проведения системного анализа результатов обследования при построении модели комплексной системы защиты информации;

- приобретение практического опыта разработки компонентов комплексной системы защиты информации предприятия (организации);
- сбор и обобщение материалов, необходимых для выполнения выпускной квалификационной работы
- изучение технологии регистрации, сбора, передачи и обработки информации о несанкционированных действиях, ознакомление с характеристиками периферийной, терминальной и вычислительной техники и особенностями их эксплуатации в условиях функционирования аппаратно-программных компонентов подсистем комплексной системы защиты информации.
- изучение документации комплексной системы защиты информации предприятия (организации), получение знаний по оформлению технических и рабочих проектов системы защиты информации и порядку внедрения утвержденных решений.
- привитие навыка системного подхода при проектировании комплексной системы защиты информации и отдельных ее подсистем.
- приобретение навыков выбора комплекса технических средств и сопряжения их в единую систему, расчета необходимого числа технических средств, расчета разграничения доступа к ресурсам информационной системы предприятия (организации).
- ознакомление с системной классификацией и кодированием информации, принятой в информационной системе предприятия (организации).
- ознакомление с психологическими аспектами проблемы внедрения и функционирования комплексной системы защиты информации на предприятии (в организации) и в особенности в области применения технических средств (регистраторов, сканеров, дисплеев, графопостроителей, факс–модемов, видеоконтроля и специального оборудования).
- анализ характеристик информационных процессов и формирование исходных данных для проектирования комплексной системы защиты информации предприятия (организации).
- приобретение навыков обслуживания средств КЗИ, ТСЗИ, ПАСЗИ, ЗИ в ЭВМ, сетях ЭВМ и автоматизированных информационных системах.
- знакомство с методами и средствами обеспечения безопасности информации в документообороте, управлении бизнес-процессами и процессами административного и оперативного руководства.
- подготовка и систематизация необходимых материалов для выполнения выпускной квалификационной работы.

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

- подготовка практических и экспериментальных исследовательских заданий на оборудовании организации (например, установка и конфигурирование необходимого программного обеспечения и оборудования, проработка аналитических задач в интересах предприятия, сбор необходимых материалов);
- подготовка учебно-методических материалов (сбор информации, выполнение обзора современных технологий);
- разработка прикладного (части прикладного) программного обеспечения, в том числе в области автоматизации аналитической деятельности и т.д.

3. Способы проведения _стационарная_

(стационарная, выездная и т.д.)

4. Формы проведения преддипломной практики

Производственная преддипломная практика проводится по окончании 8 семестра обучения. Данная практика является стационарной и проводится в течение 4 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 преддипломной практики на выпускающей кафедре и в научных лабораториях ВлГУ, руководство организационными аспектами производственной преддипломной 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, который ежегодно разрабатывается кафедрой в соответствии с профилем ее учебно-методической и научно-исследовательской деятельности. Тема задания производственной преддипломной практики предлагается студентом по согласованию с научным руководителем соответствующего направления. Руководителем производственной практики может быть только преподаватель выпускающей кафедры, являющийся руководителем темы выпускной квалификационной работы студента.

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
ОПК-6 Способен при решении профессиональных задач организовать защиту информации ограниченного доступа в	ОПК-6.1.1 Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации	Знания систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации

соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях	средств защиты информации; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя объекта информатизации
	ОПК-6.1.1 Знает систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа	
	ОПК-6.1.1 Знает основные угрозы безопасности информации и модели нарушителя объекта информатизации	
	ОПК-6.2.1 Умеет разрабатывать модели угроз и модели нарушителя объекта информатизации в соответствии с требованиями нормативно-правовых документов государственных регуляторов	Умения разрабатывать модели угроз и модели нарушителя объекта информатизации в соответствии с требованиями нормативно-правовых документов государственных регуляторов; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации в соответствии с требованиями нормативно-правовых документов государственных регуляторов
	ОПК-6.2.2 Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа	
	ОПК-6.2.3 Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации в соответствии с требованиями нормативно-правовых документов государственных регуляторов	
ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.1.1 Знает методы разработки эффективных алгоритмов решения прикладных задач; типовые методы, используемые при работе с графами, орграфами, мультиграфами и сетями; технологии разработки алгоритмов и программ, методов отладки и решения задач на ЭВМ в различных режимах; элементы теории сложности алгоритмов; основные понятия алгоритмических структур для построения алгоритмов и задач по их математическим моделям	Знания разработки эффективных алгоритмов решения прикладных задач; типовые методы, используемые при работе с графами, орграфами, мультиграфами и сетями; технологии разработки алгоритмов и программ, методов отладки и решения задач на ЭВМ в различных режимах; элементы теории сложности алгоритмов; основные понятия алгоритмических структур для построения алгоритмов; 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; принципы тестирования программных систем; основные понятия объектно-ориентированного программирования; теоретические основы методов
	ОПК-7.1.2 Знает 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; принципы тестирования программных систем;	

	основные понятия объектно-ориентированного программирования	проектирования и способы описания языков программирования, основные положения теории формальных грамматик и языков, методов синтаксического анализа и перевода для класса формальных языков, используемых для описания основных конструкций языков программирования; стандарты, используемые для языков программирования; современные средства разработки и анализа программного обеспечения на языках высокого уровня; особенности взаимодействия языков высокого и низкого уровня, организации работы с памятью в скриптовых языках; язык программирования высокого уровня
	ОПК-7.1.3 Знает теоретические основы методов проектирования и способы описания языков программирования, основные положения теории формальных грамматик и языков, методов синтаксического анализа и перевода для класса формальных языков, используемых для описания основных конструкций языков программирования	
	ОПК-7.1.4 Знает стандарты, используемые для языков программирования; современные средства разработки и анализа программного обеспечения на языках высокого уровня; особенности взаимодействия языков высокого и низкого уровня, организации работы с памятью в скриптовых языках; язык программирования высокого уровня (объектно-ориентированное программирование)	
	ОПК-7.2.1 Умеет разрабатывать оптимальные алгоритмы для решения поставленных задач; формализовывать описание поставленных задач; применять алгоритмы решения следующих задач: минимизация булевых функций; поиск кратчайших путей в графе; построение остовного дерева графа; нахождение эйлеровых и гамильтоновых циклов в графах и т.д.; выбирать и использовать структуры представления данных для решения прикладных задач профессиональной деятельности	разрабатывать оптимальные алгоритмы для решения поставленных задач; формализовывать описание поставленных задач; применять алгоритмы решения следующих задач: минимизация булевых функций; поиск кратчайших путей в графе; построение остовного дерева графа; нахождение эйлеровых и гамильтоновых циклов в графах и т.д.; 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; разработать модульную структуру программной системы, обеспечивающие ее функциональную наполненность, и дружественный интерфейс пользователя; выполнить тестирование и отладку программной системы с целью устранения синтаксических и семантических ошибок с целью повышения надежности программного обеспечения; выполнять формальное описание синтаксиса и семантики, несложных процедурно - ориентированных и проблемно - ориентированных языков программирования; разрабатывать
	ОПК-7.2.2 Умеет 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)	
	ОПК-7.2.3 Умеет разработать модульную структуру программной системы, обеспечивающие ее функциональную наполненность, и дружественный интерфейс пользователя; выполнить тестирование и отладку программной системы с	

	целью устранения синтаксических и семантических ошибок с целью повышения надежности программного обеспечения	алгоритмы, реализующие методы синтаксического анализа и перевода для наиболее часто используемых классов формальных грамматик; 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; разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред и для сред с интерфейсом, управляемым сообщениями
	ОПК-7.2.4 Умеет самостоятельно выполнять формальное описание синтаксиса и семантики, несложных процедурно - ориентированных и проблемно - ориентированных языков программирования; разрабатывать алгоритмы, реализующие методы синтаксического анализа и перевода для наиболее часто используемых классов формальных грамматик	
	ОПК-7.2.5 Умеет 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; разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред и для сред с интерфейсом, управляемым сообщениями	
	ОПК-7.3.1 Владеет навыками грамотной постановки задач, возникающих в практической деятельности для их решения с помощью ЭВМ; навыками выбора структур данных; методиками разработки оптимальных алгоритмов для решения поставленных задач	Навыки грамотной постановки задач, возникающих в практической деятельности для их решения с помощью ЭВМ; навыками выбора структур данных; методиками разработки оптимальных алгоритмов для решения поставленных задач; методами программирования, разработки эффективных программных средств решения прикладных задач; методическими подходами в области формальных методов описания и введения стандартов, используемых для описания языков программирования; разработки программ на языке программирования высокого уровня
	ОПК-7.3.2 Владеет методами программирования, разработки эффективных программных средств решения прикладных задач	
	ОПК-7.3.3 Владеет методическими подходами в области формальных методов описания и введения стандартов, используемых для описания языков программирования	
	ОПК-7.3.4 Владеет навыками разработки программ на языке программирования высокого уровня	
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы	Знания основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и

	ОПК-9.1.2 Знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения	криптографические протоколы; основные положения (основополагающие теоремы) криптологии, вытекающие из теории симметричных и ассиметричных криптографических подходов, а также информационные критерии оценок функционирования криптографических систем; классификацию и количественные характеристики технических каналов утечки информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; методы и средства контроля эффективности технической защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; технические характеристики и возможности аппаратуры защиты информации от утечки по техническим каналам и аппаратуры средств несанкционированного съема информации по техническим каналам
	ОПК-9.1.3 Знает основные положения (основополагающие теоремы) криптологии, вытекающие из теории симметричных и ассиметричных криптографических подходов, а также информационные критерии оценок функционирования криптографических систем	
	ОПК-9.1.4 Знает классификацию и количественные характеристики технических каналов утечки информации	
	ОПК-9.1.5 Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; методы и средства контроля эффективности технической защиты информации	
	ОПК-9.1.6 Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации; технические характеристики и возможности аппаратуры защиты информации от утечки по техническим каналам и аппаратуры средств несанкционированного съема информации по техническим каналам	
	ОПК-9.2.1 Умеет разрабатывать и рассчитать характеристики криптографической защиты информационных систем в зависимости от назначения этих систем (количество информации, скорость передачи информации, пропускную способность каналов связи, требуемый объём памяти и др.)	Умения разрабатывать и рассчитать характеристики криптографической защиты информационных систем в зависимости от назначения этих систем (количество информации; применять современные технологии криптографии в задачах обработки информации; применять математические модели для оценки стойкости СКЗИ; использовать СКЗИ в автоматизированных системах; анализировать и оценивать угрозы утечки информации по техническим каналам на объекте информатизации; формировать комплекс мер по технической защите объекта информатизации от утечки информации по техническим каналам с учетом технической обоснованности и реализуемости;
	ОПК-9.2.2 Умеет применять современные технологии криптографии в задачах обработки информации; применять математические модели для оценки стойкости СКЗИ	
	ОПК-9.2.3 Умеет использовать СКЗИ в автоматизированных системах	
	ОПК-9.2.4 Умеет анализировать и оценивать угрозы утечки информации по техническим каналам на объекте информатизации	
	ОПК-9.2.5 Умеет формировать комплекс мер по технической защите объекта информатизации от утечки информации по техническим каналам с учетом технической обоснованности и реализуе-	

	мости	
	ОПК-9.3.1 Владеет общими проблемы криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем	Навыки Владеет общими проблемы криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем; методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации
	ОПК-9.3.2 Владеет методами и средствами технической защиты информации	
	ОПК-9.3.3 Владеет методами расчета и инструментального контроля показателей технической защиты информации	
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1.1 Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; типы и виды программных и программно-аппаратных систем защиты информации	Знания программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях; типы и виды программных и программно-аппаратных систем защиты информации; идентификация пользователей КС-субъектов доступа к данным; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ; методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в АИС; основные виды политик управления доступом и информационными потоками в компьютерных системах; защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита
	ОПК-10.1.2 Знает- методы идентификация пользователей КС-субъектов доступа к данным; средства и методы ограничения доступа к файлам; аппаратно-программные средства криптографической защиты информации; методы и средства ограничения доступа к компонентам ЭВМ	
	ОПК-10.1.3 Знает методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования	
	ОПК-10.1.4 Знает основные механизмы информационной безопасности и типовые процессы управления этими механизмами в автоматизированной системе; основные угрозы безопасности информации и модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных система	
	ОПК-10.1.5 Знает основные виды политик управления доступом и информационными потоками в компьютерных системах; защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита	
	ОПК-10.2.1 Умеет конфигурировать программно-аппаратные сред-	Умения конфигурировать программно-

	ства защиты информации в соответствии с заданными политиками безопасности; оценивать область применения программно-аппаратного средства защиты с учетом специфика объекта защиты	аппаратные средства защиты информации в соответствии с заданными политиками безопасности; оценивать область применения программно-аппаратного средства защиты с учетом специфика объекта защиты; производить установку, настройку и обслуживание программно-аппаратных средств защиты информации; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности в АИС; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью в АИС; Умеет формулировать и настраивать политику безопасности операционных систем, а также локальных вычислительных сетей, построенных на их основе; применять основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; формулировать и настраивать политику безопасности операционных систем, а также локальных компьютерных сетей, построенных на их основе
	ОПК-10.2.2 Умеет производить установку, настройку и обслуживание программно-аппаратных средств защиты информации	
	ОПК-10.2.3 Умеет строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных систем	
	ОПК-10.2.4 Умеет разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем	
	ОПК-10.2.5 Умеет контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем	
	ОПК-10.2.6 Умеет формулировать и настраивать политику безопасности операционных систем, а также локальных вычислительных сетей, построенных на их основе	
	ОПК-10.2.7 Умеет применять основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; формулировать и настраивать политику безопасности операционных систем, а также локальных компьютерных сетей, построенных на их основе	
	ОПК-10.3.1 Владеет навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа	Навыки освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; средствами выявления угроз безопасности автоматизированным системам; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами организации и управления деятельностью служб защиты
	ОПК-10.3.2 Владеет методами и средствами выявления угроз безопасности автоматизированным системам; навыками участия в экспертизе состояния защищенности информации на объекте защиты; методами организации и управле-	

	ния деятельностью служб защиты информации на предприятии	информации на предприятии; формирования частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; конфигурирования и администрирования операционных систем
	ОПК-10.3.3 Владеет навыками формирования частных политик безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	
	ОПК-10.3.4 Владеет навыками конфигурирования и администрирования операционных систем	
ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1.1 Знает теоретические основы теории погрешностей;	Знания теоретические основы теории погрешностей; проводить физический эксперимент, обрабатывать его результаты
	ОПК-11.1.1 Знает методы и принципы постановки экспериментов в физике	
	ОПК-11.2.1 Умеет проводить физический эксперимент, обрабатывать его результаты	Умения проводить физический эксперимент, обрабатывать его результаты; использовать стандартные вероятностно-статистические методы анализа экспериментальных данных; строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных; строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных
	ОПК-11.2.3 Умеет использовать стандартные вероятностно-статистические методы анализа экспериментальных данных	
	ОПК-11.2.4 Умеет строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных	
	ОПК-11.2.5 Умеет строить стандартные процедуры принятия решений, на основе имеющихся экспериментальных данных	
	ОПК-11.3.1 Владеет методикой постановки и проведения физического эксперимента	Навыки постановки и проведения физического эксперимента; анализа и обработки результатов физического эксперимента
	ОПК-11.3.2 Владеет методикой анализа и обработки результатов физического эксперимента	
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1.1 Знает принципы формирования политики информационной безопасности в информационных системах; основные угрозы безопасности информации и модели нарушителя в информационных системах	Знания формирования политики информационной безопасности в информационных системах; основные угрозы безопасности информации и модели нарушителя в АИС; методы аттестации уровня защищенности информационных систем; методологические основы анализа данных; методы снижения размерности многомерных данных
	ОПК-12.1.2 Знает методы аттестации уровня защищенности информационных систем	
	ОПК-12.1.3 Знает методологические основы анализа данных; методы снижения размерности многомерных данных	
	ОПК-12.2.1 Умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений	Умения разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений; оценивать информационные риски в АИС; строить системы управления информационной безопасностью в различных условиях функционирования защищаемых автоматизированных систем;
	ОПК-12.2.2 Умеет оценивать информационные риски в автоматизированных системах	
	ОПК-12.2.3 Умеет строить системы управления информационной безопасностью в различных усло-	

	виях функционирования защищаемых автоматизированных систем	разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем; применять методы анализа массивов данных при разработке алгоритмов анализа и обработки измерительной информации; ставить и решать практические задачи анализа данных в условиях различной полноты исходной информации; проводить комплексный анализ данных с использованием базовых параметрических и непараметрических моделей; применять современные автоматизированные технологии семантической обработки текстов при решении прикладных информационно- аналитических задач
	ОПК-12.2.4 Умеет разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; разрабатывать частные политики информационной безопасности информационных систем	
	ОПК-12.2.5 Умеет применять методы анализа массивов данных при разработке алгоритмов анализа и обработки измерительной информации	
	ОПК-12.2.6 Умеет ставить и решать практические задачи анализа данных в условиях различной полноты исходной информации; проводить комплексный анализ данных с использованием базовых параметрических и непараметрических моделей	
	ОПК-12.2.7 Умеет применять современные автоматизированные технологии семантической обработки текстов при решении прикладных информационно- аналитических задач	
	ОПК-12.3.1 Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем	Навыки выбора и обоснования критериев эффективности функционирования защищенных информационных систем; методами оценки информационных рисков; Владеет навыками работы с программным обеспечением для автоматического анализа текстов: морфологическими и синтаксическими анализаторами, конкордансами, системами извлечения фактов и отношений, инструментами кластеризации, классификации и тематического моделирования коллекций документов; решения формализованных математических задач анализа данных с помощью пакетов прикладных программ
	ОПК-12.3.2 Владеет методами оценки информационных рисков	
	ОПК-12.3.3 Владеет навыками работы с программным обеспечением для автоматического анализа текстов: морфологическими и синтаксическими анализаторами, конкордансами, системами извлечения фактов и отношений, инструментами кластеризации, классификации и тематического моделирования коллекций документов	
	ОПК-12.3.4 Владеет навыками решения формализованных математических задач анализа данных с помощью пакетов прикладных программ	
ОПК-4.1 Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1 -1.1 Знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знания руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации
	ОПК-4.1 -1.2 Знает организационные меры по защите информации	
	ОПК-4.1 -2.1 Умеет разрабатывать политики безопасности информации автоматизированных систем	Умения разрабатывать политики безопасности информации автоматизированных систем; осуществлять планирование и организацию работы персонала АИС с
	ОПК-4.1 -2.2 Умеет осуществлять планирование и организацию ра-	

	боты персонала автоматизированной системы с учетом требований по защите информации	учетом требований по защите информации; разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при её эксплуатации
	ОПК-4.1 -2.3 Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности)	
	ОПК-4.1 -3.1 Владеет навыками обнаружения инцидентов в процессе эксплуатации автоматизированной системы; идентификации инцидентов в процессе эксплуатации автоматизированной системы	Навыки обнаружения инцидентов в процессе эксплуатации автоматизированной системы; идентификации инцидентов в процессе эксплуатации АИС; навыками оценки защищенности АИС с помощью типовых программных средств
	ОПК-4.1 -3.2 Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств	
ОПК-4.2 Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ОПК-4.2 -1.1 Знает средства, методы и протоколы идентификации, аутентификации и авторизации	Знания средства, методы и протоколы идентификации, аутентификации и авторизации
	ОПК-4.2 -2.1 Умеет устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации	Умения: устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению ЗИ; управлять полномочиями пользователей
	ОПК-4.2 -2.2 Умеет управлять полномочиями пользователей	
	ОПК-4.2 -3.1 Владеет навыками обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы	Навыки обеспечения безопасности информации с учетом требования эффективного функционирования АИС; навыками обоснования критериев эффективности функционирования защищенных АИС
	ОПК-4.2 -3.2 Владеет навыками обоснования критериев эффективности функционирования защищенных АИС	
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3 -1.1 Знает основные меры по защите информации в автоматизированных системах	Знания мер по защите информации в АИС; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем
	ОПК-4.3 -1.2 Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем	
	ОПК-4.3 -2.1 Умеет настраивать программное обеспечение системы защиты информации автоматизированной системы	Умения настраивать программное обеспечение СЗИ в АИС; выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации
	ОПК-4.3 -2.2 Умеет выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	

	ОПК-4.3 -3.1 Владеет навыками оценки последствий от реализации угроз безопасности информации в автоматизированной системе	Навыки оценки последствий от реализации угроз безопасности информации в АИС
ОПК-4.4 Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4 -1.1 Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Знания угрозы безопасности информации и модели нарушителя в АИС
	ОПК-4.4 -2.1 Умеет контролировать уровень защищенности в автоматизированных системах	Умения контролировать уровень защищенности в АИС; регистрировать и анализировать события, связанные с ЗИ в АИС
	ОПК-4.4 -2.1 Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах	
	ОПК-4.4 -3.1 Владеет навыками Анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность	Навыки Анализа воздействия изменений конфигурации АИС на ее защищенность; составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения ЗИ в АИС
	ОПК-4.4 -3.2 Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	

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

Производственная (преддипломная) практика относится к обязательной части Блока 2. «Практики» в соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационая безопасность».

Объем производственной (преддипломной) практики составляет 6(шесть) зачетных единиц (216 часов), продолжительность – _4__ недели.

Практика проводится в _8__ семестре.

7. Структура и содержание производственной (преддипломной) практики

№ п/п	Разделы (этапы) практики	Виды учебной работы, на практике включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля
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.) (166 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

8. Формы отчетности по практике

По итогам аттестации преддипломной практики выставляется зачет с оценкой.

В состав отчёта по производственной преддипломной 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 литературы 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 преддипломной практики с предоставлением 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.

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

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

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

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

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

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

Использование сети Интернет (Интернет-технологий): способствует индивидуализации учебного процесса и обращению к принципиально новым познавательным средствам. В качестве обеспечения преддипломной практики выступают:

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

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.	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+] / 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.	2021	https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 07.08.2021)
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 :	2020	https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 25.08.2021)

Юнити-Дана, 2020. – 544 с.– ISBN 978-5-238-03200-9		
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 (преддипломной) практики

Материально-техническое обеспечение производственной (преддипломной) 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 (преддипломная) практика. Для самостоятельных занятий студент использует нормативно-техническую документацию организации. Рабочее место практиканта на предприятии прохождения производственной (преддипломной) 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 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. Тельный/
(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*