**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**

**10.04.01 «Информационная безопасность»**
(код и наименование направления подготовки)

**направленность (профиль) подготовки**

**Автоматизация информационно-аналитической деятельности**
(направленность (профиль) подготовки))

г. Владимир

2021 год

**Вид практики - __ПРОИЗВОДСТВЕННАЯ_____**
(учебная, производственная)

**1. Цели практики**

Целью практики является закрепление знаний и умений, полученных в процессе теоретического обучения, овладение методикой обеспечения информационной безопасности на предприятии (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 квалификационной работы. Преддипломную практику проходят студенты 2 курса обучения в соответствии с учебными планами направления 10.04.01 «Информационная безопасность» ВлГУ.

Тема задания на преддипломную практику должна соответствовать профилю направления 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 преддипломной практики являются:

- приобретение практических навыков работы в качестве специалиста (менеджера) ИБ предприятия (организации);
- получение практических, экспериментальных, модельных результатов, используемых при выполнении выпускной дипломной работы;
- сбор сведений об организации прохождения практики, необходимых для выполнения выпускной квалификационной работы;
-получение практических консультаций действующих специалистов предприятий и организаций по вопросам тематики дипломной 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 информатиза-

ции, 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 ТЗИ, КСЗИ, 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 в 4 семестре обучения. Данная практика является стационарной и проводится в течение 6 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 или лабораторной, в зависимости от задания на ВКР. 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-1** | Способен обосновывать требования к системе информационной безопасности и разрабатывать проект технического задания на ее создание | ОПК-1.1.1 Знает принципы организации информационных систем в соответствии с требованиями по защите информации; основные этапы процесса проектирования и общие требования к содержанию проекта |
| | | ОПК-1.1.2 Знает основные меры по защите информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем |
| | | ОПК-1.1.3 Знает критерии оценки защищенности автоматизированной системы |
| | | ОПК-1.1.4 Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | | ОПК-1.1.5 Знает основные отечественные и зарубежные стандарты в области компьютерной безопасности |
| | | ОПК-1.1.6 Знает основные методы организационного обеспечения информационной безопасности специальных информационно-аналитических систем |
| | | ОПК-1.2.1 Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите |
| | | ОПК-1.2.2 Умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения |
| | | ОПК-1.2.3 Умеет осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации |
| | | ОПК-1.2.4 Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации автоматизированной системы |
| | | ОПК-1.2.5 Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств |
| | | ОПК-1.2.6 Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях |
| | | ОПК-1.2.7 Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты информации; применять средства антивирусной защиты и обнаружения вторжений в компьютерные сети |

| | | |
|---|---|---|
| | | ОПК-1.2.8 Умеет пользоваться средствами защиты, предоставляемыми системами управления базами данных |
| | | ОПК-1.2.9 Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем |
| | | ОПК-1.3.1 Владеет навыками обнаружения инцидентов в процессе эксплуатации автоматизированной системы; идентификации инцидентов в процессе эксплуатации автоматизированной системы; оценки защищенности автоматизированных систем с помощью типовых программных средств |
| | | ОПК-1.3.2 Владеет навыками оценки последствий от реализации угроз безопасности информации в автоматизированной системе; навыками анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность |
| | | ОПК-1.3.3 Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе |
| | | ОПК-1.3.4 Владеет навыками настройки межсетевых экранов; владеет методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений в компьютерные сети |
| **ОПК-2** | Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности | ОПК-2.1.1 Знает основные отечественные и зарубежные стандарты в области компьютерной безопасности |
| | | ОПК-2.1.2 Знает основные методы организационного обеспечения информационной безопасности специальных информационно-аналитических систем |
| | | ОПК-2.1.3 Знает принципы организации информационных систем в соответствии с требованиями по защите информации; основные этапы процесса проектирования и общие требования к содержанию проекта |
| | | ОПК-2.1.4 Знает основные меры по защите информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем |
| | | ОПК-2.1.5 Знает критерии оценки защищенности автоматизированной системы |
| | | ОПК-2.1.6 Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах |
| | | ОПК-2.2.1 Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях |
| | | ОПК-2.2.2 Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты информации; пользоваться средствами защиты, предоставляемыми системами управления базами данных |
| | | ОПК-2.2.3 Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем |
| | | ОПК-2.2.4 Умеет применять средства антивирусной защиты и обнаружения вторжений в компьютерные сети |
| | | ОПК-2.2.5 Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации |

| | | |
|---|---|---|
| | | ОПК-2.2.6 Умеет формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения |
| | | ОПК-2.2.7 Умеет осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации |
| | | ОПК-2.2.8 Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах; классифицировать и оценивать угрозы безопасности информации автоматизированной системы |
| | | ОПК-2.2.9 Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств |
| | | ОПК-2.3.1 Владеет навыками настройки межсетевых экранов; методикой анализа сетевого трафика |
| | | ОПК-2.3.2 Владеет методикой анализа результатов работы средств обнаружения вторжений в компьютерные сети |
| | | ОПК-2.3.3 Владеет навыками обнаружения инцидентов в процессе эксплуатации автоматизированной системы; идентификации инцидентов в процессе эксплуатации автоматизированной системы |
| | | ОПК-2.3.4 Владеет оценки защищенности автоматизированных систем с помощью типовых программных средств; навыками оценки последствий от реализации угроз безопасности информации в автоматизированной системе |
| | | ОПК-2.3.5 Владеет навыками анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность |
| | | ОПК-2.3.6 Владеет навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе |
| **ОПК-3** | Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности | ОПК-3.1.1 Знает механизмы информационной безопасности и типовые процессы управления этими механизмами в информационной системе |
| | | ОПК-3.1.2 Знает Источники и классификация угроз информационной безопасности; модели нарушителя в информационных системах; принципы формирования политики информационной безопасности в информационных системах |
| | | ОПК-3.1.3 Знает методы аттестации уровня защищенности информационных систем; основные методы управления информационной безопасностью |
| | | ОПК-3.1.4 Знает основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем |
| | | ОПК-3.1.5 Знает принципы функционирования автоматизированных систем поддержки документооборота и их безопасности |
| | | ОПК-3.1.6 Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации |
| | | ОПК-3.2.1 Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности |
| | | ОПК-3.2.2 Умеет строить системы обеспечения информационной безопасности в различных условиях функционирования защищаемых информационных систем |

| | | |
|---|---|---|
| | | ОПК-3.2.3 Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем |
| | | ОПК-3.2.4 Умеет разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем |
| | | ОПК-3.2.5 Умеет оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем |
| | | ОПК-3.2.6 Умеет составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем |
| | | ОПК-3.2.7 Умеет обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности |
| | | ОПК-3.3.1 Владеет навыками формирования комплекса мер (принципов, правил, процедур, практических приемов, методов, средств) для защиты в ИАС информации ограниченного доступа |
| | | ОПК-3.3.2 Владеет навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем; навыками организации процесса разработки частных политик безопасности компьютерных систем, в том числе политик управления доступом и информационными потоками |
| | | ОПК-3.3.3 Владеет методами управления информационной безопасностью информационных систем; методами оценки информационных рисков; |
| | | ОПК-3.3.4 Владеет методами организации и управления деятельностью служб защиты информации на предприятии |
| | | ОПК-3.3.5 Владеет навыками управления информационной безопасностью простых объектов |
| **ОПК-4** | Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок | ОПК-4.1.1 Знает основные элементы научно-технического эксперимента; приемы выбора основных факторов эксперимента и технологию построения факторных планов |
| | | ОПК-4.1.2 Знает основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации |
| | | ОПК-4.1.3 Знает основные классификационные признаки экспериментов; основные виды регрессионных экспериментов ; - основные виды планов 2-го порядка |
| | | ОПК-4.1.4 Знает основные типы оптимальных экспериментов; современные методы научных исследований с использованием компьютерных технологий |
| | | ОПК-4.1.5 Знает способы сбора, изучения, анализа и обобщения научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности |
| | | ОПК-4.1.6 Знает порядок подготовки, выполнения и защиты квалификационных и иных научных работ |
| | | ОПК-4.1.7 Знает методологические основы, методы и средства моделирования специальных информационно-аналитических систем |

| | | |
|---|---|---|
| | | ОПК-4.1.8 Знает методы построения математических моделей технологических процессов обработки информации в специальных информационно-аналитических систем в виде сетей массового обслуживания |
| | | ОПК-4.1.9 Знает методы исследования математических моделей технологических процессов обработки информации в специальных информационно-аналитических систем |
| | | ОПК-4.1.10 Знает методы планирования и оптимизации экспериментов на ЭВМ с моделями технологических процессов обработки информации в специальных информационно-аналитических системах |
| | | ОПК-4.2.1 Умеет выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; - самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач |
| | | ОПК-4.2.2 Умеет применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; проводить классификацию экспериментов ; - строить системы базисных функций, делать точечные оценки параметров регрессионной модели |
| | | ОПК-4.2.3 Умеет анализировать свойства оценок параметров регрессионной модели; выполнять оптимальное планирование экспериментов с использованием различных критериев |
| | | ОПК-4.2.4 Умеет осуществлять сбор, изучение, анализ и обобщение научно-технической информации в области технологий информационно-аналитической деятельности и специальных ИАС |
| | | ОПК-4.2.5 Умеет проводить технико-экономическое обоснование проектных решений на базе моделирования |
| | | ОПК-4.2.6 Умеет применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных информационно-аналитических системах |
| | | ОПК-4.2.7 Умеет исследовать эффективность применяемых средств моделирования |
| | | ОПК-4.3.1 Владеет методами выбора основных факторов эксперимента и построения факторных планов; методами подбора эмпирических зависимостей для экспериментальных данных |
| | | ОПК-4.3.2 Владеет методами оценки коэффициентов регрессионной модели эксперимента; методами построения планов 2-го порядка для экспериментов |
| | | ОПК-4.3.3 Владеет методами построения оптимальных планов для научно-технических экспериментов |
| | | ОПК-4.3.4 Владеет навыками аналитического и численного решения задач математической статистики |
| | | ОПК-4.3.5 Владеет методами постановки и решения задач оценки эффективности специальных информационно-аналитических систем с помощью математического моделирования |
| | | ОПК-4.3.6 Владеет навыками работы с математическими моделями технологических процессов обработки информации в специальных информационно-аналитических системах и применения методов их исследования с целью оценки эффективности и научно обоснованного выбора их характеристик |
| | | ОПК-4.3.7 Владеет навыками выбора и обоснования критериев эффективности функционирования специальных информационно-аналитических систем |

| | | |
|---|---|---|
| **ОПК-5** | Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи | ОПК-5.1.1 Знает основные элементы научно-технического эксперимента; приемы выбора основных факторов эксперимента и технологию построения факторных планов |
| | | ОПК-5.1.2 Знает основные математические методы исследования случайных процессов; основные теоретико-числовые методы применительно к задачам защиты информации |
| | | ОПК-5.1.3 Знает основные классификационные признаки экспериментов; основные виды регрессионных экспериментов; основные виды планов 2-го порядка; основные типы оптимальных экспериментов |
| | | ОПК-5.1.4 Знает современные методы научных исследований с использованием компьютерных технологий |
| | | ОПК-5.1.5 Знает способы сбора, изучения, анализа и обобщения научно-технической информации, нормативных и методических материалов в области технологий информационно-аналитической деятельности и специальных ИАС, в том числе средств обеспечения их информационной безопасности |
| | | ОПК-5.1.6 Знает порядок подготовки, выполнения и защиты квалификационных и иных научных работ |
| | | ОПК-5.1.7 Знает методологические основы, методы и средства моделирования специальных информационно-аналитических систем; знает методы построения математических моделей технологических процессов обработки информации в специальных информационно-аналитических системах в виде сетей массового обслуживания |
| | | ОПК-5.1.8 Знает методы исследования математических моделей технологических процессов обработки информации в специальных информационно-аналитических систем |
| | | ОПК-5.1.9 Знает методы планирования и оптимизации экспериментов на ЭВМ с моделями; технологических процессов обработки информации в специальных информационно-аналитических системах |
| | | ОПК-5.2.1 Умеет выбирать необходимые факторы и составлять факторные планы экспериментов различного вида; самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач |
| | | ОПК-5.2.2 Умеет применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации; проводить классификацию экспериментов |
| | | ОПК-5.2.3 Умеет строить системы базисных функций, делать точечные оценки параметров регрессионной модели; анализировать свойства оценок параметров регрессионной модели |
| | | ОПК-5.2.4 Умеет выполнять оптимальное планирование экспериментов с использованием различных критериев |
| | | ОПК-5.2.5 Умеет осуществлять сбор, изучение, анализ и обобщение научно-технической информации в области технологий информационно-аналитической деятельности и специальных ИАС |
| | | ОПК-5.2.6 Умеет проводить технико-экономическое обоснование проектных решений на базе моделирования |
| | | ОПК-5.2.7 Умеет применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных информационно-аналитических системах |
| | | ОПК-5.2.8 Умеет исследовать эффективность применяемых средств моделирования |
| | | ОПК-5.3.1 Владеет методами выбора основных факторов эксперимента и построения факторных планов; методами подбора эмпирических зависимостей для экспериментальных данных |

| | | |
|---|---|---|
| | | ОПК-5.3.2 Владеет методами оценки коэффициентов регрессионной модели эксперимента; методами построения планов 2-го порядка для экспериментов |
| | | ОПК-5.3.3 Владеет методами построения оптимальных планов для научно-технических экспериментов |
| | | ОПК-5.3.4 Владеет навыками аналитического и численного решения задач математической статистики |
| | | ОПК-5.3.5 Владеет методами постановки и решения задач оценки эффективности специальных информационно-аналитических систем с помощью математического моделирования |
| | | ОПК-5.3.6 Владеет навыками работы с математическими моделями технологических процессов обработки информации в специальных информационно-аналитических системах и применения методов их исследования с целью оценки эффективности и научно обоснованного выбора их характеристик |
| | | ОПК-5.3.7 Владеет навыками выбора и обоснования критериев эффективности функционирования специальных информационно-аналитических систем |

## 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 10.04.01 «Информационая безопасность».

Объем производственной (преддипломной) практики составляет 9(девять) зачетных единиц (324 часа), продолжительность – _6__ недель.

Практика проводится в _4__ 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.) (274 часа) | 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 преддипломной 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, | 2017 | https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 25.08.2021) |

| | | |
|---|---|---|
| О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с ISBN 978-5-8265-1737-6. | | |
| 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 : 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 (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 22 / 20 23 учебный год

Протокол заседания кафедры № 14 от 28.06.22 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

(ФИО, подпись)

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*