

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ

Декан факультета  
Компьютерных технологий  
(наименование факультета)

И.А. Трещёв  
(подпись, ФИО)

« \_\_\_\_ » \_\_\_\_\_ 2023г.

**РАБОЧАЯ ПРОГРАММА ПРАКТИКИ**

Производственная практика (преддипломная практика)

Направление подготовки 10.05.03	"Информационная безопасность автоматизированных систем"
Направленность (профиль) образовательной программы	Анализ безопасности информационных систем

Обеспечивающее подразделение
Кафедра ИБАС – Информационная безопасность автоматизированных систем

Комсомольск-на-Амуре 2023

Разработчик рабочей программы практики:

К.Э.Н., доцент

(должность, степень, ученое звание)

(подпись)

Обласов А.А.

(ФИО)

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой

Кафедра «Информационная безопасность автоматизированных систем»

\_\_\_\_\_ Обласов А.А.

## 1 Общие положения

Рабочая программа практики «Производственная практика (преддипломная практика)» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской Федерации № 1457 от 26.11.2020, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Вид практики	Преддипломная практика
Тип практики	Производственная практика
Цель практики	Выполнить основную часть действий по подготовке и реализации заданий выпускной квалификационной работы (ВКР);
Задачи практики	<p>В процессе прохождения преддипломной практики студент должен:</p> <ul style="list-style-type: none"> <li>• Собрать и проанализировать теоретический материал, необходимый для выполнения ВКР;</li> <li>• Провести разработку алгоритмов, методик, математических и т.п. моделей, необходимых для реализации задания ВКР, при необходимости провести внутренний аудит информационной безопасности предприятия;</li> <li>• Выполнить экспериментальную часть ВКР (если необходимо);</li> <li>• Провести черновое кодирование программного обеспечения по заданию ВКР(если необходимо), разработать рекомендации по обеспечению информационной безопасности на предприятии (если необходимо);</li> </ul> <p>Подготовить отчет по практике в виде тезисов текста первой главы ВКР</p>
Способ проведения практики	Стационарная; выездная

## 2 Перечень планируемых результатов обучения по практике, соотнесенных с индикаторами достижения компетенций

Процесс освоения преддипломной производственной практика на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой:

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по практике
<b>Универсальные</b>		
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода,	УК-1.1 Знает метод системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации УК-1.2 Умеет применять	<i>Знать:</i> метод системного анализа, способы обоснования решения (индукция, дедукция, по аналогии) проблемной ситуации <i>Уметь:</i> применять методики поиска,

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по практике
вырабатывать стратегию действий	методики поиска, сбора и обработки информации; осуществляет оценку адекватности информации о проблемной ситуации путём выявления диалектических и формально-логических противоречий в анализируемой информации УК-1.3 Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации; навыком выбора методов критического анализа, адекватных проблемной ситуации; навыками разработки и обоснования плана действий по решению проблемной ситуации	сбора и обработки информации; осуществляет оценку адекватности информации о проблемной ситуации путём выявления диалектических и формально-логических противоречий в анализируемой информации <i>Владеть:</i> методами поиска, сбора и обработки, критического анализа и синтеза информации; навыком выбора методов критического анализа, адекватных проблемной ситуации; навыками разработки и обоснования плана действий по решению проблемной ситуации
<b>Общепрофессиональные</b>		
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 Знает основные нормативные правовые акты в области защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации ОПК-5.2 Умеет находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью правовых информационных систем; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других	<i>Знать:</i> основные нормативные правовые акты в области защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации <i>Уметь:</i> находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью правовых информационных систем; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов <i>Владеть:</i> навыками использования нормативных актов в профессиональной деятельности.

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по практике
	<p>организационно-распорядительных документов</p> <p>ОПК-5.3 Владеет навыками использования нормативных актов в профессиональной деятельности</p>	
<p>ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>ОПК-6.1 Знает основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p>ОПК-6.2 Умеет применять на практике основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p>ОПК-6.3 Владеет навыками использования нормативных правовых актов, нормативных и методических документов ФСБ, ФСТЭК в области защиты информации ограниченного доступа при решении профессиональных задач</p>	<p><i>Знать:</i> основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p><i>Уметь:</i> применять на практике основные нормативные правовые акты, нормативные и методические документы ФСБ, ФСТЭК в области защиты информации ограниченного доступа</p> <p><i>Владеть:</i> навыками использования нормативных правовых актов, нормативных и методических документов ФСБ, ФСТЭК в области защиты информации ограниченного доступа при решении профессиональных задач</p>
Профессиональные		
<p>ПК-1: Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем</p>	<p>ПК-1.1 Знает структурные и функциональные схемы защищенных автоматизированных систем</p> <p>ПК-1.2 Умеет проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем</p> <p>ПК-1.3 Владеет навыками выявления потенциальных уязвимостей информационной безопасности автоматизированных систем</p>	<p><i>Знать:</i> структурные и функциональные схемы защищенных автоматизированных систем</p> <p><i>Уметь:</i> проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем</p> <p><i>Владеть:</i> навыками выявления потенциальных уязвимостей информационной безопасности автоматизированных систем</p>

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по практике
<p>ПК-2: Способен проводить анализ защищенности информационной инфраструктуры автоматизированной системы</p>	<p>ПК-2.1 Знает способы проведения анализа защищенности информационной инфраструктуры автоматизированных систем  ПК-2.2 Умеет выбирать способ проведения анализа защищенности информационной инфраструктуры автоматизированных систем  ПК-2.3 Владеет навыками проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p>	<p><i>Знать:</i> способы проведения анализа защищенности информационной инфраструктуры автоматизированных систем  <i>Уметь:</i> выбирать способ проведения анализа защищенности информационной инфраструктуры автоматизированных систем  <i>Владеть:</i> навыками проведения анализа защищенности информационной инфраструктуры автоматизированных систем</p>
<p>ПК-3: Способен проводить анализ технической документации информационной инфраструктуры автоматизированной системы</p>	<p>ПК-3.1 Знает методики проведения анализа технической документации информационной инфраструктуры автоматизированной системы  ПК-3.2 Умеет выбрать методику проведения анализа технической документации информационной инфраструктуры автоматизированной системы  ПК-3.3 Владеет навыками проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p>	<p><i>Знать:</i> методики проведения анализа технической документации информационной инфраструктуры автоматизированной системы  <i>Уметь:</i> выбрать методику проведения анализа технической документации информационной инфраструктуры автоматизированной системы  <i>Владеть:</i> навыками проведения анализа технической документации информационной инфраструктуры автоматизированной системы</p>
<p>ПК-4: Способен анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации</p>	<p>ПК-4.1 Знает программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем  ПК-4.2 Умеет выбрать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности инфор-</p>	<p><i>Знать:</i> программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем  <i>Уметь:</i> выбрать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах  <i>Владеть:</i> навыками анализа программных, архитектурно-технических и схемотехнических решений</p>

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по практике
в автоматизированных системах	<p>мации в автоматизированных системах</p> <p>ПК-4.3 Владеет навыками анализа программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах</p>	<p>компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах</p>
<p>ПК-6: Способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов</p>	<p>ПК-6.1 Знает способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p> <p>ПК-6.2 Умеет выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p> <p>ПК-6.3 Владеет навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p>	<p><i>Знать:</i> способы проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p> <p><i>Уметь:</i> выбрать способ проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p> <p><i>Владеть:</i> навыками проектирования подсистем безопасности информации с учетом действующих нормативных и методических документов</p>

### 3 Место практики в структуре образовательной программы

Практика входит в состав блока 2 «Практики» и относится к базовой части.

Место практики (этап формирования компетенции) отражено в схеме формирования компетенций, представленной в документе *Оценочные материалы*, размещенном на сайте университета [www.knastu.ru](http://www.knastu.ru) / *Наш университет* / *Образование* / *Информационная безопасность автоматизированных систем/Оценочные материалы*).

Производственная практика (преддипломная практика) полностью реализуется в форме практической подготовки. Практическая подготовка организуется путем проведения / выполнения индивидуальных практических заданий.

Практическая подготовка реализуется на основе профессионального стандарта утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857.

Обобщенная трудовая функция: Д Формирование требований к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости.

ТД-1 Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите, ТД-3 Планирование мероприятий по обеспечению защиты информации в автоматизированной системе, ТД-3 Определение порядка обработки информации в автоматизированной системе, ТД-4 Определение требуемого класса (уровня) защищенности автоматизированной системы, ТД-5 Анализ информационной инфраструктуры и безопасности информации автоматизированных систем, НЗ-3 Программно-аппаратные средства обеспечения защиты информации автоматизированных систем, НЗ-3 Основные меры по защите информации в автоматизированных системах, НЗ-5 Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем, НЗ-6 Национальные, межгосударственные и международные стандарты в области защиты информации, НЗ-7 Национальные, межгосударственные и международные стандарты в области защиты информации, НЗ-10 Методы защиты информации от несанкционированного доступа и утечки по техническим каналам, НУ-1 Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами, НУ-1 Выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации, НУ-3 Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем, НУ-4 Организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем, НУ-4 Проектировать и реализовывать политику безопасности вычислительных сетей, НУ-5 Выявлять известные уязвимости информационных систем, НУ-5 Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы, НУ-8 Определять эффективность применения средств информатизации.

Анализ требований к профессиональным компетенциям, предъявляемым к выпускникам на рынке труда - Профессиональный стандарт «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 525н. Уровень квалификации 7.

Обобщение отечественного и зарубежного опыта - Профессиональный стандарт «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 525н. Уровень квалификации 7.

Консультации с ведущими работодателями, объединениями работодателей отрасли, в которых востребованы выпускники - Профессиональный стандарт «СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 525н. Уровень квалификации 7.

Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел Квалификационные характеристики должностей специалистов, осуществляющих работы в сфере защиты информации.

Для специалитета

Производственная практика (преддипломная практика)» в рамках воспитательной работы с обучающимися способствует воспитанию самостоятельности личности, точности в работе и ответственности, происходит процесс привлечения студентов к профессиональному труду, сущность которого заключается в приобщении студентов к профессионально-трудовой деятельности и к связанным с ней социальным функциям в соответствии с направлением подготовки и будущим уровнем квалификации. Во время практики формируются сознательное отношение к выбранной профессии, социальная компетентность, навыки



межличностного делового общения, а также такие качества личности, как трудолюбие, рациональность, профессиональная этика, способность принимать решения, умение работать и другие. Происходит знакомство студентов с основами профессии, профессиональным опытом и этикой, повышение уровня адаптации к современному рынку труда.

#### 4 Структура и содержание практики

Практика Производственная практика (преддипломная практика) проводится:

- очная форма обучения - на 4 курсе(ах) в 8 семестре(ах);

Общая трудоемкость практики составляет 6 з.е. 216 акад. час.)

Продолжительность практики 4 недели в соответствии с утвержденным календарным учебным графиком.

Таблица – Структура и содержание практики по разделам (этапам)

Наименование разделов	Содержание раздела (этапа) практики	Форма проведения или контроля	Трудоемкость (в часах)
<b>Раздел 1 Подготовительный этап</b>			
	<i>Оформление документов по прохождению практики</i>	Подготовка приказов, согласование с предприятием,	2
	<i>Оформление временных пропусков для прохода в профильную организацию (при необходимости).</i>	Проведение организационных собраний с группой	1
	<i>Проведение медицинских осмотров (обследований) в случае выполнения обучающимся работ, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры (обследования) в соответствии с законодательством РФ</i>		1
	<i>Вводный инструктаж по правилам охраны труда, технике безопасности, пожарной безопасности, правилам внутреннего распорядка</i>	Лекция	2
<b>Текущий контроль по разделу 1</b>		Собеседование по правилам охраны труда, технике безопасности, пожарной безопасности, правилам внутреннего распорядка	2 часа
<b>Раздел 2 Основной этап</b>			

Наименование разделов	Содержание раздела (этапа) практики	Форма проведения или контроля	Трудоемкость (в часах)
<p><b>Тема 1</b> Подготовительный этап выполнения ВКР</p>	<p>Задание 1. Изучение организационной структуры предприятия, определение места подразделения, занимающегося автоматизацией его деятельности, его взаимосвязей с другими подразделениями и предприятиями. Ознакомление с общим положением предприятия. Провести анализ информационных систем и технологий, используемых на предприятии (в организации), ОТСС и ВТСС</p>	<p>Выполнение индивидуальных заданий практики</p>	<p>25</p>
<p><b>Тема 2</b> Методологические инструменты выполнения ВКР</p>	<p>Задание 2. Изучение электронного и бумажного документооборота. Изучение бизнес-процессов предприятия (организации), выполнить моделирование данных процессов с применением изученных ранее инструментальных средств. Выделить процессы и задачи, требующие автоматизации. Подбор для отчета различных пожеланий конечных пользователей: предложений, запросов, критических замечаний по инструментальным средствам. Выделить процессы и задачи, требующие автоматизации. Подбор для отчета различных пожеланий конечных пользователей: предложений, запросов, критических замечаний.</p> <p>Задание 3. Провести разработку интерфейса пользователя, алгоритмов, методик, инфологических и т.п. моделей, необходимых для реализации подсистемы информационной безопасности предприятия и задания ВКР</p>	<p>Выполнение индивидуальных заданий практики</p>	<p>45</p>

Наименование разделов	Содержание раздела (этапа) практики	Форма проведения или контроля	Трудоемкость (в часах)
<b>Тема 3</b> Разработка\сопровождение подсистемы информационной безопасности предприятия	Задание 4. Разработать, либо модифицировать подсистему информационной безопасности предприятия, с учетом пожеланий со стороны заказчика.	Выполнение индивидуальных заданий практики  Описание подсистемы информационной безопасности предприятия	60
	Задание 5. Разработать рекомендации по модификации подсистемы информационной безопасности предприятия с учетом требований по информационной безопасности актуальных нормативно-технической документации. Провести технико-экономическое обоснование проекта внедрения подсистемы информационной безопасности предприятия		
	<i>Консультации руководителя(-ей) практики о ходе выполнения заданий, оформлении и содержании отчета, по производственным вопросам</i>	Собеседование с обучающимся	4
	<i>Подготовка отчета по практике</i>	Разделы отчета по практике	12
<b>Текущий контроль по разделу 2</b>		Результаты выполненной работы	
<b>Раздел 3 Завершающий этап</b>			
	<i>Проверка отчета по практике, оформление характеристики руководителя(-ей) практики</i>	Отчет по практике, дневник практики	
<b>Текущий контроль по разделу 3</b>	Анализ собранных материалов, составление и оформление отчета по практике	Защита отчета по практике	62
<b>Промежуточная аттестация по практике</b>	<i>Собеседование</i>	Дифференцированный зачет	10
<b>ИКР</b>			

## 5 Формы отчетности по практике

Формами отчетности по практике являются:

1. Дневник по практике, который содержит:
  - ФИО студента, группа, факультет;

- номер и дата выхода приказа на практику;
- сроки прохождения практики;
- ФИО руководителей практики от университета и профильной организации, их должности;
- цель и задание на практику;
- график прохождения практики;
- отзыв о работе студента.

## 2. Отчет обучающегося по практике.

В отчет по практике включаются:

- титульный лист;
- содержание;
- индивидуальное задание;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения (при необходимости).

## 6 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по практике

Фонды оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обсуждаются и утверждаются на заседании кафедры. Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов прохождения практики хранится на кафедре-разработчике в бумажном или электронном виде, также фонды оценочных средств доступны студентам в личном кабинете – раздел учебно-методическое обеспечение.

## 7 Учебно-методическое и информационное обеспечение практики

### 7.1 Основная и дополнительная литература

Перечень рекомендуемой основной и дополнительной литературы представлен на сайте университета [www.knastu.ru](http://www.knastu.ru) / *Наш университет / Образование / Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр литературы*.

### 7.2 Методические указания для студентов по выполнению заданий практики

*Приводится список опубликованных методических указаний по выполнению заданий практики или указывается ссылка на их размещение в электронно-образовательной среде университета, либо методические рекомендации приводятся в п. 8.3 программы практики.*

### 7.3 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по практике

Каждому обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, с которыми у университета заключен договор.

Перечень рекомендуемых профессиональных баз данных и информационных справочных систем представлен на сайте университета [www.knastu.ru](http://www.knastu.ru) / *Наш университет /*

Актуальная информация по заключенным на текущий учебный год договорам приведена на странице Научно-технической библиотеки (НТБ) на сайте университета <https://knastu.ru/page/3244>

#### **7.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения практики**

На странице НТБ можно воспользоваться интернет-ресурсами открытого доступа по укрупненной группе направлений и специальностей (УГНС) 10.05.03 "Информационная безопасность автоматизированных систем":

<https://knastu.ru/page/539>

Название сайта	Электронный адрес
Научная электронная библиотека «Киберленинка»	<a href="http://cyberleninka.ru">http://cyberleninka.ru</a>
Научная электронная библиотека eLIBRARY	<a href="http://elibrary.ru/default.asp">http://elibrary.ru/default.asp</a> ,

### **8 Организационно-педагогические условия**

Организация образовательного процесса регламентируется учебным планом и календарным учебным графиком. Язык обучения (преподавания) - русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на зачёт соответствующих практик, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного прохождения.

Зачёт практики осуществляется при условии, что её вид и продолжительность, указанные в представленных обучающимся документах об образовании, соответствуют учебному плану образовательной программы с учётом направленности (профиля) Анализ безопасности информационных систем

В нижеперечисленных случаях выпускающая кафедра может проводить оценивание (переаттестацию) фактического достижения обучающимся планируемых результатов практики:

- наименование ранее пройденной практики не совпадает с действующим учебным планом, но компетенции по практике совпадают;
- наименование ранее пройденной практики совпадает с действующим учебным планом, но компетенции совпадают частично;
- не совпадает профиль образовательной программы;
- трудоёмкость пройденной практики совпадает с трудоёмкостью практики в действующем учебном плане менее чем на 80 %.

#### **8.1 Образовательные технологии**

В процессе прохождения практики используются следующие технологии:

##### **Стандартные методы обучения:**

- самостоятельная работа обучающихся вне аудитории, в которую включается выполнение заданий практики в соответствии с индивидуальным заданием и рекомендованными источниками литературы;
- освоение методов анализа информации и интерпретации результатов;

– выполнение письменных аналитических и расчетных заданий в рамках практики с использованием рекомендуемых информационных источников (учебники, издания периодической печати, сайты в сети Интернет);

– консультации преподавателя по актуальным вопросам, возникающим у студентов в ходе прохождения практики; методологии выполнения практических заданий, подготовке отчета по практике, выполнению аналитических заданий.

#### **Методы обучения с применением интерактивных форм:**

Для выполнения индивидуального задания и формирования отчета по практике обучающиеся используют широкий арсенал программных продуктов (п. 9.1).

Прохождение практики предполагает использование технологий:

– электронно-библиотечных систем для самостоятельного изучения научной и учебно-методической литературы;

– справочно-правовых систем, в том числе, КонсультантПлюс;

– информационные технологии для сбора, хранения и обработки информации.

### **8.2 Самостоятельная работа обучающихся по практике**

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений, навыков без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета и объекта прохождения практики.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

### **8.3 Методические рекомендации для обучающихся по прохождению практики**

#### **Права и обязанности студентов**

Во время прохождения практики студенты имеют право:

- получать информацию, не раскрывающую коммерческой тайны организации для выполнения программы и индивидуального задания практики;

- с разрешения руководителя организации и руководителей ее структурных подразделений пользоваться информационными ресурсами организации;

- получать компетентную консультацию специалистов организации по вопросам, предусмотренным заданием практики;

- принимать непосредственное участие в профессиональной деятельности организации - базы практики.

**Перед прохождением практики студенты обязаны:**

- ознакомиться с программой прохождения практики и внимательно изучить ее;
- выбрать место прохождения практики и написать заявление;
- оформить дневник практики;
- разработать календарный план прохождения этапов практики.

**Во время прохождения практики студенты обязаны:**

- выполнить программу практики;
- вести дневник практики о характере выполненной работы и достигнутых результатах;
- подчиняться действующим в организации правилам внутреннего распорядка дня;
- соблюдать требования трудовой дисциплины;
- изучить и строго соблюдать правила эксплуатации оборудования, техники безопасности, охраны труда и другие условия работы в организации.

**По окончании практики студенты обязаны:**

- оформить все отчетные документы.

**Порядок ведения дневника**

В соответствии с РИ 7.5-2 «Организация и проведение практик обучающихся» все студенты в обязательном порядке ведут дневники по практике. В дневнике отмечаются: сроки, отдел, участок работы, виды выполненных работ, фиксируется участие студента в различных мероприятиях.

Дневник прохождения производственной практики должен содержать:

- ежедневные записи о выполняемых действиях с указанием даты, фактического содержания и объема действия, названия места выполнения действия, количества дней или часов, использованных на выполнение действия, возможные замечания
- предложения студента-практиканта. После каждого рабочего дня надлежащим образом оформленный дневник представляется студентом-практикантом на подпись непосредственного руководителя практики по месту прохождения практики, который заверяет соответствующие записи своей подписью;

по итогам практики в конце дневника ставится подпись непосредственного руководителя производственной практики, которая, как правило, заверяется печатью.

**Составление отчета по практике**

Отчет по практике выполняется в печатном варианте в соответствии с требованиями РД 013-2016 «Текстовые студенческие работы. Правила оформления» и подшивается в папку (типа «скоросшиватель»). Отчет состоит из: введения, основной части, заключения, списка литературы и приложений.

Введение должно отражать актуальность практики, ее цель и задачи (какие виды практической деятельности и какие умения, навыки планирует приобрести студент) (1,5 - 2 страницы).

Основная часть включает в себя характеристику объекта исследования, сбор и обработку соответствующей статистической, технической, нормативно-правовой и (или) иной информации по предмету исследования, в т.ч. с использованием профессионального программного обеспечения и информационных технологий. По возможности, включаются в отчет и элементы научных исследований. Содержание основной части минимум 11 страниц.

В заключении приводятся общие выводы и предложения, а также краткое описание проделанной работы и даются практические рекомендации.(1,5 - 2 страницы).

Список литературы состоит из нормативно-правовых актов, учебников и учебных пособий, научных статей, использованных в ходе выполнения индивидуального задания.

Приложения помещают после списка литературы в порядке их отсылки или обращения к ним в тексте. В качестве приложений рекомендуется предоставлять копии документов, бланков договоров, организационно-распорядительных документов, аналитических таблиц, иных документов, иллюстрирующих содержание основной части.

По окончании практики в последний рабочий день студенты оформляют и представляют отчет по практике и все необходимые сопроводительные документы.

Отчет и характеристика рассматриваются руководителем практики от кафедры. Отчет предварительно оценивается и допускается к защите после проверки его соответствия требованиям, предъявляемым данными методическими указаниями. Защита отчетов организуется в форме собеседования. По результатам защиты руководитель выставляет общую оценку, в которой отражается качество представленного отчета и уровень подготовки студента к практической деятельности; результаты оцениваются по пятибалльной системе. При неудовлетворительной оценке студент должен повторно пройти практику.

Сданный на кафедру отчет и результат защиты, зафиксированный в ведомости и зачетной книжке студента, служат свидетельством успешного окончания практики.

### **Примеры индивидуальных заданий**

1. Аттестация объекта информатизации на соответствие требованиям по защите информации для (на материалах конкретного предприятия).
2. Исследование ... (наименование технического канала утечки информации) в (на материалах конкретного предприятия).
3. Аттестация ИСПДн класса ...(указание класса) для (на материалах конкретного предприятия).
4. Комплексная система защиты информации (на материалах конкретного предприятия).
5. Выбор СЗИ (на материалах конкретного предприятия).
6. Исследование параметров (наименование технического канала утечки информации) (на материалах конкретного предприятия).
7. Проектирование защищенной автоматизированной системы (на материалах конкретного предприятия).
8. Управление рисками информационной безопасности на предприятии.
9. Разработка программного комплекса для расчета параметров защиты от утечки по каналу (наименование технического канала утечки информации).
10. Совершенствование системы защиты информации в соответствии с актуальными требованиями законодательства.
11. Обеспечение информационной безопасности распределенных информационных систем.
12. Создание и аттестация альтернативной измерительной площадки (на материалах конкретного предприятия).
13. Проектное управление информационной безопасностью.
14. Разработка программных комплексов защиты от НСД.
15. Разработка программно-аппаратных комплексов защиты от НСД.
16. Разработка программно-технических комплексов для удостоверяющих центров.
17. Разработка программного обеспечения для автоматизации процесса аудита информационной безопасности.
18. Разработка программно-технических комплексов для защиты от утечки по (наименование технического канала утечки информации).



19. Разработка системы контроля устранения выявленных в работе по информационной безопасности несоответствий (на материалах конкретного предприятия).
20. Разработка защищенных мобильных приложений.

### **Примеры вопросов (заданий) при проведении промежуточной аттестации**

#### **Тема 1 Подготовительный этап выполнения ВКР**

Вопрос 1. Что мы понимаем под информационными потребностями сотрудников организации (отдела).

Вопрос 2. Состав и характеристики функциональных подсистем

Вопрос 3. Состав проектной документации стадии предпроектного обследования?

Вопрос 4. Методы проведения препроектного обследования.

Вопрос 5. Что включает в себя постановка задачи и предпроектные исследования?

Вопрос 6. Перечислите функциональные и эксплуатационные требования к подсистеме информационной безопасности.

Вопрос 7. Перечислите правила разработки технического задания.

Вопрос 8. Назовите основные разделы технического задания.

#### **Тема 2 Методологические и программные инструменты выполнения ВКР**

Вопрос 1. Методологии и технологии проектирования ИС и систем защиты.

Вопрос 2. Охарактеризуйте архитектуру информационных технологий и архитектуру организации по месту прохождения практики.

Вопрос 3. Различные подходы к классификации моделей.

Вопрос 4. Основные законодательные акты по защите информации.

Вопрос 5. Защита информации ограниченного доступа.

Вопрос 6. Антивирусные средства.

Вопрос 7. Средства защиты от несанкционированного доступа.

Вопрос 8. Межсетевые экраны.

Вопрос 9. Средства криптографической защиты информации.

Вопрос 10. Системы обнаружения и предотвращения вторжений.

Вопрос 11. Атаки на информационные системы.

Вопрос 12. Комплексный подход к обеспечению информационной безопасности.

#### **Тема 3 Разработка\сопровождение подсистемы информационной безопасности**

Вопрос 1. Общая характеристика процесса проектирования

Вопрос 2. Принципы и особенности проектирования интегрированных ИС?

Вопрос 3. Основные задачи и особенности этапа технического проектирования?

Вопрос 4. Этап тестирования. Стадия ввода в эксплуатацию (внедрение)?

Вопрос 5. Структурная модель предметной области

Вопрос 6. Классификация технологий проектирования. Стандарты проектирования

Вопрос 7. Системы экономических показателей которые можно использовать при создании подсистем информационной безопасности

Вопрос 8. Системы документации

Вопрос 9. Системы классификации и кодирования.

Вопрос 10. Понятие информационной безопасности. Основные составляющие.

Вопрос 11. Структура хранилища данных. Основные свойства данных, находящихся в хранилище данных. Защита баз данных

Вопрос 12. Транзакционные и аналитические системы. Откат и фиксация транзакций. Механизм блокировок. Уровни и типы блокировок

Вопрос 13. Требования к компонентам интегрированной системы управления.

Вопрос 14. Требования к совместимости и взаимодействию компонентов интегрированной АИС

## **9 Материально-техническое обеспечение, необходимое для осуществления образовательного процесса по практике**

### **9.1 Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по практике**

Состав программного обеспечения, необходимого для прохождения практики, приведен на сайте университета [www.knastu.ru](http://www.knastu.ru) / *Наш университет / Образование / Информационная безопасность автоматизированных систем / Рабочий учебный план / Реестр ПО.*

Актуальные на текущий учебный год реквизиты / условия использования программного обеспечения приведены на странице ИТ-управления на сайте университета:

<https://knastu.ru/page/1928>

### **9.2 МТО практики**

Практика проводится в структурном подразделении университета и/или учреждениях и организациях, с которыми заключены договора о практической подготовке. Выполнение отчета, подготовка презентационных материалов может осуществляться студентом на базе Университета в аудиториях, библиотеке.

Для реализации программы практики в структурном подразделении ФГБОУ ВО «КНАГУ» используется материально-техническое обеспечение:

Структурное подразделение	Используемое Оборудование / ПО	Назначение оборудования
СКБ ФКТ	Microsoft® Office Professional Plus 2007 Russian	Выполнение индивидуальных заданий
СКБ ФКТ	Microsoft® Windows Professional 7 Russian	Выполнение индивидуальных заданий
СКБ ФКТ	Microsoft® Office Standard 2013 Russian	Выполнение индивидуальных заданий
СКБ ФКТ	Консультант Плюс	Выполнение индивидуальных заданий

Для реализации программы практики «Производственная практика (преддипломная практика)» на базе профильной организации используется материально-техническое обеспечение, указанное в договорах о практической подготовке или договорах о сетевом взаимодействии

## **10 Другие сведения**

### **Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов**

Освоение практики обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.