аМИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
Р.Ю. Демина
«08» июня 2023 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой
информационной безопасности ИБ
Р.Ю. Демина
от «08» июня 2023 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Тип практики	**Преддипломная**
Составитель(-и)	**Гурская Т.Г., доцент, к.т.н., доцент кафедры информационной безопасности**
Направление подготовки / специальность	**10.03.01 Информационная безопасность**
Направленность (профиль) ОПОП	**Организация и технологии защиты информации**
Квалификация (степень)	**бакалавр**
Форма обучения	**Очно-заочная**
Год приема	**2023**
Курс	**5**
Семестр	**9**

Астрахань, 2023

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

1.1. Целью прохождения преддипломной практики является:

подготовка студентов к решению задач комплексного обеспечения информационной безопасности предприятия и к выполнению выпускной квалификационной работы.

1.2. Задачи прохождения преддипломной практики:

– осуществить сбор и подготовку материала для выполнения выпускной квалификационной работы (ВКР), а именно:

- поиск и подбор литературы (учебники, монографии, статьи в периодических изданиях) по теме ВКР;
- всесторонний анализ собранной информации с целью обоснования актуальности темы ВКР, определения целей ВКР, задач и способов их достижения, а также ожидаемого результата ВКР;
- составление технического задания;
- выполнение технического задания (сбор фактических материалов для подготовки ВКР);
- оформление отчета о прохождении студентом преддипломной практики.

2. СПОСОБ И МЕСТА ПРОВЕДЕНИЯ ПРАКТИКИ

2.1. Способ проведения практики – стационарная.

2.4. Места проведения практики.

Прохождение преддипломной практики предполагает направление студентов на предприятия и организации г. Астрахани или Астраханской области, а для иногородних студентов – по месту их проживания, или в структурные подразделения АГУ, в которых решаются производственные задачи, связанные с обеспечением информационной безопасности.

Для организации преддипломной практики АГУ были заключены следующие договоры с предприятиями и организациями:

1. Государственное бюджетное учреждение Астраханской области «Инфраструктурный центр электронного правительства».
2. ООО «Кредитэкспресс Финанс»,
3. ЗАО «БАККА СОФТ»,
4. ПАО «Ростелеком».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ

Процесс прохождения практики направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

профессиональных (ПК):

ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем.

ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации.

ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем.

ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях.

Таблица 1 – Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по практике		
	Знать	Уметь	Владеть
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем	ИПК-1.1. Знать: нормативные правовые акты в области защиты информации, организационные меры по защите информации, программно-аппаратные средства обеспечения защиты информации автоматизированных систем, методы контроля эффективности защиты информации от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах	ИПК 1.2. Уметь: определять источники и причины возникновения инцидентов, устранять нарушения правил разграничения доступа, Применять программные средства обеспечения безопасности данных, осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, использовать криптографические методы и средства защиты информации в автоматизированных системах	ИПК-1.3. Владеть: методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации	ИПК 2.1. Знать: технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие	ИПК 2.2. Уметь: проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, Проводить техническое обслуживание защищенных технических средств обработки информации в	ИПК 2.3. Владеть: методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее

	требованиям безопасности информации	соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.	
ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем	ИПК-3.1. Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы, типовые средства, методы и протоколы идентификации, аутентификации и авторизации основные меры по защите информации в автоматизированных системах, нормативные правовые акты в области защиты информации	ИПК-3.2. Уметь: администрировать программные средства системы защиты информации автоматизированных систем, устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы	ИПК-3.3. Владеть: методикой анализа структурных и функциональных схем защищенной автоматизированной системы
ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях	ИПК 4.1. Знать: источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; принципы функционирования программных средств криптографической защиты информации; виды политик управления доступом и информационными потоками в	ИПК 4.2. Уметь: анализировать угрозы безопасности информации в компьютерных системах и сетях; настраивать правила обработки пакетов в компьютерных сетях; настраивать политики безопасности операционных систем, оценивать угрозы безопасности информации в	ИИПК 4.3. Владеть: навыками управления средствами межсетевого экранирования в компьютерных сетях методикой оценки оптимальности выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

	компьютерных сетях; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации	компьютерных системах и сетях, противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем, настраивать антивирусные средства защиты информации в операционных системах,	

4. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

4.1. Преддипломная практика относится к части, формируемой участниками образовательных отношений.

4.2. Для прохождения данной практики необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами (модулями) и (или) практиками:

1. Безопасность жизнедеятельности.
2. Теория информации.
3. Математическая логика и теория алгоритмов.
4. Аудит информационной безопасности.
5. Методы и средства криптографической защиты информации.
6. Организационное и правовое обеспечение информационной безопасности.
7. Сети и системы передачи информации.
8. Аппаратные средства вычислительной техники.
9. Основы программирования.
10. Экономика.
11. Производственная практика.

В результате освоения этих дисциплин, студент должен получить:

Знания:

- основных экономических категорий и закономерностей, методов анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро и макро-) уровнях, основных понятий экономической и финансовой деятельности отрасли и ее структурных подразделений;
- основных понятий и методов математической логики и теории алгоритмов, теории информации;
- математических методов обработки экспериментальных данных;
- правовых основ организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны;
- правовых норм и стандартов по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
- принципов и методов организационной защиты информации;

- принципов построения криптографических алгоритмов, криптографические стандарты и их использования в информационных системах;
- современных средств разработки и анализа программного обеспечения на языках высокого уровня;
- аппаратных средств вычислительной техники;
- принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- опасных и вредных факторов системы «человек – среда обитания», методов анализа антропогенных опасностей, научные и организационные основы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий.

Умения:

- анализировать и оценивать угрозы информационной безопасности объекта;
- использовать математические методы и модели для решения прикладных задач;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- пользоваться нормативными документами по защите информации;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать степень риска проявления факторов опасности системы «человек – среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности.

Навыки:

- владения методами количественного анализа процессов обработки, поиска и передачи информации;
- владения методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
- выявления и уничтожения компьютерных вирусов;
- работы с нормативными правовыми актами;
- владения методами и средствами выявления угроз безопасности автоматизированным системам;
- организации и обеспечения режима секретности;
- владения методами формирования требований по защите информации;
- владения методами организации и управления деятельностью служб защиты информации на предприятии;
- владения методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- владения профессиональной терминологией;
- безопасного использования технических средств в профессиональной деятельности.

4.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения и навыки, формируемые данной практикой:

1. Бакалаврская работа.

5. ОБЪЕМ И СОДЕРЖАНИЕ ПРАКТИКИ

Объем практики в зачетных единицах (**9 зачетных единиц**) и ее продолжительности в неделях **(6 недель**) составляет 324 академических часа:

Таблица 2.
Структура и содержание практики

№	Раздел (этап) практики	Содержание раздела (этапа)	Код компетенции	Трудо-емкость (в академ. часах)	Формы текущего контроля
1	Подготовительный этап	инструктаж по ТБ, ознакомление с должностными обязанностями стажера	ПК 1, ПК 2, ПК 3, ПК 4	24	дневник преддипломной практики, отзыв-характери-стика, рабочий график (план), отчет
2	Производственный этап	выполнение производственных заданий	ПК 1, ПК 2, ПК 3, ПК 4	100	дневник преддипломной практики, отчет, отзыв-характери-стика, рабочий график (план)
3	Этап обработки и анализа полученной информации	сбор, обработка и систематизация фактического и литературного материала	ПК 1, ПК 2, ПК 3, ПК 4	100	отчет, презентация, дневник преддипломной практики, рабочий график (план)
4	Этап подготовки отчета по практике	оформление отчета	ПК 1, ПК 2, ПК 3, ПК 4	100	отчет, презентация, дневник преддипломной практики, рабочий график (план)

Содержание

Подготовительный этап

Перед началом практики со студентами проводится вводное занятие, на котором студентов знакомят с принципами организации производственной (преддипломной) практики, требованиями к содержанию и оформлению результатов, формой защиты. Также проводятся инструктажи по технике безопасности и охране труда, по пожарной безопасности, заполняются соответствующие журналы. Выдается индивидуальное задание на практику, которое учитывает планируемую тематику ВКР и место практики, составляется рабочий план-график на период практики, до студентов доводится необходимость ведения дневника по практике.

Производственный этап

- знакомство со структурой предприятия, основными задачами и функциями производственной деятельности, нормативно-технической, и правовой документацией, материально-техническим и программным обеспечением производственного процесса и т.п.
- ознакомление с должностными обязанностями практиканта, знакомство с рабочими местами специалистов;

- изучение особенностей охраны труда, техники безопасности, принятых на предприятии, а также техники безопасности при испытаниях и эксплуатации средств защиты информации;
- проведение научно-технических исследований, проектных работ, моделирования, технического обслуживания и т.п.

Сбор и подготовка данных для ВКР

- анализ поставленной задачи и путей их решения по выбранной теме работы;
- аналитический обзор научно-технической и патентной литературы по теме;
- выбор методов проведения исследований;
- подбор нормативно-правовой и научно-технической документации;
- анализ, обработка экспериментальных данных;
- выработка рекомендаций, предложений, разработка проекта в соответствии с темой работы.

Обработка данных и оформление отчета по практике

- составление письменного отчета в соответствие с требованиями ГОСТ, ЕСКД и нормативной документаций вуза. В отчете приводится описание индивидуального задания, способы решения, результаты работы с предоставлением чертежей, технологических карт, распечаток программ и т.п.;
- составление презентации для публичной защиты результатов прохождения практики.

6. ФОРМА ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Итоговая форма контроля по практике – дифференцированный зачет.

Формой отчётности по итогам практики являются:

- Индивидуальное задание студента,
- Отчет,
- Рабочий график (план) проведения практики,
- Дневник преддипломной практики,
- Характеристика на студента или отзыв руководителя практики от предприятия,
- Презентация по результатам выполненной работы.

Главной формой отчетности по итогам практики является отчёт, в котором отражаются все разделы практики. В каждом разделе представлены все материалы, полученные в ходе практики: краткие теоретические вступления, таблицы, рисунки, карты, диаграммы, описательный материал, выводы, рекомендации и т.д.

Аттестация студента проводится на заседании кафедры (конференции), где по результатам защиты отчета по практике выставляется зачет с оценкой.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРАКТИКЕ

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по *преддипломной* практике проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин и прохождением практик, а в процессе прохождения практики – последовательным достижением результатов освоения содержательно связанных между собой разделов (этапов) практики.

Таблица 3 – Соответствие разделов (этапов) практики, результатов обучения по практике и оценочных средств

№ п/п	Контролируемый раздел (этап) практики	Код контролируемой компетенции	Наименование оценочного средства
1	Подготовительный этап	ПК 1, ПК 2, ПК 3, ПК 4	дневник преддипломной практики, отзыв-характеристика, рабочий график (план), отчет
2	Производственный этап	ПК 1, ПК 2, ПК 3, ПК 4	дневник преддипломной практики, отчет, отзыв-характеристика, рабочий график (план)
3	Этап обработки и анализа полученной информации	ПК 1, ПК 2, ПК 3, ПК 4	отчет, презентация, дневник преддипломной практики, рабочий график (план)
4	Этап подготовки отчета по практике	ПК 1, ПК 2, ПК 3, ПК 4	отчет, презентация, дневник преддипломной практики, рабочий график (план)

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Итогом прохождения практики является готовность студентов к выполнению или освоение соответствующего вида профессиональной деятельности. Итогом проверки является однозначное решение (вид профессиональной деятельности освоен / не освоен) и оценка по 5-балльной системе.

Оценка по преддипломной практике выставляется на основании: подготовки и защиты отчета по практике; характеристики профессиональной деятельности студента на практике; дневника практики с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика. При решении комплексной ситуационной задачи можно использовать следующие критерии оценки (Таблица 4).

Таблица 4 – Показатели оценивания результатов обучения по практике

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий по практике, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий по практике, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя

3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетво рительно»	не способен правильно выполнить задания по практике

7.3. Контрольные задания или иные материалы, необходимые для оценки результатов обучения по практике

Наименование оценочного средства - отчет

Структура и порядок оформления отчета (пояснительной записки) результатов преддипломной практики.

Объем отчета не должен превышать 27 – 40 страниц формата А4, оформленных и распечатанных с использованием компьютерных технологий.

В структуре отчета по преддипломной практике должны присутствовать следующие основные разделы:

ВВЕДЕНИЕ
Глава 1 Аналитическая часть
Глава 2 Теоретическая часть
Глава 3 Проектная часть
ЗАКЛЮЧЕНИЕ (ВЫВОДЫ)
ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ, СИМВОЛОВ И ТЕРМИНОВ
СПИСОК ЛИТЕРАТУРЫ
ПРИЛОЖЕНИЯ: программная документация, схемы, результаты математического моделирования, таблицы, графики, материалы на электронном носителе и т.п.

СОДЕРЖАНИЕ – это перечень заголовков глав, пунктов, подпунктов и приложений с указанием номеров страниц, на которых размещается начало материала каждого раздела. Содержание должно быть предельно подробным и включать все заголовки, имеющиеся в пояснительной записке.

Содержание ПЗ размещают на отдельной пронумерованной странице (страницах) после реферата, снабжают ненумерованным заголовком СОДЕРЖАНИЕ и включают в общее количество страниц ПЗ.

В содержание ПЗ включают номера разделов, подразделов, пунктов и подпунктов, имеющих заголовок, их наименование и номера страниц. При наличии в ПЗ приложений в содержание включают номера приложений (например, Приложение А) с их наименованием и номера страниц; а также включают прочие наименования (перечень рисунков, таблиц и т.п.) и номера страниц.

Наименования, включенные в содержание, записывают строчными буквами. Прописными должны печататься заглавные буквы и аббревиатуры.

ВВЕДЕНИЕ во введении должна быть кратко описана область, в которой будет вестись разработка, приводится критический обзор состояния дел в этой области, обосновывается новизна и актуальность темы (работы).

Введение должно содержать:

- развернутую оценку современного состояния решаемой задачи;
- актуальность и новизну темы;
- постановку задачи исследования (проектирования) с указанием цели, используемых методов и средств;
- исходные данные для исследования (разработки);
- планируемые результаты;
- обязанности стажера.

Объем введения 1 – 1,5 страницы.

Заголовок раздела не нумеруется.

ОСНОВНАЯ ЧАСТЬ в общем виде основная часть пояснительной записки должна содержать несколько разделов.

Глава 1 Аналитическая часть

Аналитическая часть отчета может включать:

- анализ системы защиты предприятия;
- анализ современных систем и методик решения аналогичных задач;
- выбор и обоснование модели злоумышленника;
- выбор и обоснование моделей защиты выбранного объекта;
- анализ и систематизация уязвимостей объекта защиты на основе модели угроз;
- описание имеющего на предприятии оборудования, связанного с решением задач преддипломной практики и относящегося к области защиты информации

Аналитическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием главных направлений проектных решений.

Объем аналитической части может составлять 5 – 7 страниц.

Глава 2 Теоретическая часть

Задачами теоретической части являются раскрытие понятий и сущности изучаемых явлений или процессов и обоснование на этой основе мер и методов по обеспечению защиты информации выбранного объекта.

В теоретической части на основе обзора отечественной и зарубежной литературы, достижений в области информатизации и по другим источникам обосновывается выбор применяемых методов, описывается их суть, принципы их использования. Здесь также возможно рассмотреть тенденции развития тех или иных социальных, экономических, информационных процессов на предприятии в результате реализации предлагаемых решений, провести обзор по вопросам обеспечения информационной безопасности по профилю свой деятельности и рассмотреть опыт других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

Для задач, решаемых на основе программно-аппаратной защитой информации объектов, необходимо рассмотреть модели компьютерных систем, модели безопасного взаимодействия и управления безопасностью в информационных системах, модели сетевых средств безопасности, методы декомпозиции моделей угроз, обосновать выбор методов и средств защиты информации выбранного объекта на аппаратном и/или программном уровнях.

Для задач, связанных с защитой и обработкой конфиденциальных документов, необходимо рассмотреть типовой состав технологических стадий входного, выходного и внутреннего документопотоков, провести анализ несанкционированного получения документированной информации, каналов практической реализации возможных угроз, принципов защиты документопотоков, обосновать выбор защищенной технологии и уровень ее автоматизации.

Для задач, решаемых с использованием правового обеспечения защиты информации на предприятиях, в телекоммуникационных и информационных сетях, организациях, а также защиты информации, составляющую государственную, коммерческую и другие тайны, интеллектуальную собственность, должны быть рассмотрены и проанализированы соответствующие законодательные акты, виды, условия и порядок их применения. Должен быть выбран и обоснован комплекс правовых мер и мероприятий, обеспечивающих защиту выбранного объекта.

Для задач, решаемых на основе инженерно-технической защиты информации выбранного объекта, необходимо провести анализ существующих методов, способов и средств его инженерно-технической охраны в соответствии с видами угроз, основ организации и методического обеспечения такой защиты, выбрать и обосновать комплекс организационно-распорядительных мероприятий по защите объекта.

Для задач, решаемых с использованием криптографических систем защиты объектов, необходимо обосновать выбор криптосистем, требования к ним, характеристики, режимы их

применения, определить алгоритмы их реализации в виде блок-схем или пошагового описания, соответствующего языка программирования, рассмотреть модели таких систем с позиций надежности защиты и экономики.

Для задач, решаемых на основе применения организационных мер по защите информации выбранного объекта, необходимо рассмотреть совокупность нормативных и распорядительных документов, определяющих политику информационной безопасности объектов, обладающих конфиденциальной информацией, принципы и задачи ограничения и разграничения доступа к такого рода информации, обосновать необходимость применения такого рода мер, разработать модель их использования.

Для решения задач комплексной защиты информации на предприятии должен быть проведен системный анализ основ защиты информации, должны быть рассмотрены модели комплексной системы защиты информации (КСЗИ): функциональная, информационная, организационная, потенциального нарушителя, на основе которых может быть определен технический и/или рабочий проект организации КСЗИ с технико-экономическим обоснованием. Указанное обоснование необходимо представить в виде аналитического описания или в виде алгоритмической интерпретации. Могут быть описаны средства, обеспечивающие функционирование КСЗИ с учетом различных ситуаций.

На основе теорий различных дисциплин в этом разделе должны быть в рамках бакалаврской работы достаточно подробно описаны алгоритмы, модели, методы, способы, меры, которые после рассмотрения различных альтернатив в конечном итоге должны быть положены в базовую часть проектной части работы.

В теоретической части студент имеет право сделать собственные предложения по развитию, совершенствованию, модернизации, адаптации математических моделей, алгоритмов, аналитических выражений к особенностям рассматриваемых задач, может предложить собственные концепции решения задач, собственные подходы к тем или иным аспектам проблематики.

Теоретическая часть должна заканчиваться выводами по рассмотренным вопросам с обоснованием решений по главным направлениям работы.

Объем теоретической части отчета может составлять 5 – 7 страниц.

Глава 3 Проектная часть

Проектная часть должна содержать материал, соответствующий исключительно конкретным особенностям объекта и задачам разработки. Здесь должны быть представлены рекомендации по дальнейшей реализации технического и/или рабочего проекта, в том числе: можно представить рекомендованные организационные мероприятия и ответственных за их проведение; описать задачи, которые решались в коллективе во время выполнения производственных заданий; описать какие программные средства системного, прикладного и специального назначения можно применять; описать какие инструментальные средства и системы программирования можно использовать для решения профессиональных задач

В отчете необходимо провести предварительный технико-экономический анализ проектных решений, можно провести анализ рисков, представить модель угроз предприятию, рассчитать вероятность возникновения этих угроз и провести оценку потерь от реализации угроз.

Наряду с изложенным, можно оценить улучшение качественных характеристик процесса функционирования предприятия и влияние предлагаемых разработок на эффективность его деятельности.

В отчете может быть дана оценка эффективности внедрения на предприятии проектных предложений по обеспечению информационной безопасности объектов защиты.

В последнем пункте отчета студенту необходимо провести комплексную разработку конкретных вопросов производственной безопасности, безопасности в экстремальных ситуациях, а именно, организации охраны труда на предприятии, участке, рабочем месте; вопросов производственной санитарии и гигиены труда; пожарной профилактики, организация спасательных и аварийных работ.

В данном пункте отчета рекомендуется осветить следующие вопросы:

- идентификация опасных и вредных производственных факторов деятельности человека;
- воздействие производственных факторов на организм человека;
- описание рабочего места, оборудования, выполняемых операций;
- организационные, технические мероприятия по созданию безопасных условий труда;
- обеспечение электробезопасности на производственном участке;
- обеспечение пожаробезопасности на производственном участке.

Проектную часть желательно закончить кратким перечнем основных предложенных в работе проектных решений.

Примерный объем проектной части составляет 20–22 страницы.

В **ЗАКЛЮЧЕНИИ** делаются выводы в соответствии с задачами, которые необходимо было решить в ходе преддипломной практики, дается оценка их выполнения, описываются возможности внедрения результатов преддипломной практики на предприятии и необходимость дальнейшего их развития.

Объем заключения должен составлять 1 – 1,5 страницы.

В **СПИСКЕ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** перечисляются все источники информации, использованные в отчете, и в том числе ссылки на материалы из сети Internet, а также зарубежные источники

Список наименований должен содержать не менее 15 источников. При оформлении библиографического описания источников в списке необходимо руководствоваться ГОСТ Р 7.0.5-2008.

В **ПРИЛОЖЕНИИ** размещены материалы, которые носят вспомогательный, поясняющий характер или имеющие большой объем (документы, используемые в организации по рассматриваемым вопросам, тексты программ, примеры распечаток полученных результатов, табличный и иллюстративный материалы по отдельным показателям или по интегрированным оценкам, которые использованы в качестве дополнительной аргументации, более подробные блок-схемы по отдельным частям разработанных программ).

В приложения следует выносить вспомогательный материал, который более детально раскрывает смысл основных разделов, но при включении его в основной текст приведет к необоснованному увеличению объема выпускной работы.

Объем приложения не лимитируется.

Все приложения нумеруются и располагаются в конце пояснительной записки в порядке ссылок на них. Каждое приложение начинается с новой страницы и имеет содержательный заголовок. При необходимости текст приложения может быть разбит на разделы, подразделы, пункты и подпункты, которые следует нумеровать в пределах каждого приложения в соответствии с требованиями для основной части записки. Программная документация, выносимая в приложения ВКР, должна оформляться в соответствии с требованиями ЕСПД.

2. ***Наименование оценочного средства – дневник преддипломной практики.***

Титульный лист и содержание дневника преддипломной практики приведены в Приложении Д.

Разделы дневника должны быть заполнены в соответствии с индивидуальным заданием.

3. ***Наименование оценочного средства – рабочий график (план) проведения практики.*** В нем должны быть отражены по дням недели выполняемые задания и полученный результат**.** Шаблон приведен в Приложении В, Г.

4. Наименование оценочного средства – отзыв-характеристика (Приложение Е). В нем должны быть отражены основные знания и умения, которые приобрел за время прохождения практики студент, а также руководителем практики должны быть выставлена оценка.

5. Наименование оценочного средства – презентация. Презентация должны содержать следующие элементы:

- Титульный лист с указанием названия практики, сроков ее прохождения, Ф.И.О. студента и группы, Ф.И.О. руководителя практики, его должности.
- Актуальность темы, выбранной для прохождения практики.
- Цель и задачи практики.
- Описание организации, места прохождения практики.
- Анализ системы защиты предприятия.
- Анализ и систематизация уязвимостей объекта защиты на основе модели угроз.
- Обоснование мер и методов по обеспечению защиты информации выбранного объекта.
- Рекомендации по внедрению разработанных мер и методов защиты информации и оценке эффективности его результатов.
- Организация труда и техники безопасности на предприятии.

7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по практике

Отчет по практике должен включать в себя следующие элементы, которые характеризуют формирование компетенций:

- анализ имеющейся системы защиты информации с указанием выявленных недостатков;
- построение частной модели угроз предприятия;
- составление таблицы с расчетом вероятности угроз предприятию;
- обоснование рекомендаций по улучшению существующей системы защиты информации;
- сравнительный анализ предлагаемых технических решений;
- описание особенностей охраны труда и правил техники безопасности на предприятии;
- подбор нормативно-правовой, научно-технической документации, оформленной в соответствии с ГОСТ.

Оценка по преддипломной практике выставляется на основании:

- подготовки и публичной защиты отчета по практике,
- отзыва-характеристики профессиональной деятельности студента во время прохождения преддипломной практики,
- дневника практики с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика,
- календарного плана-графика прохождения практики.

Оценка по практике осуществляется в соответствии с разработанными критериями:

Критерии	Оценка
Студент владеет освоенными в процессе прохождения практики компетенциями в полном объеме, может доступно излагать материал отчета, приводит примеры по объекту практики. Отчет раскрывает основные критические пункты программы практики и индивидуального задания. Электронная презентация визуально оформлена интересно, с использованием доступных грамотных схем. Текст доступен для восприятия слушателем. Студент ответил на все вопросы, допустил не более 1 ошибки в ответе.	отлично

Студент владеет основными освоенными в процессе прохождения практики компетенциями, может доступно излагать материал отчета, примеры по объекту практики отсутствуют. Отчет раскрывает основные критические пункты программы практики и индивидуального задания не в полном объеме. Электронная презентация визуально оформлена в основном в форме текста, без графического и табличного представления. Текст доступен для восприятия слушателем. Студент ответил на все вопросы, допустил более 1, но менее 3 ошибок.	хорошо
Студент слабо освоил необходимые компетенции, материал отчета изложен не логично, примеры по объекту практики отсутствуют. Отчет не раскрывает основные критические пункты программы практики и индивидуального задания. Электронная презентация визуально оформлена в основном в форме текста, без графического и табличного представления. Текст плохо доступен для восприятия слушателем. Студент ответил не на все вопросы, но в тех, на которые дал ответ, не допустил ошибки.	удовлетворительно
Студент не освоил необходимые компетенции, материал отчета изложен не логично, примеры по объекту практики отсутствуют. Отчет не раскрывает критические пункты программы практики, оформлен не в соответствии с требованиями. Электронная презентация визуально оформлена не интересно, в основном в форме текста и не соответствует программы практики и индивидуальному заданию. Текст презентации плохо доступен для восприятия слушателем. Студент ответил не на все вопросы, допустил более 5 ошибок.	Неудовлетворительно

Таблица 5 – Технологическая карта рейтинговых баллов по практике

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Текущая работа				
1.	Дневник практики	1/25	25	По расписанию
2.	План (график)	1/25	25	
Всего			**50**	-
Качество отчёта и его защита				
3.	Отчет	1/25	25	По расписанию
4.	Презентация	1/25	25	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 6 – Система штрафов

Показатель	Балл
Опоздание	-1
Нарушение учебной дисциплины	-1
Неготовность к выполнению задания на практике	-1

Показатель	Балл
Пропуск одного дня практики без уважительной причины	-1

Таблица 7 – Шкала перевода рейтинговых баллов в итоговую оценку по практике

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

В зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

8.1. Основная литература:

1. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202749.html (ЭБС «Консультант студента»).
2. Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 5. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202756.html (ЭБС «Консультант студента»).
3. Управление рисками информационной безопасности: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 2. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202725.html (ЭБС «Консультант студента»).
4. Концептуальные основы создания и применения системы защиты объектов / Ворона В.А., Тихонов В.А. - Вып. 1. - М. : Горячая линия - Телеком, 2012. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202404.html
5. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202336.html6(ЭБС «Консультант студента»).
6. Инженерно-техническая и пожарная защита объектов [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 4. - М. : Горячая линия - Телеком, 2012. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991201797.html (ЭБС «Консультант студента»).
7. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература:

1. Мельников, В.П. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб. пособия для студентов вузов, обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников,

Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ; стер. - М. : Академия, 2009. - 336 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-6150-4 : 306-46. (19 экз.)
2. ГОСТ 19.701-90 ЕСПД ГОСТ 2.125-88 Правила выполнения конструкторских документов. Сб. ГОСТов. - М.: Стандартинформ, 2010
3. ГОСТ 2.105-95 ЕСКД. Основные требования к текстовым документам. Сб. ГОСТов. - М.: Стандартинформ, 2011.
4. ГОСТ 2.004-88 ЕСКД. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ. Сб. ГОСТов. - М.: Стандартинформ, 2011.
5. ГОСТ Р 7.05-2008 Библиографическая ссылка. СИБИД, М.: Стандартинформ, 2008.
6. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745181.html (ЭБС «Консультант студента»).
7. Ермаков, С.Л. Экономика : рек. УМО по образованию в области экономики и экон. теории в качестве учеб. пособия для неэкон. направлений бакалавриата. - М. : КНОРУС, 2013. - 272 с. - (Бакалавриат). - ISBN 978-5-406-02606-9: 352-00 : 352-00. (10 экз.)
8. Информационная безопасность и защита информации / Шаньгин В.Ф. - М: ДМК Пресс, 2014. - URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).
9. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - URL: http://www.studentlibrary.ru/book/ISBN9785940745181.html (ЭБС «Консультант студента»).
10. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / Коваленко Ю.И. - М. : Горячая линия - Телеком, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785991202619.html (ЭБС «Консультант студента»).

8.3. Интернет-ресурсы, необходимые в процессе прохождения практики

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

При реализации различных видов работ по практике могут использоваться электронное обучение и дистанционные образовательные технологии.

9.1. Информационные технологии

Информационные технологии, используемые при реализации различных видов учебной и внеучебной работы:

- использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));
- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;
- использование возможностей электронной почты преподавателя;
- использование средств представления учебной информации (электронных учебных пособий и практикумов, презентаций и т.д.);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные

ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

- использование виртуальной обучающей среды (или системы управления обучением LMS Moodle) или иных информационных систем, сервисов и мессенджеров.

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии: виртуальная обучающая среда (LMS Moodle «Электронное образование») или иные информационные системы, сервисы и мессенджеры.

9.2. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

9.2.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда

9.2.2. Современные профессиональные базы данных и информационные справочные системы

- Справочная правовая система Консультант Плюс http://www.consultant.ru,
- Информационно – правовое обеспечение «Система ГАРАНТ» http://garant-astrakhan.ru,
- специализированное ПО, установленное на конкретном производстве.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Материально-техническое обеспечение практики должно быть достаточным для достижения целей практики и должно соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.

Студентам должна быть обеспечена возможность доступа к информации, необходимой для выполнения задания по практике и написанию отчета.

Организации, учреждения и предприятия, а также учебно-научные подразделения Университета должны обеспечить рабочее место студента компьютерным оборудованием в объемах, достаточных для достижения целей практики.

Список основного оборудования, установленного в лабораториях программно-аппаратных средств обеспечения информационной безопасности и технической защиты информации Астраханского государственного университета:

1. Детектор атак. Платформа IPC-25*NFR АПКШ «Континент» 3.7.
2. Сервер доступа «Континент» АПКШ 3.7. ЦУС-платформа IPC-25 (4 порта).
3. Межсетевой экран Cisco ASA 5512-X with SW.6GE Data 1GE Mgmt.AC.DES.
4. Учебно-методический комплекс ViPNet "Программно-аппаратная защита информации":
5. Учебное пособие - Система защиты информации ViPNet (курс лекций)
6. Учебное пособие - Система защиты информации ViPNet (практикум)
7. Учебное пособие - Программно-аппаратные комплексы ViPNet (практикум)
8. Учебное пособие - Технология построения виртуальных защищенных сетей ViPNet Windows&Linux (практикум)
9. CD-диск (содержащий программное обеспечение и лицензии предназначенный для проведения лабораторных работ, дополнительные материалы)
10. Программно-аппаратный комплекс ViPNet Coordinator HW1000.
11. Программно-аппаратный комплекс ViPNet Coordinator HW100C.
12. TrustAccess для защиты 1 сервера.
13. TrustAccess для защиты 1 рабочей станции.
14. Комплекс программно-аппаратный «Соболь» (версия 3.0), PCI (NFR-образец).
15. Комплекс программно-аппаратный «Соболь» (версия 3.0), PCI-E (NFR-образец).
16. Средство защиты информации SecretNet 7. Клиент (автономный).
17. OSC5000 deLuxe-спектральный коррелятор
18. SI-2060 – устройство защиты телефонной линии
19. SI-3001 – шумогенератор виброакустический
20. SI-4000 – программно-аппаратный комплекс
21. SP-41/C – шумогенератор сетевой
22. ST 006 – детектор поля
23. ST-031 «Пиранья» – поисковый комплекс
24. Гром ЗИ 4 шумогенератор
25. Кобра защита проводных линий
26. КРЦ-3 – шумогенератор
27. Онега-23М – нелинейный локатор импульсный
28. УЛАН – проверочное устройство проводных линий
29. ФСП-1Ф-7А сетевой фильтр
30. OMS-2000 – акустический излучатель Cisco Packet Tracer

Оборудование, необходимое для прохождения практики на предприятиях г. Астрахани и области зависит от тематики бакалаврской работы.

Программа практики при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание программы практики может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

ПРИЛОЖЕНИЕ А
Образец оформления титульного листа отчета

МИНОБРНАУКИ РОССИИ
АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. В.Н. ТАТИЩЕВА

Кафедра информационной безопасности

ОТЧЕТ
о прохождении производственной (преддипломной) практики
название вида практики

в _____
(наименование профильной организации)

студента (ки)_____ курса___ группы_____ отделения_____факультета_____

_____
(фамилия, имя, отчество)

Сроки проведения практики с «____» _____ по «____» _____ 20__г.

Оценка_____

Руководитель практики от кафедры _____ _____
подпись *ФИО, должность*

«_____» _____ 20___ г.

Астрахань - 20_

ПРИЛОЖЕНИЕ Б
Образец оформления Задания на преддипломную практику

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. В.Н. ТАТИЩЕВА

Кафедра информационной безопасности

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ ОБУЧАЮЩЕГОСЯ
на производственную (преддипломную) практику

Обучающийся_____ курса_____ группы_____формы обучения_____
факультета _____

_____*(ф*
амилия, имя, отчество)

Место прохождения практики: _____
(полное наименование профильной организации)

Адрес профильной организации: _____
(указывается фактический адрес)

Срок прохождения практики с «___» _____ 20___ г. по «____» _____ 20___ г.

Задание:
1) провести анализ имеющейся системы защиты информации предприятия;
2) обосновать меры и методы по обеспечению защиты информации предприятия;
3) разработать рекомендации по внедрению проекта и оценке эффективности его результатов;
4) рассмотреть организацию охраны труда и техники безопасности на предприятии.

_____

Обязанности обучающегося при прохождении практики:

_____
_____
_____

Планируемые результаты практики:

_____
_____

систематизация и обобщение материала для написания ВКР;
публичная защита своих выводов и отчета по практике.

Руководитель практики
от университета _____ _____
подпись *ФИО, должность*
«_____»_____20__г.

Согласовано:
Руководитель практики
от профильной организации _____ _____
подпись *ФИО, должность*
«_____»_____20__г.

Задание принято к исполнению: _____ _____
подпись обучающегося *ФИО обучающегося*
«_____»_____20__г.
дата получения задания

ПРИЛОЖЕНИЕ В
Образец оформления календарного плана-графика

Образец оформления графика (плана) для студентов, проходящих практику в профильных организациях

Совместный рабочий график (план) проведения практики

Направление подготовки 10.03.01 Информационная безопасность
Профиль подготовки Организация и технологии защиты информации
Форма обучения очная
Курс 4

Наименование профильной организации _____

Структурное подразделение _____

Сроки проведения практики с «____» _____20___г. по «____» _____20___г.

Планируемые работы

_____

(по преддипломной практике)

№ п/п	Содержание работы**	Сроки выполнения	Форма отчётности	Отметка руководителя от организации о выполнении
1.	Оформление документов по прохождению практики		Индивидуальное задание на практику, договор, приказ о направлении на практику, предписание	
2.	Организационное собрание (установочная конференция)		Проведение вводного инструктажа	
8.	Итоговая отчётная конференция		Отчеты. Ведомость	

**Содержание работы определяется руководителями практики

Руководитель практики от университета _____ _____
подпись *ФИО, должность*

Руководитель практики от профильной организации _____ _____
подпись *ФИО, должность*

Дата составления:
«_____»_____20____г.

ПРИЛОЖЕНИЕ Г
Образец оформления графика (плана) для студентов, проходящих практику в университете)

Рабочий график (план) проведения практики

Направление подготовки 10.03.01
Информационная безопасность
Профиль подготовки Организация и технологии защиты информации
Форма обучения очная
Курс 4

ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева»

Структурное подразделение
_____

Сроки проведения практики с «____» _____20___г. по «____» _____20___г.

Вид практики производственная (тип – преддипломная)

№ п/п	Дата/Неделя прохождения практики	Формы прохождения практики (мероприятия, задания, поручения)	Результат
1.	1 неделя	Ознакомление с программой практики, получение индивидуального задания, совместного графика (плана) проведения практики. Решение организационных вопросов.	Опрос
2.	1 неделя	Прохождение инструктажа и ознакомление с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка.	Опрос
…..			
5.	2 неделя	Анализ итогов работы в ходе проведения практики. Подготовка к прохождению и прохождение промежуточной аттестации.	Итоговая отчётная конференция

Руководитель (и) практики
от университета _____ _____
подпись *ФИО, должность*

Ознакомлен (ны):

_____ _____
подпись *ФИО обучающегося*

Дата:
«____» _____20___г.

ПРИЛОЖЕНИЕ Д
Образец оформления титульного листа Дневника

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В.Н. Татищева»

Факультет цифровых технологий и кибербезопасности
Кафедра информационной безопасности

ДНЕВНИК
по производственной практике
обучающегося 4 курса ЗИ 41 группы очной формы обучения
направление подготовки/(специальность) 10.03.01 Информационная безопасность
шифр, наименование

_____
фамилия, имя, отчество обучающегося

Место проведения практики:
_____
наименование профильной организации

Адрес профильной организации:
_____

Начало практики «____».____20____г.
Окончание практики «____».____20____г.

Руководитель практики от университета:
_____

Руководитель практики от профильной организации:
_____

Астрахань-20__

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ - КОМПЕТЕНЦИЯМИ

Планируемые результаты освоения образовательной программы (компетенции), формируемые в рамках производственной практики	**Индикаторы достижения компетенций**	**Планируемые результаты обучения при прохождении производственной практики** (*имеются в виду освоенные умения и приобретенный практический опыт*)
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем	ИПК-1.1.	Обучающийся, прошедший производственную практику, будет: **знать:** нормативные правовые акты в области защиты информации, организационные меры по защите информации, программно-аппаратные средства обеспечения защиты информации автоматизированных систем, методы контроля эффективности защиты информации от утечки по техническим каналам, основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах
	ИПК 1.2.	**уметь:** определять источники и причины возникновения инцидентов, устранять нарушения правил разграничения доступа, Применять программные средства обеспечения безопасности данных, осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, использовать криптографические методы и средства защиты информации в автоматизированных системах
	ИПК-1.3.	**владеть:** методикой оценки последствий выявленных инцидентов и обнаружения нарушения правил разграничения доступа
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации	ИПК 2.1.	Обучающийся, прошедший производственную практику, будет: **знать:** технические описания и инструкции по эксплуатации технических средств обработки информации в защищенном исполнении, методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий, порядок аттестации объектов информатизации на соответствие требованиям
	ИПК 2.2.	**уметь:** проводить настройку защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами, Проводить техническое обслуживание

		защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-технической документацией.
	ИПК 2.3.	**владеть:** методами защиты информации от несанкционированного доступа и специальных программных воздействий на нее
ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем	ИПК-3.1.	Обучающийся, прошедший производственную практику, будет: **знать:** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы, типовые средства, методы и протоколы идентификации, аутентификации и авторизации основные меры по защите информации в автоматизированных системах, нормативные правовые акты в области защиты информации
	ИПК-3.2.	**уметь:** администрировать программные средства системы защиты информации автоматизированных систем, устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации, определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы
	ИПК-3.3.	**владеть:** методикой анализа структурных и функциональных схем защищенной автоматизированной системы
ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях	ИПК 4.1.	Обучающийся, прошедший производственную практику, будет: **знать:** источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; принципы функционирования программных средств криптографической защиты информации; виды политик управления доступом и информационными потоками в компьютерных сетях; требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; принципы работы и правила эксплуатации программно-аппаратных средств защиты информации
	ИПК 4.2.	**уметь:** анализировать угрозы безопасности информации в компьютерных системах и сетях; настраивать правила обработки

		пакетов в компьютерных сетях; настраивать политики безопасности операционных систем, оценивать угрозы безопасности информации в компьютерных системах и сетях, противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем, настраивать антивирусные средства защиты информации в операционных системах
	ИИПК 4.3.	**владеть:** навыками управления средствами межсетевого экранирования в компьютерных сетях методикой оценки оптимальности выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах

Примечание: Планируемые результаты обучения при прохождении практики должны быть прописаны в строгом соответствии с программой практики и учебным планом

2. ИНСТРУКТАЖ

Инструктаж по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности и правилами внутреннего трудового распорядка:

1. Инструктаж в АГУ им. В.Н. Татищева

Провёл
Ответственный от АГУ им. В.Н. Татищева
_____ / _____
(подпись) *(Ф.И.О)*

Дата «____» _____» 20____г.

Ознакомлен
Обучающийся
_____ / _____
(подпись) *(Ф.И.О)*

Дата «____» _____» 20____г.

2. Инструктаж в профильной организации

Провёл
Ответственный от профильной организации
_____ / _____
(подпись) *(Ф.И.О)*

Дата «____» _____» 20____г.

Ознакомлен
Обучающийся
_____ / _____
(подпись) *(Ф.И.О)*

Дата «____» _____» 20____г.

3. ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

Краткое содержание индивидуального задания	Отметка о выполнении

СОГЛАСОВАНО:

Руководитель практики от университета
_____ (ФИО, должность)

Руководитель практики от профильной организации
_____ (ФИО, должность)

4. ХОД ПРАКТИКИ

№	Дата	Вид работы	Краткое содержание работы	Примечания, наблюдения, анализ выполненной работы
1.				
2.				

5. АТТЕСТАЦИОННЫЙ ЛИСТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

(заполняется руководителем практики от организации)

Обучающийся _____
прошел (ла)_____практику _____
в организации _____

Виды выполненных работ	**Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой осуществлялась практика**		
	5	4	3

Руководитель практики от профильной организации:_____ (_____)
подпись *ФИО*

Дата «____» _____» 20____г.

6. ОТЗЫВ РУКОВОДИТЕЛЯ ПРАКТИКИ ОТ АГУ ИМ. В.Н. ТАТИЩЕВА

Освоенные в результате производственной практики индикаторы достижения компетенций (в соответствии с выполненными практическими заданиями)	**Уровень освоения компетенций**		
	5	**4**	**3**
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации в процессе эксплуатации автоматизированных систем			
ПК-2. Способен выполнять работы по установке, настройке и техническому обслуживанию защищенных технических средств обработки информации			
ПК-3. Способен осуществлять внедрение систем защиты информации для обеспечения информационной безопасности автоматизированных систем			
ПК-4. Способен администрировать средства защиты информации в компьютерных системах и сетях			

Руководитель практики от университета:_____ (_____)
подпись *ФИО*

Дата «____» _____» 20____г.

ПРИЛОЖЕНИЕ Е
Примерный образец Отзыва-характеристики по практике студента

ОТЗЫВ-ХАРАКТЕРИСТИКА
о прохождении производственной (преддипломной) практики

на студента _____ _____курса _____группы
(фамилия, имя, отчество)
_____очной_формы обучения_____

направления подготовки 10.03.01 Информационная безопасность

Профиль подготовки Организация и технологии защиты информации

_____

Место практики _____
(наименование предприятия, структурного подразделения)

Студент выполнил задания программы практики _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Дополнительно ознакомился/изучил
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Заслуживает оценки _____

Руководитель практики от профильной организации

_____
«____» _____20 ___ г.