

МИНОБРНАУКИ 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
Р.Ю. Демина

« 08 » июня 2023 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Тип практики	ТЕХНОЛОГИЧЕСКАЯ
Составитель(и)	Черкасова В.А., доцент, к.ф.-м.н., доцент кафедры прикладной математики и информатики; Гурская Т.Г., доцент, к.т.н., доцент кафедры и информационной безопасности;
Направление подготовки / специальность	10.03.01 ИНФОРМАЦИОННАЯ
Направленность (профиль) / специализация ОПОП	БЕЗОПАСНОСТЬ «Организация и технологии защиты информации (в сфере информационных и коммуникационных технологий)»
Квалификация (степень)	бакалавр
Форма обучения	Очно-заочная
Год приёма	2023
Курс	3
Семестр	6

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

1. **Целью прохождения производственной практики** является подготовка студентов к решению задач комплексного обеспечения информационной безопасности предприятия (в соответствии с индивидуальным заданием).
2. **Задачи прохождения производственной практики:**
 - приобрести практические навыки по организации защиты информации на объектах практики;
 - ознакомиться с используемыми на объектах практики программными и техническими средствами защиты информации;
 - применить к объекту практики знания нормативных документов, обеспечить установку и настройку технических, программно-аппаратных средств защиты информации, разработать соответствующую документацию;
 - оформить отчет о прохождении студентом производственной (технологической) практики.

2. МЕСТА ПРОВЕДЕНИЯ ПРАКТИКИ

2.2. Места проведения практики.

Прохождение производственной 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 производственной практики АГУ им. В.Н. Татищева 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».

Несколько студентов планируется направить в подразделения и отделы АГУ им. В.Н. Татищева.

Местом проведения практики могут являться структурные подразделения университета.

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:

Общепрофессиональные (ОПК):

ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.

ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности.

ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности.

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.

ОПК-7. Способен использовать языки программирования и технологии разработки

программных средств для решения задач профессиональной деятельности.

ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ОПК-2.2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.

ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами.

Таблица 1. Декомпозиция результатов обучения

Код компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
<i>ОПК-2.</i>	<i>ОПК-2.</i> Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.	<i>ОПК-2.1.</i> Знать: современные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности.	<i>ОПК-2.2.</i> Уметь: выбирать информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности.	<i>ОПК-2.3.</i> Владеть: навыками применения современных информационно-коммуникационных технологий, программных средств системного и прикладного назначения, в том числе отечественного производства, при решении задач профессиональной деятельности.
<i>ОПК-3.</i>	<i>ОПК-3.</i> Способен использовать необходимые математические методы для решения задач профессиональной деятельности.	<i>ОПК-3.1.</i> Знать: основы математики, основные математические методы.	<i>ОПК-3.2.</i> Уметь: решать стандартные профессиональные задачи с применением методов математического анализа и моделирования.	<i>ОПК-3.3.</i> Владеть: навыками математического исследования объектов профессиональной деятельности.
<i>ОПК-4.</i>	<i>ОПК-4.</i> Способен применять необходимые физические законы и модели для решения	<i>ОПК-4.1.</i> Знать: основы физики.	<i>ОПК-4.2.</i> Уметь: решать стандартные профессиональные задачи с применением	<i>ОПК-4.3.</i> Владеть: навыками теоретического и экспериментального физического исследования

Код компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
	задач профессиональной деятельности.		физических законов и моделей.	объектов профессиональной деятельности.
<i>ОПК-5.</i>	<i>ОПК-5.</i> Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.	ОПК-5.1. Знать: основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОПК-5.2. Уметь: применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.	ОПК-5.3. Владеть: навыками работы с нормативными правовыми актами, нормативными и методическими документами, регламентирующими деятельность по защите информации в сфере профессиональной деятельности.
<i>ОПК-7.</i>	<i>ОПК-7.</i> Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности.	ОПК-7.1. Знать: основы программирования.	ОПК-7.2. Уметь: использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности.	ОПК-7.3. Владеть: навыками программирования для решения задач профессиональной деятельности.
<i>ОПК-11.</i>	<i>ОПК-11.</i> Способен проводить эксперименты по заданной методике и обработку их результатов.	ОПК-11.1. Знать: методику проведения экспериментов.	ОПК-11.2. Уметь: уметь решать задачи вычислительного и теоретического характера, проводить эксперименты.	ОПК-11.3. Владеть: методами корректной оценки погрешностей измерений и расчетов
<i>ОПК-12.</i>	<i>ОПК-12.</i> Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты	ОПК-12.1. Знать: основные исходные данные для проектирования подсистем.	ОПК-12.2. Уметь: проводить экспериментальные исследования и проектировать подсистемы и средств обеспечения защиты информации.	ОПК-12.3. Владеть: методами технико-экономического обоснования соответствующих проектных решений.

Код компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по практике (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
	информации и для технико-экономического обоснования соответствующих проектных решений.			
<i>ОПК-2.2.</i>	<i>ОПК-2.2.</i> Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.	ОПК-2.2.1. Знать: структуру и функциональные процессы объекта защиты и его информационные составляющие	ОПК-2.2.2. Уметь: формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.3. Владеть: методами повышения их устойчивости к деструктивным воздействиям на информационные ресурсы
<i>ОПК-2.4.</i>	<i>ОПК-2.4.</i> Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами.	ОПК-2.4.1. Знать: нормативные документы и особенности проведения аудита защищенности объекта информатизации	ОПК-2.4.2. Уметь: проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-2.4.3. Владеть: методикой проведения аудита защищенности объекта информатизации

4. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

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

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

1. Безопасность жизнедеятельности.
2. Математика (продвинутый уровень).
3. Основы программирования.

4. Документоведение.
5. Основы информационной безопасности.
6. Аппаратные средства вычислительной техники.

В результате освоения этих дисциплин, студент должен получить:

Знания:

- 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;
- современных средств разработки и анализа программного обеспечения на языках высокого уровня;
- аппаратных средств вычислительной техники;
- стандартов по оформлению документации; опасных и вредных факторов системы «человек – среда обитания», методов анализа антропогенных опасностей, научных и организационных основ 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;
- разрабатывать документы в соответствии со стандартами;
- 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 навыками выявления и уничтожения компьютерных вирусов;
- владения методами формирования требований по защите информации;
- владения профессиональной терминологией;
- безопасного использования технических средств в профессиональной деятельности.

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

1. Проектирование и эксплуатация защищённых информационных систем;
2. Проектирование инженерно-технической защиты информации;
3. Защита информационных процессов в компьютерных системах;
4. Комплексное обеспечение защиты информации объекта информатизации;
5. Производственная (преддипломная) практика.

5. ОБЪЁМ И СОДЕРЖАНИЕ ПРАКТИКИ

Объём практики составляет 3 зачётных(ые) единиц(ы), продолжительность – 2 недели.

Таблица 2. Структура и содержание практики

Раздел (этап) практики	Содержание раздела (этапа)	Код компетенции	Трудоёмкость (в академ. часах)	Форма текущего контроля
Подготовительный этап	инструктаж по ТБ, ознакомление с	ОПК-2, ОПК-3, ОПК-4,	27	дневник производственной

Раздел (этап) практики	Содержание раздела (этапа)	Код компетенции	Трудоёмкость (в академ. часах)	Форма текущего контроля
	должностными обязанностями стажера	ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4		практики, отзывы-характеристики а, рабочий график (план), отчет
Производственный этап	выполнение производственных заданий	ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4	27	дневник производственной практики, отчет, отзывы-характеристики а, рабочий график (план)
Этап обработки и анализа полученной информации	сбор, обработка и систематизация фактического и литературного материала	ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4	27	отчет, презентация, дневник производственной практики
Этап подготовки отчета по практике	оформление отчета	ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4	27	отчет, презентация, дневник производственной практики

Содержание

Подготовительный этап

Перед началом практики со студентами проводится вводное занятие, на котором студентов знакомят с принципами организации производственной (технологической) 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, составляется рабочий план-график на период практики, до студентов доводится необходимость ведения дневника по практике.

Определение роли и места выбранной темы выпускной квалификационной работы в производственной, эксплуатационной и инвестиционной (научной) работе организации или сферы информационной безопасности.

Производственный этап

Сбор и анализ информации об организационной структуре предприятия, сфере его деятельности.

Анализ применяемых на предприятии проектных решений, касающихся темы выпускной квалификационной работы.

Аналитический обзор правовой базы и научно-технической литературы по теме выпускной квалификационной работы.

Подбор или разработка проектных решений, направленных на повышение защищенности предприятия.

Этап обработки и анализа полученной информации

Разработка соответствующей документации, регламентирующей внедрение предлагаемых решений. Оценка эффективности предложенных решений. Выработка рекомендаций, предложений по улучшению существующей системы защиты предприятия.

Этап подготовки отчета по практике

Обработка данных и оформление отчета по практике:

- составление письменного отчета в соответствии с требованиями ГОСТ, ЕСКД и нормативной документацией 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 ОТЧЁТНОСТИ ПО ПРАКТИКЕ

Итоговая форма контроля по практике – дифференцированный зачёт.

Формой отчётности по итогам практики является:

- Индивидуальное задание студента,
- Отчет,
- Рабочий график (план),
- Дневник производственной 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 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 производственной 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 (модулей) 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

Контролируемый раздел (этап) практики	Код контролируемой компетенции	Наименование оценочного средства
Подготовительный этап	ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4	дневник производственной практики, отзыв-характеристика, рабочий график (план), отчет
Производственный этап	ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4	дневник производственной практики, отчет, отзыв-характеристика, рабочий график (план)
Этап обработки и анализа полученной информации	ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4	отчет, презентация, дневник производственной практики
Этап подготовки отчета по практике	ОПК-2, ОПК-3, ОПК-4, ОПК-5, ОПК-7, ОПК-11, ОПК-12, ОПК-2.2, ОПК-2.4	отчет, презентация, дневник производственной практики

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

Итогом прохождения практики является готовность обучающихся 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 учебной / производственной практике выставляется на основании: подготовки и защиты отчёта по практике; характеристики профессиональной деятельности обучающегося на практике; дневника практики с указанием видов работ, выполненных обучающимся во время практики, их объёма, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика. Для оценки выполнения обучающимся заданий по практике можно использовать следующие показатели (табл. 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

Шкала оценивания	Критерии оценивания
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задания по практике

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

1. Наименование оценочного средства - отчет.

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

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

При оформлении отчета по практике необходимо руководствоваться следующим документом: Методические рекомендации по оформлению отчета по практике (учебной, производственной, преддипломной) для студентов, обучающихся по направлению 10.03.01 Информационная безопасность / Составители: Т.Г. Гурская [Электронный ресурс].

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

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

ОСНОВНАЯ ЧАСТЬ

Глава 1 Аналитическая часть

Глава 2 Теоретическая часть

Глава 3 Проектная часть

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

ПРИЛОЖЕНИЯ

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 (ПЗ).

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

В содержание ПЗ включают номера разделов, подразделов, пунктов и подпунктов, имеющих заголовков, 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 производственной 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 своей 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, 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 СПИСКЕ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ перечисляются все источники информации, использованные в отчете, и в том числе ссылки на материалы из сети Internet.

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 производственной практики. Титульный лист и содержание дневника производственной 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:

- описание должностных обязанностей стажера;
- подготовка текста одной (нескольких) должностных инструкций сотрудников;
- описание имеющего на предприятии оборудования, связанного с решением задач производственной практики и относящегося к области защиты информации;
- построение модели угроз предприятия;
- обоснование рекомендаций по улучшению существующей системы защиты информации;
- описание особенностей охраны труда и правил техники безопасности на предприятии;
- подбор нормативно-правовой, научно-технической документации, оформленной в соответствии с ГОСТ.

Оценка по производственной практике выставляется на основании:

- подготовки и публичной защиты отчета по практике,
- отзыва-характеристики профессиональной деятельности студента во время прохождения производственной 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	хорошо

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.	
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
<i>Опоздание</i>	-1
<i>Нарушение учебной дисциплины</i>	-10
<i>Неготовность к выполнению задания на практике</i>	-10
<i>Пропуск одного дня практики без уважительной причины</i>	-1
<i>Нарушение сроков сдачи отчетности</i>	-10

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. 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»).
5. Информационная безопасность и защита информации / Шаньгин В.Ф. - М: ДМК Пресс, 2014. - URL: <http://www.studentlibrary.ru/book/ISBN9785940747680.html> (ЭБС «Консультант студента»).

8.2. Дополнительная литература

1. Мельников, В.П. Информационная безопасность и защита информации: доп. УМО по унтскому 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. Хорев, П.Б. Программно-аппаратная защита информации: рек. кафедрой информационной безопасности Российского государственного социального университета для студентов вузов, обучающихся по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев. - М. : ФОРУМ, 2009. - 352 с. - (Высшее образование). - ISBN 978-5-91134-353-8 : 249-92. (12 экз.)
3. ГОСТ 19.701-90 ЕСПД ГОСТ 2.125-88 Правила выполнения конструкторских документов. Сб. ГОСТов. - М.: Стандартиформ, 2010
4. ГОСТ 2.105-95 ЕСКД. Основные требования к текстовым документам. Сб. ГОСТов. - М.: Стандартиформ, 2011.
5. ГОСТ 2.004-88 ЕСКД. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ. Сб. ГОСТов. - М.: Стандартиформ, 2011.
6. ГОСТ Р 7.05-2008 Библиографическая ссылка. СИБИД, М.: Стандартиформ, 2008.
7. 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»).
8. 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.)
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»).
11. 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> (ЭБС «Консультант студента»).
12. 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.html> (ЭБС «Консультант студента»).
13. Инженерно-техническая и пожарная защита объектов / 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»).

8.3. Интернет-ресурсы, необходимые в процессе прохождения практики

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. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

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

9.1. Информационные технологии

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 (LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров.

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
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional, 10	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

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 им. В.Н. Татищева:

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 «Пирания» – поисковый комплекс
24. Гром ЗИ 4 шумогенератор
25. Кобра защита проводных линий
26. КРЦ-3 – шумогенератор
27. Онега-23М – нелинейный локализатор импульсный
28. УЛАН – проверочное устройство проводных линий
29. ФСП-1Ф-7А сетевой фильтр
30. OMS-2000 – акустический излучатель Cisco Packet Tracer.

11. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ПРАКТИКИ ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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.

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация по практике для лиц с нарушениями слуха (отчет по практике) проводится в письменной форме, при этом используются общие критерии оценивания, требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.)

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование звукозаписывающих устройств (диктофонов и т. д.). Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации (отчет по практике) для лиц с нарушением зрения рекомендуется применять устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).