

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОГЛАСОВАНО
Заведующий кафедрой
«Информационная безопасность»


М.И. Ожиганова
(И.О. Фамилия)
«13» 05 2022 г.

УТВЕРЖДАЮ
И.о. директора Института
радиоэлектроники и
информационной безопасности

С.Н. Девицына
(И.О. Фамилия)
2022 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика

(вид практики)

Преддипломная практика

(тип практики)

10.03.01 Информационная безопасность

(код и направление подготовки/специальность)

Организация и технологии защиты информации

(по отрасли или в сфере профессиональной деятельности)

(наименование профиля подготовки/специализации)

бакалавриат

(уровень высшего образования)

очная, 2022

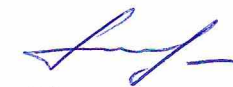
(форма обучения, год набора)

Севастополь
2022 г.

Рабочая программа преддипломной практики составлена на основе ФГОС по направлению подготовки/специальности 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Рабочая программа практики рассмотрена и одобрена на заседании кафедры «Информационная безопасность» «24» мая 2022 г., протокол № 12.

Руководитель образовательной программы


(подпись)

М.И. Ожиганова
(И.О. Фамилия)

Программа составлена:
Старший преподаватель

(должность, ученая степень, ученое звание)


(подпись)

М.А. Маслова
(И.О. Фамилия)

Программа составлена:
Старший преподаватель

(должность, ученая степень, ученое звание)


(подпись)

В.В. Пелись
(И.О. Фамилия)

Рецензент (*ведущий специалист – представитель работодателей или их объединений в соответствующей области профессиональной деятельности*):

Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя

(должность, ученая степень, ученое звание)


(подпись)

В.С. Кобизской
(И.О. Фамилия)

СОДЕРЖАНИЕ

1. Цель практики	4
2. Задачи практики	4
3. Место практики в структуре ООП	4
4. Тип практики, способ и форма ее проведения	5
5. Планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения образовательной программы	5
6. Структура и содержание практики	11
7. Формы отчетности по практике	12
8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике	13
9. Учебно-методическое и информационное обеспечение практики	15
10. Материально-техническое обеспечение практики	16

1 Цели практики

Целью прохождения преддипломной практики является изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте; сбор, обработка (анализ) и подготовка материалов для написания выпускной квалификационной работы, а также для написания выпускной квалификационной работы.

2 Задачи практики

Задачи преддипломной практики:

- углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;
- расширение представлений о функциональных возможностях защищенных информационных систем;
- усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;
- сбор материала для последующего его использования при написании выпускной квалификационной работы;
- углубление практических умений и навыков по профессиональной деятельности в рамках направления "Информационная безопасность";
- приобретение практических навыков по сбору и анализу информационных материалов;
- формирование умения анализировать и оценивать свою собственную профессиональную деятельность.

3 Место практики в структуре ООП

В соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» блок основной образовательной программы бакалавриата «Практика» может содержать обязательные, рекомендуемые и дополнительные (устанавливаемые образовательной организацией) типы практик. Преддипломная практика является обязательной.

Преддипломная практика проводится в 8 семестре 4 года обучения (курса), базируется на всех учебных дисциплинах, изученных за период обучения, и является основой для успешного написания и защиты выпускной квалификационной работы.

Приступая к прохождению практики, обучающийся должен:

- **знать:** права и обязанности человека и гражданина, ответственное отношение к делу, своему гражданскому и профессиональному долгу; методы организации и ведения рабочего процесса;
- **уметь:** применять современные методы организации и ведения рабочего процесса в организации; использовать в социальной, познавательной и профессиональной деятельности навыки работы с персональным компьютером, программным обеспечением и сетевыми ресурсами, пользоваться базами данных; пользоваться в процессе работы знаниями в области ИКТ; использовать навыки воспитательной в преддипломной деятельности; использовать на практике методы гуманитарных, социальных и экономических наук в различных видах профессиональной и социальной деятельности;
- **владеть:** способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности.

4 Тип практики, способ и форма ее проведения

Тип практики – преддипломная.

Способ проведения практики – стационарная (в Университете на базе кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности, по договорам на предприятиях, в учреждениях, организациях, расположенных на территории г. Севастополя) или выездная (по договорам на предприятиях, в учреждениях, организациях, расположенных за пределами г. Севастополя).

Форма проведения практики – непрерывно.

Преддипломная практика представляет собой вид учебных занятий, непосредственно ориентированный на сбор, обработку (анализ) и подготовку материалов для написания выпускной квалификационной работы бакалавра.

Преддипломная практика проходит в форме профессиональной деятельности, основанной на самостоятельном выполнении студентами производственных функций на конкретных местах, отвечающих требованиям программы практики.

Отличительной особенностью данного вида практики является ее акцент на сборе, обработке (анализе) и подготовке материалов для написания выпускной квалификационной работы.

Возможными местами проведения данной практики в организациях и на предприятиях могут являться:

- отделы защиты информации;
- отделы АСУ, вычислительные центры;
- отделы, занимающиеся разработкой и внедрением программного обеспечения, проектированием, монтажом и поддержкой вычислительных сетей;
- отделы ФСТЭК;
- отделы службы казначейства;
- отделы ВЧ;
- отделы, занимающиеся разработкой, продвижением и поддержкой web-сайтов;
- др. отделы, связанные с тематикой данного профиля.

5 Планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения образовательной программы

Формируемые в результате освоения ООП компетенции	Планируемые результаты обучения при прохождении практики
ПК-2.1 – Способен обеспечивать защиту от несанкционированного доступа объекта информатизации и сетей связи (за исключением сетей связи специального назначения)	Знать: - методы контроля функционирования сетей связи, их защищенности от НСД; - принципы построения современных сетей связи, математические модели каналов связи, виды модуляции сигналов; - функциональное назначение и основные характеристики средств контроля функционирования сетей связи, их защищенности от НСД; - организацию и содержание мониторинга функционирования объекта информатизации и средств связи, их защищенности от НСД; - возможные источники и технические каналы утечки информации; - нормативные правовые акты в области связи и защиты информации
	Уметь:

	- использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты объекта информатизации и сетей связи от НСД; - проводить контроль функционирования средств и сетей связи, их защищенности от НСД; - определять технические характеристики средств и сетей связи, их защищенности от НСД; - оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры; - осуществлять проверки средств и сетей связи, программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации от НСД на соответствие заданным требованиям; - проводить документационное обеспечение функционирования СССЭ, их защищенности от НСД Владеть: - навыками применения средств анализа функциональности средств и сетей связи, их защищенности от НСД; - навыками контроля целостности средств и систем связи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от НСД; - навыками составления отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации
ПК-2.2 – Способен обеспечить управление защитой информации на объектах информатизации	Знать: - основные методы управления защитой информации; - основные угрозы безопасности информации и модели нарушителя на объектах информатизации; - методы защиты информации от "утечки" по техническим каналам; - нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Уметь: - оценивать информационные риски на объектах информатизации; - классифицировать и оценивать угрозы безопасности информации; - определять подлежащие защите информационные

	ресурсы объектов информатизации; - применять нормативные документы по противодействию технической разведке; - разрабатывать предложения по совершенствованию системы управления защиты информации на объектах информатизации; - конфигурировать параметры систем защиты информации на объектах информатизации; - применять технические средства контроля эффективности мер защиты информации Владеть: - навыками анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность; - навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации на объекте информатизации; - навыками оценки последствий от реализации угроз безопасности информации на объекте информатизации; - навыками анализа изменения угроз безопасности информации объекта информатизации, возникающих в ходе его эксплуатации
ПК-2.3 – Способен внедрять системы защиты информации на объектах информатизации	Знать: - основные угрозы безопасности информации и модели нарушителя для объектов информатизации; - типовые средства, методы и протоколы идентификации, аутентификации и авторизации; - основные меры по защите информации на объектах информатизации; - нормативные правовые акты в области защиты информации; - нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации на объектах информатизации; - принципы построения средств защиты информации от "утечки" по техническим каналам и способы защиты от нее; - способы контроля эффективности защиты информации от "утечки" по техническим каналам; - организационные меры по защите информации;

	- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации; - методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; - методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем
	Уметь: - администрировать программные средства систем защиты информации на объектах информатизации; - устранять известные и выявленные уязвимости автоматизированных систем, приводящие к возникновению угроз безопасности информации; - применять нормативные документы по противодействию технической разведке; - применять аналитические и компьютерные модели объектов информатизации, автоматизированных систем и систем защиты информации; - проводить анализ структурных и функциональных схем защищенных автоматизированных систем; - определять параметры настройки программного обеспечения систем защиты информации на объектах информатизации; - классифицировать и оценивать угрозы информационной безопасности; - контролировать эффективность принятых мер по защите информации на объектах информатизации; - разрабатывать предложения по совершенствованию системы управления защитой информации на объекте информатизации; - проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств
	Владеть: - навыками проведения входного контроля качества комплектующих изделий системы защиты информации на объектах информатизации; - навыками осуществления автономной наладки технических и программных средств систем защиты информации на объектах информатизации; - навыками проведения предварительных и приемочных испытаний систем защиты информации на объектах информатизации; - навыками внесения в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний; - навыками определения правил и процедур управления

	системой защиты информации на объекте информатизации; - навыками определения правил и процедур выявления инцидентов и реагирования на них; - навыками определения правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы; - навыками определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации; - навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем; - навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации объекта информатизации; - навыками проведения экспертизы состояния защищенности информации на объекте информатизации; - навыками уточнения модели угроз безопасности информации на объекте информатизации
ПК-2.4 – Способен формировать требования к защите информации на объектах информатизации	Знать: - основные информационные технологии, используемые на объектах информатизации; - основные угрозы безопасности информации и модели нарушителя для объектов информатизации; - виды информационных воздействий и критерии оценки защищенности информации на объектах информатизации; - методы защиты информации от "утечки" по техническим каналам; - программно-аппаратные средства обеспечения защиты информации на объектах информатизации; - методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; - принципы формирования политики информационной безопасности объектов информатизации; - нормативные правовые акты в области защиты информации; - национальные, межгосударственные и международные стандарты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации; - методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; - содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем

	и систем защиты информации; - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях; - способы реализации угроз безопасности в автоматизированных системах Уметь: - анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами; - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и объектов информатизации в целом; - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации объекта информатизации; - организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем объектов информатизации; - использовать рисковую методологию управления защитой информации в автоматизированной системе объекта информатизации; - определять класс защищенности автоматизированных систем и их составных частей Владеть: - навыками анализа характера обрабатываемой информации и определения перечня информации, подлежащей защите; - навыками выявления степени участия персонала в обработке защищаемой информации; - навыками планирования мероприятий по обеспечению защиты информации на объекте информатизации; - навыками определения требуемого класса (уровня) защищенности автоматизированной системы объекта информатизации; - навыками обоснования необходимости использования криптографических средств защиты информации; - навыками разработки отчетных документов и разделов технических заданий
ПК-2.5 – Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и	Знать: - алгоритмы выполнения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации Уметь: - выполнять работы по установке, настройке, администрированию, обслуживанию и проверке

технических средств защиты информации	работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	Владеть: - навыками установки, настройки, администрирования, обслуживания и проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

6 Структура и содержание практики

Преддипломная практика содержит следующие этапы:

- **подготовительный:** установочная конференция и вводный инструктаж;
- **основной:** изучение структуры организации и органов защиты информации; изучение способов, средств и методов защиты информации, применяемых в организации; практическое выполнение обязанностей на различных должностях в зависимости от возможностей организации; изучение перспектив и направлений развития средств защиты информации в организации;
- **обработка и анализ полученной информации:** выполнение индивидуального задания; подготовка отчета о выполнении преддипломной практики; итоговая конференция; защита по результатам прохождения практики; выставление оценок.

6.1 Структура практики

Общая трудоемкость преддипломной практики составляет 6 зачетных единиц (216 часов), продолжительность – 4 недели.

№ п/п	Разделы (этапы) практики	Виды учебной деятельности на практике, включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля
	Подготовительный этап	2	
1	Установочная конференция	1	отчет
2	Предварительный инструктаж	1	отчет
	Основной этап	184	
3	Изучение структуры организации и органов защиты информации	16	отчет
4	Изучение видов угроз безопасности информации, характерных для организации	16	отчет
5	Изучение способов, средств и методов защиты информации, применяемых в организации	16	отчет
6	Изучение и подбор материала темы дипломной работы	40	отчет
7	Написание статьи совместно с руководителем дипломной работы	24	отчет
8	Выполнение индивидуального задания по теме выпускной квалификационной работы	72	отчет
	Обработка и анализ полученной информации	30	

9	Подготовка отчета о выполнении преддипломной практики	24	отчет
10	Итоговая конференция	6	отчет
	Итого	216	Диф. зачет

6.2 Содержание практики

6.2.1. Подготовительный этап

Установочная конференция – проводится в первый день практики ответственным лицом от Университета за данный вид практики, на которой доводятся цели практики, критерии оценивания и проводится предварительный инструктаж.

Предварительный инструктаж: проводится специалистом кафедры и подтверждается подписями инструктируемого и инструктирующего в дневнике практики. Предварительный инструктаж включает:

- инструктаж по технике безопасности;
- инструктаж по охране труда;
- инструктаж по пожарной безопасности;
- инструктаж по правилам внутреннего распорядка.

6.2.2. Производственный этап: рассматриваются более детально основные вопросы, вынесенные на практику.

- изучение структуры организации и органов защиты информации,
- изучение видов угроз безопасности информации, характерных для организации,
- изучение способов, средств и методов защиты информации, применяемых в организации,
- изучение и подбор материала темы дипломной работы,
- написание статьи совместно с руководителем дипломной работы,
- выполнение индивидуального задания по теме выпускной квалификационной работы.

6.2.3. Обработка и анализ полученной информации:

- выполнение индивидуального задания: каждый студент получает индивидуальное задание, которое он должен выполнить в виде реферата (20-25 страниц печатного текста),
- подготовка отчета о выполнении производственной практики (реферат оформляется согласно Приложения 2),
- итоговая конференция – назначается день и время, когда студенты за круглым столом обсуждают прохождение практики и делают доклады с презентацией своего реферата.

7 Формы отчетности по практике

Оценка качества прохождения преддипломной практики включает текущую и промежуточную аттестации.

Текущая аттестация осуществляется кафедральным руководителем практики и руководителями практики от организаций.

По итогам практики обучающиеся представляют кафедральному руководителю:

- 1) индивидуальный план, подписанный руководителем практики от предприятия, организации;
- 2) задание на практику;
- 3) отзыв руководителя практики от предприятия, организации, содержащий оценку по 5-балльной шкале, и заверенный в предприятии, организации;
- 4) дневник практики;
- 5) отчет по практике, оформленный согласно установленным требованиям.

Промежуточная аттестация представляет собой дифференцированный зачет (зачет с оценкой), включающий в себя подготовку и защиту отчета по практике.

По завершении преддипломной практики на кафедре проводится итоговая конференция, на которой подводятся итоги работы студентов в период практики. На конференции студенты отчитываются о своей работе, проведенной в период практики, заслушиваются и анализируются пожелания студентов по улучшению организации практики, обосновываются и объявляются итоговые оценки.

Студенты, не выполнившие программу практики по уважительной причине, направляются на практику повторно, в свободное от учебы время.

Студенты, не выполнившие программу практики без уважительной причины или получившие неудовлетворительную отметку, могут быть отчислены из университета как имеющие академическую задолженность, в порядке, предусмотренном уставом СевГУ.

8 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике включает:

- порядок оценивания результатов прохождения практики обучающимися;
- типовые контрольные задания или иные материалы, необходимые для оценки результатов прохождения практики, критерии оценивания.

Перечень вопросов, выносимых на зачет:

- нормативные документы по разработке политики безопасности на базе практики;
- описание и основные характеристики средств информационной защиты на базе практики;
- оформленный отчет по практике.

Таблица 8.1 – Таблица соответствия оценок

Оценка ECTS	Определение оценки в системе ECTS	Оценка по 100-балльной шкале	Оценка по национальной шкале
А	Все компетенции освоены на повышенном уровне по когнитивным и деятельностно-практическим критериям; выполнена вся программа практики и на защите индивидуального отчета показано глубокое и всестороннее знание комплекса мер по обеспечению информационной безопасности; свободное ориентирование в литературе и предоставленной на практике документации.	90-100	отлично
В	Все компетенции освоены на хорошем уровне, однако при ответе на вопросы допущены несущественные неточности в изложении самостоятельно изученного материала; при указании на ошибки обучающийся легко их корректирует; программа практики выполнена практически полностью и на защите индивидуального отчета показаны достаточные знания комплекса мер по обеспечению информационной	82-89	хорошо

	безопасности; показано умение применять теоретические знания на практике в ситуациях легкой и средней тяжести; хорошее ориентирование в технической литературе и предоставленной на практике документации.		
С	Все компетенции освоены на хорошем уровне, однако при ответе на вопросы допущены неточности в изложении самостоятельно изученного материала; при указании на ошибки обучающийся корректирует их с трудом; программа практики выполнена практически полностью и на защите индивидуального отчета показаны достаточные знания комплекса мер по обеспечению информационной безопасности; показано умение применять теоретические знания на практике в ситуациях легкой и средней тяжести; хорошее ориентирование в технической литературе и предоставленной на практике документации.	75-81	
D	Усвоения всех компетенций на пороговом уровне; студент в основном выполнил программу практики и на защите индивидуального отчета показывает достаточные знания специфики математических методов и информационных технологий, изученных ранее; умеет применять теоретические знания для решения некоторых задач по защите информации и реализации мероприятий на практике; ориентируется в большей части технической документации; обучающийся проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов.	69-74	удовлетворительно
E	Обучающийся способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом информации; дает неполноценные ответы на поставленные вопросы.	60-68	
F	Существуют компетенции, не освоенные на пороговом уровне; студент не выполнил программу практики; обучающийся не способен ответить на вопросы даже при дополнительных	35-59	неудовлетворительно

	наводящих вопросах экзаменатора.		
FX	Обучающийся не сдал ни одного вида контроля, большую часть времени, отведенного для практики, отсутствовал.	1-34	

9 Учебно-методическое и информационное обеспечение практики

9.1 Основная литература

№ п/п	Наименование и полное библиографическое описание
Основная литература	
1	Лопин В.Н. Защита информации в компьютерных системах [Текст]: учеб. пособие / В.Н. Лопин, И.С. Захаров; Курск. Гос. Техн. Ун-т. Курск, 2006. 175 с.
2	Лопин В.Н. Основы защиты информационных систем: учеб. пособие / В.Н. Лопин, В.А. Кудинов; Курск. Гос. Ун-т.- Курск. Гос. Ун-т, 2010.- 227 с.
3	Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. – М.: ИД «Форум»: ИНФРА-М, 2010.-592 с. Режим доступа: http://www.knigafund.ru/books/112645 .

9.2 Дополнительная литература

Дополнительная литература	
1	Сердюк В.А. Организация и технологии защиты информации: учеб. пособие / В.А. Сердюк. – Гос. Ун-т- Высшая школа экономики. – М.: Изд. Дом Гос. Ун-та – Высшей школы экономики, 2011. 572 с.
2	Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и Техника, 2004. – 384 с.
3	Хореев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие / П.Б. Хореев. – М.: Издательский центр «Академия», 2005. – 256 с.

9.3 Периодические издания

Использование периодических изданий не предусматривается.

9.4 Интернет-ресурсы

Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для проведения практики.

№ п/п	Адрес сайта и его описание
1	http://znanium.com – Электронная библиотечная система «ZNANIUM.COM»
2	http://www.iprbookshop.ru – Электронная библиотечная система «IPR BOOKS»
3	http://www.biblio-online.ru – Электронная библиотечная система «ЮРАЙТ»
4	http://e.lanbook.com – Электронная библиотечная система издательства «Лань»

9.5 Методические указания по практике

Методические указания по практике для обучающихся по направлению подготовки

10.03.01 Информационная безопасность.

9.6 Информационные технологии

1. MS Windows 7 Professional
2. MS Office 2013
3. PyCharm
4. Wireshark
5. Kali Linux
6. Python

7. Microsoft Visual Studio Community 2019
8. Smart-Soft Traffic Inspector Gold Edition
9. InfoWatch Traffic Monitor Enterprise Edition
10. Falcongaze Secure Tower NFR
11. Secret Net Studio 8 (ООО «Код Безопасности»)
12. СКЗИ «Континент-АП» (ООО «Код Безопасности»)
13. СЗИ vGate R2 Enterprise Plus (ООО «Код Безопасности»)
14. СЗИ от НСД Secret Net LSP (ООО «Код Безопасности»)

10 Материально-техническое обеспечение практики

Практика проводится на базе имеющегося материально-технического обеспечения в местах прохождения практики.

Для полноценного прохождения учебной практики в распоряжение студентов предоставлены компьютерные классы кафедры «Информационная безопасность», укомплектованные современным вычислительным оборудованием и периферией, специализированные учебные и научно-исследовательские лаборатории различного профиля.

В библиотеке вуза студентам обеспечивается доступ к справочной, научной и учебной литературе, монографиям и периодическим научным изданиям по специальности.

Помещения для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

Наименование специализированных аудиторий, кабинетов, лабораторий, тренажеров и пр.	Перечень основного оборудования
405, 410, 422, 431, 433, 435	Персональные ЭВМ, специальное оборудование

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

ДНЕВНИК ПРАКТИКИ

	Производственная (преддипломная) практика
	(вид и тип практики)
обучающегося	
	(Фамилия, Имя, Отчество)
	Институт радиоэлектроники и информационной безопасности
	Кафедра (департамент) «Информационная безопасность»
	Уровень высшего бакалавриат
	Направление подготовки/специальность 10.03.01 Информационная безопасность
	Профиль/специализация Организация и технологии защиты информации

___ курс, учебная группа _____

Обучающийся _____
(фамилия, имя, отчество)
 прибыл на предприятие (в организацию, учреждение)

М.П.

« ____ » _____ 20 ____ г.

(подпись)_____
(должность, фамилия и инициалы ответственного лица)

Отметки о проведении инструктажа

Наименование инструктажа	Дата проведения инструктажа	ФИО, должность инструктирующего	Подпись	
			инструкти- рующего	инструкти- руемого
Инструктаж по технике безопасности				
Инструктаж по охране труда				
Инструктаж по пожарной безопасности				
Инструктаж по правилам внутреннего распорядка				

Убыл из предприятия (организации, учреждения)

М.П.

« ____ » _____ 20 ____ г.

(подпись)_____
(должность, фамилия и инициалы ответственного лица)

Индивидуальное задание

[illegible]

Руководитель по практической подготовке от Университета

(подпись)

(должность, фамилия и инициалы ответственного лица)

Руководитель по практической подготовке от профильной организации

(подпись)

(должность, фамилия и инициалы ответственного лица)

« _____ » 20 ____ г.

Рабочий график (план) прохождения практики

[illegible]

Руководитель по практической подготовке от Университета

(подпись)

(должность, фамилия и инициалы ответственного лица)

Руководитель по практической подготовке от профильной организации

(подпись)

(должность, фамилия и инициалы ответственного лица)

« _____ » 20 ____ г.

Рабочие записи во время практики

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Отзыв (характеристика)

(фамилия, имя, отчество обучающегося))

Руководитель по практической подготовке от профильной организации

(подпись)

(должность, фамилия и инициалы ответственного лица)

« ____ » _____ 20 ____ г.

Сведения об уровне усвоения обучающимся компетенций

Код и наименование компетенции	Планируемые результаты обучения при прохождении практики	Сведения об уровне освоения обучающимся компетенций	
		Руководитель от профильной организации	Руководитель от Университета
ПК-2.1 – способность обеспечивать защиту от несанкционированного доступа объекта информатизации и сетей связи (за исключением сетей связи специального назначения)	ПК-2.1.1. Знает методы контроля функционирования сетей связи, их защищенности от НСД, принципы построения современных сетей связи, математические модели каналов связи, виды модуляции сигналов, функциональное назначение и основные характеристики средств контроля функционирования сетей связи, их защищенности от НСД, организацию и содержание мониторинга функционирования объекта информатизации и средств связи, их защищенности от НСД, возможные источники и технические каналы утечки информации, нормативные правовые акты в области связи и защиты информации. ПК-2.1.2. Умеет использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты объекта информатизации и сетей связи от НСД, проводить контроль функционирования средств и сетей связи, их защищенности от НСД, определять технические характеристики средств и сетей связи, их защищенности от НСД, оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры, осуществлять	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена

	проверки средств и сетей связи, программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации от НСД на соответствие заданным требованиям, проводить документационное обеспечение функционирования СССЭ, их защищенности от НСД. ПК-2.1.3. Владеет навыками применения средств анализа функциональности средств и сетей связи, их защищенности от НСД, контроля целостности средств и систем связи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от НСД, составления отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации.		
ПК-2.2 – способность обеспечить управление защитой информации на объектах информатизации	ПК-2.2.1. Знает основные методы управления защитой информации, основные угрозы безопасности информации и модели нарушителя на объектах информатизации, методы защиты информации от "утечки" по техническим каналам, нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2.2. Умеет оценивать	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена

	информационные риски на объектах информатизации, классифицировать и оценивать угрозы безопасности информации, определять подлежащие защите информационные ресурсы объектов информатизации, применять нормативные документы по противодействию технической разведке, разрабатывать предложения по совершенствованию системы управления защиты информации на объектах информатизации, конфигурировать параметры систем защиты информации на объектах информатизации, применять технические средства контроля эффективности мер защиты информации. ПК-2.2.3. Владеет навыками анализа воздействия изменений конфигурации автоматизированной системы на ее защищенность, составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации на объекте информатизации, оценки последствий от реализации угроз безопасности информации на объекте информатизации, анализа изменения угроз безопасности информации объекта информатизации, возникающих в ходе его эксплуатации.		
ПК-2.3 – способность внедрять системы защиты информации на объектах информатизации	ПК-2.3.1. Знает основные угрозы безопасности информации и модели нарушителя для объектов информатизации, типовые средства, методы и протоколы	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена

	идентификации, аутентификации и авторизации, основные меры по защите информации на объектах информатизации, нормативные правовые акты в области защиты информации, нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации, основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации на объектах информатизации, принципы построения средств защиты информации от "утечки" по техническим каналам и способы защиты от нее, способы контроля эффективности защиты информации от "утечки" по техническим каналам, организационные меры по защите информации, методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации, методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации, методы, способы и средства обеспечения		
--	---	--	--

	отказоустойчивости автоматизированных информационных систем. ПК-2.3.2. Умеет администрировать программные средства систем защиты информации на объектах информатизации, устранять известные и выявленные уязвимости автоматизированных систем, приводящие к возникновению угроз безопасности информации, применять нормативные документы по противодействию технической разведке, применять аналитические и компьютерные модели объектов информатизации, автоматизированных систем и систем защиты информации, проводить анализ структурных и функциональных схем защищенных автоматизированных систем, определять параметры настройки программного обеспечения систем защиты информации на объектах информатизации, классифицировать и оценивать угрозы информационной безопасности, контролировать эффективность принятых мер по защите информации на объектах информатизации, разрабатывать предложения по совершенствованию системы управления защитой информации на объекте информатизации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств. ПК-2.3.3. Владеет навыками проведения входного контроля		
--	---	--	--

	качества комплектующих изделий системы защиты информации на объектах информатизации, осуществления автономной наладки технических и программных средств систем защиты информации на объектах информатизации, проведения предварительных и приемочных испытаний систем защиты информации на объектах информатизации, внесения в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний, определения правил и процедур управления системой защиты информации на объекте информатизации, определения правил и процедур выявления инцидентов и реагирования на них, определения правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы, определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации, выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем, проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации объекта информатизации, проведения экспертизы состояния защищенности информации на объекте информатизации, уточнения модели угроз безопасности информации на объекте информатизации.		
ПК-2.4 – способность	ПК-2.4.1. Знает основные информационные технологии,	освоена / освоена	освоена / освоена

формировать требования к защите информации на объектах информатизации	используемые на объектах информатизации, основные угрозы безопасности информации и модели нарушителя для объектов информатизации, виды информационных воздействий и критерии оценки защищенности информации на объектах информатизации, методы защиты информации от "утечки" по техническим каналам, программно-аппаратные средства обеспечения защиты информации на объектах информатизации, методы, способы и средства обеспечения отказоустойчивости автоматизированных систем, принципы формирования политики информационной безопасности объектов информатизации, нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, организационные меры по защите информации, методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации, содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации, основные криптографические методы, алгоритмы,	частично / не освоена	частично / не освоена
--	---	------------------------------	------------------------------

	протоколы, используемые для обеспечения безопасности в вычислительных сетях, способы реализации угроз безопасности в автоматизированных системах. ПК-2.4.2. Умеет анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами, выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и объектов информатизации в целом, классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации объекта информатизации, организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем объектов информатизации, использовать рисковую методологию управления защитой информации в автоматизированной системе объекта информатизации, определять класс защищенности автоматизированных систем и их составных частей. ПК-2.4.3. Владеет навыками анализа характера обрабатываемой информации и определения перечня информации, подлежащей защите, выявления степени участия персонала в обработке защищаемой информации, планирования мероприятий по обеспечению защиты информации на объекте информатизации, определения требуемого класса (уровня)		
--	---	--	--

	защищенности автоматизированной системы объекта информатизации, обоснования необходимости использования криптографических средств защиты информации, разработки отчетных документов и разделов технических заданий.		
ПК-2.5 – способность выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации		освоена / освоена частично / не освоена	освоена / освоена частично / не освоена
Руководитель по практической подготовке от Университета _____ (подпись) (инициалы и фамилия) Руководитель по практической подготовке от профильной организации _____ (подпись) (инициалы и фамилия) «__» _____ 20__ г.		Руководитель по практической подготовке от Университета _____ (подпись) (инициалы и фамилия) Руководитель по практической подготовке от профильной организации _____ (подпись) (инициалы и фамилия) «__» _____ 20__ г.	

Оценка результатов прохождения практики обучающимся
(заполняется руководителем практики от Университета)

(фамилия, имя, отчество обучающегося)

Дата сдачи отчета « ____ » _____ 20__ г.

Оценка: _____

Руководитель по практической подготовке от Университета

(подпись)

(должность, фамилия и инициалы ответственного лица)

*Структура и требования к оформлению отчета о практике***Структура отчета о практике**

Структурными элементами отчета о практике являются:

- титульный лист;
- индивидуальное задание на практику;
- содержание;
- введение;
- основная часть;
- заключение;
- список литературы;
- приложения.

Требования к оформлению отчета по практике

1. Оформление отчета о практике должно соответствовать требованиям к текстовым учебным документам соответствующих ГОСТов.

2. Текстовая часть отчета о практике выполняется с использованием печатающих и графических устройств на одной стороне листа белой бумаги формата А4 с параметрами: междустрочный интервал – 1,5; кегль – 14; шрифт – Times New Roman, обычный; цвет шрифта – черный; поля, не менее:

верхнее – 20 мм; левое – 30 мм;
нижнее – 20 мм; правое – 15 мм.

3. Иллюстрационно-графический материал в зависимости от специфики программы может включать: чертежи, схемы (технологические, кинематические, гидравлические, автоматизации, алгоритмов и др.), плакаты, диаграммы, макеты, фотографии, аудио- и видеоматериалы, натурные образцы и др.

Иллюстрационно-графический материал может быть представлен на бумажном, электронном носителе или в ином виде. Возможно представление иллюстрационно-графического материала в виде брошюр.

4. Отчет должен быть переплетен доступным способом.

Пример оформления титульного листа отчета о практике

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
 ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
 УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
 «СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт радиоэлектроники и информационной безопасности

Кафедра «Информационная безопасность»

№	Дата поступления на кафедру	Подпись отв. за регистрацию	Подпись преподавателя

ОТЧЕТ

о производственной (преддипломной) практике
 (вид практики) (тип практики)

В _____
 (наименование организации)

Выполнил _____
 (Фамилия И.О. обучающегося)

 (шифр группы)
 Направление / специальность 10.03.01
Информационная безопасность
 (код, наименование)

Руководитель по практической подготовке
 от Университета

 (должность)

 (Фамилия И.О. руководителя)

Севастополь
 20__ г.