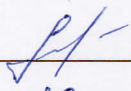


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОГЛАСОВАНО
Заведующий кафедрой
«Информационная безопасность»


М.И. Ожиганова
(И.О. Фамилия)
« 10 » 04 2023 г.

УТВЕРЖДАЮ
Директор Института
информационных технологий


В.Н. Бондарев
(И.О. Фамилия)
« 10 » 04 2023 г.



РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика

(вид практики)

Б2.В.ДВ.01.01(П) Профессиональный трек

(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, 2023

(форма обучения, год набора)

Севастополь
2023 г.

Рабочая программа Элективных практик (модулей) 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» «10 апреля 2023 г., протокол № 11.

Руководитель образовательной программы


(подпись)

М.И. Ожиганова
(И.О. Фамилия)

Рабочая программа практики составлена:

Старший преподаватель

(должность, ученая степень, ученое звание)

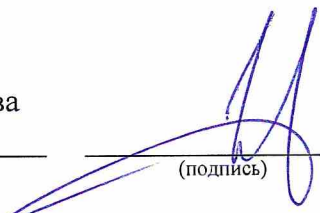

(подпись)

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	5
4. Тип практики, способ и форма ее проведения	6
5. Планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения образовательной программы	7
6. Структура и содержание практики	12
7. Формы отчетности по практике	13
8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике	14
9. Учебно-методическое и информационное обеспечение практики	16
10. Материально-техническое обеспечение практики	17

1 Цели практики

Целью прохождения практики является углубление и закрепление знаний и компетенций, полученных в процессе теоретического обучения, изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств или организаций, приобретение студентами практических навыков и опыта профессиональной работы в организации, учреждении, на предприятии.

Основная цель практики профессионального трека: углубление и закрепление знаний и навыков, полученных в процессе теоретического обучения и практической подготовки, и приобретение практических навыков и опыта профессиональной работы в организации, учреждении, на предприятии.

2 Задачи практики

Задачами практики являются:

- закрепление, углубление и развитие знаний, полученных в процессе теоретической подготовки в предшествующий период обучения;
- формирование у обучаемых полного представления о своей профессии;
- выполнение обязанностей на первичных должностях служб защиты информации предприятий, других структурных подразделений, имеющих отношение к информационной безопасности;
- получение практических навыков по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- получение практических навыков по применению программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования для решения профессиональных задач;
- получение практических навыков администрирования подсистемы информационной безопасности объекта защиты;
- получение практических навыков по реализации политики информационной безопасности, применению комплексного подхода к обеспечению информационной безопасности объекта защиты;
- получение практических навыков в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- получение практических навыков в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- получение практических навыков в выполнении комплекса работ по обеспечению информационной безопасности предприятия;
- изучение организационно-функциональной структуры базы практики;
- 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 изучении учебных дисциплин;
- изучение и определение состава и видов информационных технологий, применяемых на базе практике;
- изучение основных средств защиты информационных технологий, применяемых на базе практике (техническое, программное, лингвистическое обеспечение и т.п.);

- формирование умения анализировать и оценивать свою собственную профессиональную деятельность;
- описание информационных ресурсов, применяемых на базе практики (базы данных, web-ресурсы, архивы и т.п.);
- изучение опыта профессиональной, исследовательской или предпринимательской деятельности на месте прохождения практики;
- получение практических навыков, соответствующих выбранному обучающимся треку.

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. Профессиональный трек – дополнительный тип производственной практики, установленный ФГАОУ ВО «Севастопольский государственный университет».

В рамках практики у обучающегося имеется возможность продолжить следование выбранной ранее траектории обучения: профессиональный трек, исследовательский трек или предпринимательский трек.

Практика базируется на учебных дисциплинах «Угрозы информационной безопасности», «Защита от угроз информационной безопасности», «Теория информации в информационной безопасности», «Теория информации для защиты информационных процессов», «Основы информационной безопасности», «Этичный хакинг и кибербезопасность», «Теоретико-числовые методы в криптографии», «Защита программ и данных», «Системы распределенных реестров в информационной безопасности», «Документальное обеспечение информационной безопасности», «Аппаратные средства вычислительной техники обеспечения информационной безопасности», «Физические основы защиты информации», «Физические основы технических средств защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Сети и системы передачи информации», «Программно-аппаратные средства защиты информации», «Инженерно-техническая защита информации», «Системы защиты баз данных», «Международные и российские нормативные акты и стандарты в информационной безопасности», «Методы и средства криптографической защиты информации», «Математические методы исследования операций в информационной безопасности», «Технические средства охраны», «Системы искусственного интеллекта в информационной безопасности», «Защита информации от утечки по техническим каналам», «Алгоритмизация и программирование», и является основой для успешного освоения учебных дисциплин «Основы управления информационной безопасностью», «Защита информации от утечки по техническим каналам», «Моделирование процессов и систем защиты информации», «Информационная безопасность автоматизированных систем», «Комплексное обеспечение защиты информации объекта информатизации», «Системы охраны государственной тайны», «Администрирование и обеспечение информационной безопасности компьютерных сетей», «Защита информации в критической информационной инфраструктуре», «Информационное противодействие угрозам терроризма», «Защита информации в информационных системах персональных данных», «Организация и управление службой защиты информации», а также для преддипломной практики, подготовки и защиты выпускной квалификационной работы (далее – ВКР).

Приступая к прохождению практики, обучающийся должен:

- **знать**: организационно-правовые формы хозяйствования, состав информационных систем и технологий, существующие угрозы информационным активам, способы и методы защиты информации, требования нормативных документов по информационной

безопасности, способы и методы защиты информации;

- **уметь**: проводить оценку информационных активов предприятия, а также рисков информационной безопасности, применять организационные, технические и программные методы и средства защиты информации, оформлять организационно-распорядительную документацию по вопросам защиты информации, анализировать уровень информационной безопасности предприятия;

- **владеть**: навыками составления перечня ценной информации предприятия, проведения оценки рисков информационной безопасности, разработки перечня мер по ее повышению; навыками пользования техническими и программными методами защиты информации.

4 Тип практики, способ и форма ее проведения

Тип практики – Профессиональный трек.

Способ проведения практики – стационарная (в Университете на базе кафедры «Информационная безопасность» Института информационных технологий, по договорам на предприятиях, в учреждениях, организациях, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках ООП ВО, и расположенных на территории г. Севастополя) или выездная (по договорам на предприятиях, в учреждениях, организациях, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках ООП ВО, и расположенных за пределами г. Севастополя).

Форма проведения практики – концентрированная.

Практика проводится в 6 семестре 3 года обучения (курса) и является базовой для преддипломной практики, а также выполнения ВКР.

Возможными местами проведения данной практики в организациях и на предприятиях являются:

- отделы защиты информации;
- отделы АСУ, вычислительные центры;
- отделы, занимающиеся разработкой и внедрением программного обеспечения, проектированием, монтажом и поддержкой вычислительных сетей;
- отделы, занимающиеся разработкой, продвижением и поддержкой web-сайтов.

Практика представляет собой вид учебных занятий, непосредственно ориентированных на приобретение навыков профессиональной работы в рамках выбранного ранее индивидуального трека, углубление и закрепление знаний и компетенций, полученных в процессе теоретического обучения.

Практика направлена на расширение и углубление теоретических знаний, формирование умений и навыков выполнения разработки и проектирования в профессиональной сфере, подготовки технических отчетных документов. Практика выполняет интегрирующие функции в формировании навыков (владений) самостоятельного применения изученных в рамках профессиональных и профильных дисциплин инструментов и методов разработки и проектирования в предметной области. Место практики в учебном процессе определяет ее важную роль в подготовке бакалавров к практическому внедрению научных результатов - важному этапу инновационной деятельности. Выполняемые в рамках практики проектные работы составляют основу соответствующих разделов выпускной квалификационной работы бакалавра. Выполнение практики ориентировано на самостоятельную практическую внедренческую (проектную) деятельность в рамках реализуемого инновационного проекта под руководством и контролем руководителя практики, назначаемого непосредственно по месту ее прохождения.

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 привлечение студентов к практическому освоению программно-аппаратных средств и защищенных информационных технологий, используемых на базе практики.

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 СССРЭ, 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-2.3 – 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 технических средств защиты информации	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 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

Практика проводится непрерывно и содержит следующие этапы:

- **подготовительный**: установочная конференция и вводный инструктаж;
- **производственный**: 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 Элективных практик; итоговая конференция; защита по результатам прохождения практики; выставление оценок.

6.1. Структура практики

Общий объем практики составляет 6 зачетных единиц (216 часов), 4 недели.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу обучающихся и трудоемкость (в часах)	Формы текущего контроля
	Подготовительный этап	4	
1	Установочная конференция	2	отчет
2	Предварительный инструктаж	2	отчет
	Производственный этап	142	
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	24	отчет
6	Практическое выполнение обязанностей на различных должностях в зависимости от возможностей организации	70	отчет
7	Изучение перспектив и направлений развития средств защиты информации в организации	16	отчет
	Обработка и анализ полученной информации	70	
8	Выполнение индивидуального задания.	40	
9	Подготовка отчета о выполнении Элективных практик	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 и органов защиты информации организации;
- знакомство студентов с базой проведения практики, проведение теоретических занятий;
- изучение видов угроз безопасности информации, характерных для организации;
- 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.

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 Элективных практик (реферат оформляется согласно Приложению 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 практики включает текущую и промежуточную аттестацию.

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 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, включающий:

- 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;
- структура и органы защиты информации организации;
- виды угроз безопасности информации, характерных для организации;
- способы, средства и методы защиты информации, применяемых в организации;
- обязанности на различных должностях в зависимости от возможностей организации;
- перспективы и направления развития средств защиты информации в организации;
- 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 безопасности; показано умение применять теоретические знания на практике в ситуациях легкой и средней тяжести;	82-89	хорошо

	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 наводящих вопросах экзаменатора.	35-59	неудовлетворительно
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 Элективных практик 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 практика
(вид и тип практики)
(Профессиональный трек)
обучающегося
(Фамилия, Имя, Отчество)
Институт информационных технологий
Кафедра (департамент) «Информационная безопасность»
Уровень образования бакалавриат
Направление подготовки 10.03.01 Информационная безопасность
Профил Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

___ курс, 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)

(инициалы и фамилия)

Руководитель по практической подготовке от профильной организации

(подпись)

(инициалы и фамилия)

« » 20 г.

Рабочий график (план) прохождения практики

[illegible]

Руководитель по практической подготовке от Университета

(подпись)

(инициалы и фамилия)

Руководитель по практической подготовке от профильной организации

(подпись)

(инициалы и фамилия)

« _____ » 20 ____ г.

Рабочие записи во время практики

[illegible]

Отзыв (характеристика)

(фамилия, имя, отчество обучающегося))

Руководитель по практической подготовке от профильной организации

(подпись)

(инициалы и фамилия)

« ____ » _____ 20 ____ г.

Сведения об уровне усвоения обучающимися компетенций

Код и наименование компетенции	Планируемые результаты обучения при прохождении практики	Сведения об уровне освоения обучающимися 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; - знает принципы построения современных сетей связи, математические модели каналов связи, виды модуляции сигналов; - знает функциональное назначение и основные характеристики средств контроля функционирования сетей связи, их защищенности от НСД; - знает организацию и содержание мониторинга функционирования объекта информатизации и средств связи, их защищенности от НСД; - знает возможные источники и технические каналы утечки информации; - знает нормативные правовые акты в области связи и защиты информации. ПК-2.1.2: - умеет использовать средства мониторинга	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена

	работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты объекта информатизации и сетей связи от НСД; - умеет проводить контроль функционирования средств и сетей связи, их защищенности от НСД; - умеет определять технические характеристики средств и сетей связи, их защищенности от НСД; - умеет оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры; - умеет 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; - умеет 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; - владеет навыками контроля целостности средств и систем связи, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты от НСД; - владеет 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-2.3 – способность внедрять системы защиты информации на объектах информатизации	ПК-2.3.1: - знает основные угрозы безопасности информации и модели нарушителя для объектов информатизации; - знает типовые средства, методы и протоколы идентификации, аутентификации и авторизации; - знает основные меры по защите информации на объектах	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена

	информатизации; - знает нормативные правовые акты в области защиты информации; - знает нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; - знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации на объектах информатизации; - знает принципы построения средств защиты информации от "утечки" по техническим каналам и способы защиты от нее; - знает способы контроля эффективности защиты информации		
--	---	--	--

	от "утечки" по техническим каналам; - знает организационные меры по защите информации; - знает методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации; - знает методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; - знает методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем. ПК-2.3.2: - умеет администрировать программные средства систем защиты информации на объектах информатизации; - умеет устранять известные и выявленные уязвимости автоматизированных систем, приводящие к возникновению угроз безопасности информации; - умеет применять нормативные		
--	---	--	--

	документы по противодействию технической разведке; - умеет применять аналитические и компьютерные модели объектов информатизации, автоматизированных систем и систем защиты информации; - умеет проводить анализ структурных и функциональных схем защищенных автоматизированных систем; - умеет определять параметры настройки программного обеспечения систем защиты информации на объектах информатизации; - умеет классифицировать и оценивать угрозы информационной безопасности; - умеет контролировать эффективность принятых мер по защите информации на объектах информатизации; - умеет разрабатывать предложения по совершенствованию системы управления защитой информации на объекте информатизации; - умеет 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; - владеет навыками осуществления автономной наладки технических и программных средств систем защиты информации на объектах информатизации; - владеет навыками проведения предварительных и приемочных испытаний систем защиты информации на объектах информатизации; - владеет навыками внесения в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний; - владеет навыками определения правил и процедур управления системой защиты информации на объекте информатизации; - владеет навыками определения правил и процедур выявления инцидентов и		
--	---	--	--

	реагирования на них; - владеет навыками определения правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы; - владеет навыками определения правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации; - владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем; - владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации объекта информатизации; - владеет навыками проведения экспертизы состояния защищенности информации на объекте информатизации; - владеет навыками уточнения модели угроз безопасности информации на объекте информатизации.		
ПК-2.4 – способность формировать требования к защите	ПК-2.4.1: - знает основные информационные	освоена / освоена частично / не освоена	освоена / освоена

информации на объектах информатизации	технологии, используемые на объектах информатизации; - знает основные угрозы безопасности информации и модели нарушителя для объектов информатизации; - знает виды информационных воздействий и критерии оценки защищенности информации на объектах информатизации; - знает методы защиты информации от "утечки" по техническим каналам; - знает программно-аппаратные средства обеспечения защиты информации на объектах информатизации; - знает методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; - знает принципы формирования политики информационной безопасности объектов информатизации; - знает нормативные правовые акты в области защиты информации; - знает национальные, межгосударственные и международные стандарты в области защиты информации; - знает руководящие и		частично / не освоена
--	--	--	------------------------------

	методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - знает организационные меры по защите информации; - знает методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации; - знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации; - знает основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях; - знает способы реализации угроз безопасности в автоматизированных системах. ПК-2.4.2: - умеет анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными		
--	---	--	--

	системами; - умеет выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и объектов информатизации в целом; - умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации объекта информатизации; - умеет организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем объектов информатизации; - умеет использовать рисковую методологию управления защитой информации в автоматизированной системе объекта информатизации; - умеет 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; - владеет навыками выявления степени участия персонала в обработке защищаемой информации; - владеет навыками планирования мероприятий по обеспечению защиты информации на объекте информатизации; - владеет навыками определения требуемого класса (уровня) защищенности автоматизированной системы объекта информатизации; - владеет навыками обоснования необходимости использования криптографических средств защиты информации; - владеет навыками 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	ПК-2.5.1: - знает алгоритмы выполнения работ по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. ПК-2.5.2:	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена

	- умеет выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. ПК-2.5.3: - владеет навыками установки, настройки, администрирования, обслуживания и проверки работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.		
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.	

[illegible]

Оценка: _____

(подпись) _____ (инициалы и фамилия)

*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.

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

Кафедра «Информационная безопасность»

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

(трек)

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.