

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

« 10 » 04 2024 г.

УТВЕРЖДАЮ

Директор Института

информационных технологий



В.Н. Бондарев

2024 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика

(вид практики)

Б2.О.01(П) Преддипломная практика

(тип практики)

10.04.01 Информационная безопасность

(код и направление подготовки/специальность)

Управление информационной безопасностью в органах государственной власти

(наименование профиля подготовки/специализации)

магистратура

(уровень высшего образования)

очная, очно-заочная, 2024

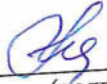
(форма обучения, год набора)

Севастополь
2024

Рабочая программа практики составлена на основе ФГОС по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1455.

Рабочая программа практики рассмотрена и одобрена на заседании кафедры «Информационная безопасность» «10» апреля 2024 г., протокол № 11.

Руководитель образовательной
программы


(подпись)

Ю.Ю. Гончаренко
(И.О. Фамилия)

Рабочая программа составлена:
Старший преподаватель
(должность, ученая степень, ученое звание)


(подпись)

В.В. Пелись
(И.О. Фамилия)

Рецензент:
Начальник Управления защиты
государственной тайны и
мобилизационной работы Правительства
г. Севастополя
(должность, ученая степень, ученое звание)


(подпись)

В.С. Кобизской
(И.О. Фамилия)

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), подготовка материалов и написание выпускной квалификационной работы.

2 Задачи практики

Задачами преддипломной практики являются:

- 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;
- написание 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 10.04.01 «Информационная безопасность» блок «Практика» основной образовательной программы магистратуры может содержать обязательные, рекомендуемые и дополнительные (устанавливаемые образовательной организацией) типы практик. Преддипломная практика относится к обязательной части блока Б2 учебного плана ООП.

Преддипломная практика проводится в 4 семестре для очной формы обучения и в 5 семестре для очно-заочной формы обучения, 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:** навыками научного анализа социально-значимых проблем и процессов; культурой мышления; способностью в письменной и устной речи правильно и убедительно

оформить результаты мыслительной деятельности; навыками работы с информацией; способностью к социальному взаимодействию, к сотрудничеству и разрешению конфликтов; толерантность и социальная мобильность; чувство социальной ответственности; способностью к толерантному отношению к расовым, национальным, религиозным различиям людей, способностью к планированию, организации и управлению своей профессиональной деятельностью и работы различных коллективов.

4 Тип практики, способ и форма ее проведения

Тип практики - преддипломная.

Способ проведения практики – стационарная (в Университете на базе кафедры «Информационная безопасность» Института информационных технологий, по договорам на предприятиях, в учреждениях, организациях, расположенных на территории г. Севастополя).

Форма проведения практики – концентрированная.

Преддипломная практика представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся и подготовку материалов для написания выпускной квалификационной работы.

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

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.

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

Практика проводится в 4 семестре 2 года обучения (курса) для очной формы обучения и в 5 семестре 3 года обучения (курса) для очно-заочной формы обучения и является базовой для выполнения ВКР.

5 Планируемые результаты обучения при прохождении практики, соотнесенные с планируемыми результатами освоения образовательной программы
Таблица 5.1.

Формируемые в результате освоения ООП компетенции	Планируемые результаты обучения при прохождении практики
УК-1 – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Знать: - методы и средства осуществления саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; - методы и способы фильтрации, анализа и оценки информации, ее достоверности; - способы и алгоритмы построения логических умозаключений на основе поступающих информации и данных
	Уметь: - анализировать условия окружающей действительности и выбирать наиболее оптимальный путь саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; - применять методы и средства осуществления саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; - выявлять недостающие необходимые, как специалисту по информационной безопасности, компетенции и развивать их; - применять методы и способы фильтрации, анализа и оценки информации, ее достоверности; - применять способы и алгоритмы построения логических умозаключений на основе поступающих информации и данных; - анализировать проблемную ситуацию как систему, осуществлять ее декомпозицию на отдельные задачи, выявляя ее составляющие и связи между ними; - определять пробелы в информации, необходимой для решения проблемной ситуации, и проектировать процессы по их устранению; - критически оценивать надежность источников информации, работать с противоречивой информацией из разных источников; - разрабатывать и содержательно аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов; - строить сценарии реализации стратегии, определяя возможные риски и предлагая пути их устранения, формировать возможные варианты решения задач
	Владеть: - навыками анализа условий окружающей действительности и выбора наиболее оптимального пути саморазвития, как специалиста по информационной безопасности, в условиях неопределенности; - навыками применения способов решения возникающих жизненных задач и средств развития (в том

	числе с использованием цифровых средств) других необходимых, как специалисту по информационной безопасности, компетенций; - навыками применения методов и способов фильтрации, анализа и оценки информации, ее достоверности; - навыками применения способов и алгоритмов построения логических умозаключений на основе поступающих информации и данных
УК-2 – Способен управлять проектом на всех этапах его жизненного цикла	Знать: - стандартные модели, алгоритмы и методы решения стандартных задач анализа инцидентов информационной безопасности; - способы и методики, применяемые для генерации новых идей, поиска нестандартных моделей, новых алгоритмов, способов решения задач анализа инцидентов информационной безопасности; - современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; - способы и методы критического анализа информации и данных в областях Big Data и Data Mining Уметь: - формулировать на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления; - разрабатывать концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи, обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения; - разрабатывать план реализации проекта с учетом возможных рисков реализации и возможностей их устранения, планирует необходимые ресурсы; - применять способы и методики, помогающие в генерации новых идей, поиске нестандартных моделей, новых оптимальных алгоритмов, способов решения задач анализа инцидентов информационной безопасности; - осуществлять мониторинг хода реализации проекта, корректировать отклонения, вносить дополнительные изменения в план реализации проекта, уточнять зоны ответственности участников проекта на всех этапах его жизненного цикла; - реализовывать процедуры и механизмы оценки качества проекта, инфраструктурные условия для внедрения результатов проекта; - применять современные способы, методы и цифровые средства управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; - использовать способы и методы критического анализа информации и данных в областях Big Data и Data

	Mining Владеть: - навыками генерации новых идей для решения нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; - навыками абстрагирования от стандартных моделей при решении нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; - навыками перестроения сложившихся способов решения нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; - навыками выработки новых оптимальных алгоритмов действий при решении нестандартных задач анализа инцидентов информационной безопасности, цифровой экономики; - навыками применения современных способов, методов и цифровых средств управления (поиска, анализа, синтеза) информацией и данными при решении задач в областях Big Data и Data Mining; - навыками применения способов и методов критического анализа информации и данных в областях Big Data и Data Mining
ОПК-1 – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на её создание	Знать: - основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности; - направления развития и проблемы компьютерного моделирования сложных систем; - направления развития технологий проектирования информационных, автоматизированных и автоматических систем; - современную нормативную базу и ГОСТы, регламентирующие процесс разработки ТЗ; - правила, способы и методы организации совместных разработок; - методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности Уметь: - проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности; - обосновывать и планировать состав и архитектуру моделируемых сложных систем; - обосновывать и планировать состав и архитектуру проектируемых информационных, автоматизированных и автоматических систем; - формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ; - разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения ИБ, оценивать эффективность решений и анализировать

	показатели деятельности; - обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности Владеть: - навыками участия в разработке системы обеспечения информационной безопасности объекта; - навыками разработки концептуальных стратегий решения задач моделирования и проектирования автоматизированных информационных систем и систем обеспечения ИБ; - навыками планирования и оценки трудоёмкости проекта, включая техническое, кадровое и финансовое обеспечение, принятие совместных решений
ОПК-2 – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Знать: - методы концептуального проектирования технологий обеспечения информационной безопасности; - направления развития и проблемы компьютерного моделирования сложных систем, направления развития технологий проектирования информационных, автоматизированных и автоматических систем; - современные методы и средства тестирования; - принципы построения и функционирования современных информационных систем; - назначение комплексной системы защиты информации, принципы её организации и этапы разработки; - требования к системам комплексной защиты информации Уметь: - выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью; - разрабатывать тестовые планы и сценарии тестирования разработанного продукта; - управлять коллективом исполнителей и принимать управленческие решения; - проектировать подсистемы безопасности информационных систем с учётом действующих нормативных и методических документов; - разрабатывать модели угроз и нарушителей информационной безопасности информационных систем Владеть: - навыками выполнения работы по изготовлению, монтажу, наладке, испытаниям и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности; - навыками практической реализации типовых задач разработки и исследования систем защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасностью;

	- средствами автоматизированного и ручного функционального тестирования; - навыками участия в организации комплексной системы защиты объекта
ОПК-3 – Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Знать: - основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью с целью разработки проектов организационно-распорядительных документов; - правила создания технического задания на создание подсистем безопасности информационных систем; - основные угрозы безопасности информации и модели нарушителя в информационных системах; - основные нормативные правовые акты в области обеспечения информационной безопасности; - нормативные методические документы ФСБ России в области защиты информации; - нормативные методические документы ФСТЭК России в области информационной безопасности
	Уметь: - разрабатывать технические задания на создание подсистем обеспечения информационной безопасности; - проводить выбор, исследовать эффективность, проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; - разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации; - разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации; - разрабатывать организационно-распорядительную документацию по обеспечению информационной безопасности; - работать с технической и эксплуатационной документацией; - оценивать различные инструменты в области проектирования и управления информационной безопасностью
	Владеть: - навыками разработки политик безопасности различных уровней; - навыками расчёта и управления рисками информационной безопасности, навыками разработки положения о применимости механизмов контроля в контексте управления рисками информационной безопасности; - правилами построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации; - навыками работы с нормативными правовыми

	актами в области информационной безопасности
ОПК-4 – Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	Знать: - способы формулирования научной проблемы, гипотезы, выбора предмета, объекта, целей, задач исследования; - основные принципы создания эскизного, технического, рабочего проектов; - методы анализа и обоснования выбора решений по обеспечению требуемого уровня безопасности информационных систем; - современные достижения науки в области информационной безопасности; - правила, способы и методы организации, выполнения и представления результатов научного исследования; - правила и стандарты разработки отчетной документации; - основные категории и понятия информационно-аналитической работы, принципы и методы ее ведения; - методы выработки и принятия информационного решения; - технологии поиска, изучения, обобщения и систематизации научной информации; - виды отчетно-информационных документов, методы их подготовки; - основные теоретико-числовые методы применительно к задачам защиты информации
	Уметь: - составлять пошаговый план научной деятельности, проводить предпроектные исследования; - работать с научной литературой, отбирать информацию по теме научного исследования, систематизировать, классифицировать полученную информацию; - определять комплекс мер для обеспечения безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности систем; - использовать методы и средства анализа защищенности информационных систем; - использовать программные и аппаратные средства персонального компьютера для поиска и обработки информации; - разрабатывать планы и программы проведения научных исследований в соответствии с техническим заданием, ресурсным обеспечением и заданными сроками выполнения работы; - представлять результаты научно-исследовательской деятельности в виде презентаций, отчетов, устных докладов; - логически мыслить, вести научные дискуссии; - использовать справочную и научную литературу по

	тематике решаемых информационных задач, оценивать специальную информацию, систематизировать ее, принимать решение о ее дальнейшем использовании Владеть: - навыками структурирования информации по теме исследования; - навыками самостоятельного научного мышления, обобщения и систематизации информации; - навыками сбора и обработки информации в глобальной компьютерной сети, в том числе в мультидисциплинарных реферативных базах данных Scopus, Web of Knowledge; - методикой создания технического задания и технического проекта при организации НИОКР; - программными и программно-аппаратными средствами анализа систем защиты информации; - навыками поиска информации в глобальной информационной сети Интернет; - методологией научных исследований в сфере информационной безопасности; - навыками планирования научного исследования; - основными методами поиска и структурирования информации
ОПК-5 – Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	Знать: - теоретические и эмпирические методы научных исследований; - порядок проведения научных исследований; - методику проведения патентных исследований, объектом которых могут являться объекты техники, промышленной и интеллектуальной собственности (изобретения, полезные модели, программы для ЭВМ и базы данных и др.), ноу-хау и пр.; - порядок организации процесса исследования эффективности системы управления ИБ; - нормативные и методические материалы в сфере информационной безопасности; - принципы организации технического, программного и информационного обеспечения информационной безопасности; - методы построения оптимальных планов для научных экспериментов; - правила, способы и методы организации, выполнения и представления результатов научного исследования; - принципы построения и функционирования современных информационных систем; - основные элементы научно-технического эксперимента; - приемы выбора основных факторов эксперимента и технологию построения факторных планов; - требования ГОСТов на оформление научно-технической документации;

	- современные модели и методы измерения, прогнозирования, принятия решений при решении практических задач; - принципы построения вероятностных моделей применительно к практическим задачам Уметь: - применять методы научных исследований в научной деятельности, в частности, при написании магистерской диссертации и научных статей; - составлять отчеты о патентных исследованиях по ГОСТ; - формализовать задачи анализа безопасности информационных систем, разрабатывать методики исследования и применять инструментальные средства анализа безопасности; - составлять и корректировать план проведения работ в зависимости от полученных результатов; - оформлять и представлять результаты, полученные в ходе выполнения научно-исследовательского проекта грамотно, лаконично, в достаточном объеме на русском и иностранном языках; - выбирать и применять в профессиональной деятельности экспериментальные и расчетно-теоретические методы исследований; - работать со специальными программными средствами для оформления проектной и отчетной документации; - обобщать полученные экспериментальные данные, анализировать и делать выводы Владеть: - навыками оформления научных публикаций в соответствие с шаблоном IEEE, требованиями научных конференций; - теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ; - методикой оформления отчетов по научно-исследовательским работам согласно ГОСТ; - навыками выбора и обоснования критериев оценки защищенности открытых информационных систем; - навыками обработки, оценки и представления результатов исследования эффективности решений по управлению информационной безопасностью; - навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации; - навыками анализа получаемых результатов и формулировки выводов; - навыками формирования и аргументированного обоснования собственной позиции по различным проблемам защиты информации;
--	---

	- навыками представления результатов работы в виде презентаций, пояснительных записок, научных докладов и статей; - навыками самостоятельной работы, самоорганизации
ПК-1 – Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	Знать: - основные подходы к математическому моделированию и прогнозированию информационных угроз; - организационную структуру предприятия и место отдела информационной безопасности; - требования и виды моделей систем защиты информации в автоматизированных системах; - международное, российское законодательство (стандарты) в области защиты информации и способы их применения при защите современных технологичных информационных объектов; - корпоративные стандарты по управлению информационными рисками; - модели и методы анализа и управления информационными рисками; - модели управления информационной безопасностью; - модели надежности программных систем.
	Уметь: - создавать политику и регламенты информационной безопасности; - управлять информационными рисками; - проводить аудит систем управления информационной безопасностью; - осуществлять методологический анализ процесса решения задач моделирования и прогнозирования информационных угроз; - проводить анализ информационных рисков; - анализировать надежность программного обеспечения АС; - адаптировать международные и отечественные стандарты при защите современных технологичных информационных объектов; - оценивать затраты и риски.
	Владеть: - навыками разработки теоретических и экспериментальных моделей защиты информации в АС; - методиками получения оценки информационных рисков, в т.ч. остаточных рисков; - методами управления информационными рисками; - навыками адаптировать международные и отечественные стандарты при защите современных технологичных информационных объектов; - навыками работы с автоматизированными комплексами разработки и управления информационными рисками и политикой безопасности

ПК-2 – Способен разрабатывать системы и комплексы обеспечения информационной безопасности	информационной системы.
	Знать: - международные и отечественные стандарты и способы их применения при защите современных технологичных информационных объектов; - требования нормативных документов по обеспечению информационной безопасности на предприятии; - правила оформления организационно-распорядительной документации по вопросам защиты информации; - виды угроз и уязвимости для информационных активов предприятия; - методы защиты информации от различных видов угроз; - методы управления рисками информационной безопасности.
	Уметь: - адаптировать международные и отечественные стандарты при защите современных технологичных информационных объектов; - анализировать информационные ресурсы предприятия с целью выявления конфиденциальной информации; - оформлять нормативную документацию по информационной безопасности предприятия; - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности; - применять отечественные и зарубежные стандарты в области информационной безопасности.
	Владеть: - навыками адаптировать международные и отечественные стандарты при защите современных технологичных информационных объектов; - методами количественного анализа процессов обработки, поиска и передачи информации; - методикой отнесения информации к коммерческой тайне; - методикой выявления и анализа, потенциально существующих угроз безопасности информации, составляющей коммерческую тайну; - методами анализа и оценки риска, методами определения размеров возможного ущерба вследствие разглашения сведений, составляющих коммерческую тайну; - методами организации и моделирования комплексной системы защиты информации,

	составляющей коммерческую тайну.
ПК-3 – Способен организовать управление информационной безопасностью	Знать: - требования нормативных документов по обеспечению информационной безопасности на предприятии; - правила оформления организационно-распорядительной документации по вопросам защиты информации; - виды угроз и уязвимости для информационных активов предприятия; - методы защиты информации от различных видов угроз; - методы управления рисками информационной безопасности; - основные принципы, методы и средства организации управления информационной безопасностью; - основные угрозы безопасности информации и модели нарушителя;
	Уметь: - анализировать информационные ресурсы предприятия с целью выявления конфиденциальной информации; - оформлять нормативную документацию по информационной безопасности предприятия; - анализировать и оценивать угрозы информационной безопасности объекта; - пользоваться нормативными документами по защите информации; - осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности; - применять отечественные и зарубежные стандарты в области информационной безопасности; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - контролировать эффективность принятых мер по реализации частных политик информационной безопасности;
	Владеть: - методами количественного анализа процессов обработки, поиска и передачи информации; - методикой отнесения информации к коммерческой тайне; - методикой выявления и анализа, потенциально существующих угроз безопасности информации, составляющей коммерческую тайну; - методами анализа и оценки риска, методами определения размеров возможного ущерба вследствие разглашения сведений, составляющих коммерческую тайну;

	- методами организации и моделирования комплексной системы защиты информации, составляющей коммерческую тайну; - методами управления комплексной системой защиты информации, составляющей коммерческую тайну; - методами организации и управления службами защиты информации; - навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; - методами оценки информационных рисков; - навыками участия в экспертизе состояния защищенности информации на объекте защиты.
ПК-4 – Способен организовывать работу по созданию или модернизации систем обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	Знать: - положения правовых нормативных актов и нормативных методических документов ФСБ РФ, ФСТЭК РФ по созданию или модернизации систем обеспечения информационной безопасности; - методы организации работы по созданию или модернизации систем обеспечения информационной безопасности; - методы защиты информации от различных видов угроз; - методы управления рисками информационной безопасности; - принципы построения систем обеспечения информационной безопасности объектов информатизации;
	Уметь: - применять на практике положения правовых нормативных актов и нормативных методических документов ФСБ РФ, ФСТЭК РФ; - организовывать работу по созданию или модернизации систем обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.
	Владеть: - навыками применения положений правовых нормативных актов и нормативных методических документов ФСБ РФ, ФСТЭК РФ; - навыками организации работ по созданию или модернизации систем обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.
ПК-5 – Способен принимать значимость информационной безопасности, как системообразующего фактора сфер жизни современного	Знать: - направления и тенденции развития современных вычислительных и информационно-коммуникационных средств и систем, средств обеспечения информационной безопасности;

общества, ее влияния на состояние экономической, политической, оборонной и других составляющих национальной безопасности	- степень зависимости современного общества, состояния экономической, политической, оборонной и других составляющих национальной безопасности от уровня обеспечения информационной безопасности. Уметь: - определять актуальные угрозы безопасности защищаемого объекта информатизации; - принимать значимость информационной безопасности, как системообразующего фактора сфер жизни современного общества, ее влияния на состояние экономической, политической, оборонной и других составляющих национальной безопасности. Владеть: - навыками анализа направлений и тенденций развития современных вычислительных и информационно-коммуникационных средств и систем, средств обеспечения информационной безопасности; - навыками определения актуальных угроз безопасности защищаемого объекта информатизации.
ПК-6 – Способен выявлять, анализировать и устранять различные каналы утечки и средства съема информации, используемые техническими разведками, а также применять методы и средства противодействия техническим разведкам	Знать: - источники возникновения различных технических каналов утечки информации; - принципы функционирования и устройство средств съема информации; - методы и средства противодействия техническим разведкам. Уметь: - выявлять источники возникновения различных технических каналов утечки информации; - выявлять, анализировать и устранять различные каналы утечки и средства съема информации, используемые техническими разведками; - применять методы и средства противодействия техническим разведкам. Владеть: - навыками и методами выявления источников возникновения различных технических каналов утечки информации; - навыками и методами выявления, анализа и устранения различных каналов утечки и средств съема информации, используемых техническими разведками; - навыками применения методов и средств противодействия техническим разведкам.

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 15 зачетных единиц (540 часов), 10 недель.

Таблица 6.1.

№ п/п	Разделы (этапы) практики	Виды учебной деятельности на практике, включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля
	Подготовительный этап	6	
1	Установочная конференция	2	отчет
2	Предварительный инструктаж	4	отчет
	Основной этап	498	
3	Изучение структуры организации и органов защиты информации	30	отчет
4	Изучение видов угроз безопасности информации, характерных для организации	30	отчет
5	Изучение способов, средств и методов защиты информации, применяемых в организации	30	отчет
6	Изучение и подбор материала темы дипломной работы	120	отчет
7	Написание статьи совместно с руководителем дипломной работы	60	отчет
8	Выполнение индивидуального задания по теме выпускной квалификационной работы	228	отчет
	Обработка и анализ полученной информации	36	
9	Подготовка отчета о выполнении преддипломной практики	30	отчет
10	Итоговая конференция	6	отчет
	Итого	540	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 преддипломной практики (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 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 безопасности; показано умение применять теоретические знания на практике в ситуациях легкой и средней тяжести; хорошее ориентирование в технической литературе и предоставленной на практике документации.	82-89	хорошо
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	75-81	

	на практике в ситуациях легкой и средней тяжести; хорошее ориентирование в технической литературе и предоставленной на практике документации.		
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 10.04.01 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 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 информационных технологий

Кафедра (департамент) «Информационная безопасность»

Уровень образования магистратура

Направление подготовки 10.04.01 Информационная безопасность

Профиль Управление информационной безопасностью в органах государственной власти

___ 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 практики от Университета

(подпись)

(должность, фамилия и инициалы ответственного лица)

Руководитель практики от профильной организации

(ПОДПИСЬ)

(должность, фамилия и инициалы ответственного лица)

« » 20 г.

Рабочий график (план) прохождения практики

[illegible]

Руководитель практики от Университета

(подпись)

(должность, фамилия и инициалы ответственного лица)

Руководитель практики от профильной организации

(ПОДПИСЬ)

(должность, фамилия и инициалы ответственного лица)

« » 20 г.

[illegible]

Отзыв (характеристика)

(фамилия, имя, отчество обучающегося)

Руководитель практики от профильной организации

(подпись)

(должность, фамилия и инициалы ответственного лица)

« ____ » _____ 20__ г.

Сведения об уровне усвоения обучающимися компетенций

№ п/п	Формируемые компетенции	Руководитель от профильной организации	Руководитель от Университета
1.	ПК-1 – способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена
2.	ПК-2 – способность разрабатывать системы и комплексы обеспечения информационной безопасности	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена
3.	ПК-3 – способность организовать управление информационной безопасностью	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена
4.	ПК-4 – способность организовывать работу по созданию или модернизации систем обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена
5.	ПК-5 – способность принимать значимость информационной безопасности, как системообразующего фактора сфер жизни современного общества, ее влияния на состояние экономической, политической, оборонной и других составляющих национальной безопасности	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена
6.	ПК-6 – способность выявлять, анализировать и устранять различные каналы утечки и средства съёма информации, используемые техническими разведками, а также применять методы и средства противодействия техническим разведкам	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена

Руководитель практики от Университета

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

Руководитель практики от профильной организации

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

« ____ » _____ 20 ____ г.

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

(фамилия, имя, отчество обучающегося)

Дата сдачи отчета «___» _____ 20__ г.

Оценка: _____

Руководитель практики от Университета

(подпись)

(должность, фамилия и инициалы ответственного лица)

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 информационных технологий

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 10.04.01
Информационная безопасность
 (код, наименование)

Руководитель практики от Университета

 (должность)

 (Фамилия И.О. руководителя)

Севастополь
 20__ г.