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
(инициалы, фамилия)
«10» 04 2023 г.

УТВЕРЖДАЮ
Директор Института
информационных технологий

В.Н. Бондарев
(инициалы, фамилия)
«10» 04 2023 г.
М.П.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика
(вид практики)

Б2.В.01(П) Эксплуатационная 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, 2023
(форма обучения, год набора)

Севастополь
2023 г.

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 2023 г., протокол № 11.

Руководитель образовательной программы _____ Ю.Ю. Гончаренко
(подпись) (И.О. Фамилия)

Программа составлена:
Старший преподаватель _____ В.В. Пелись
(должность, ученая степень, ученое звание) (подпись) (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 _____ В.С. Кобизской
(должность, ученая степень, ученое звание) (подпись) (И.О. Фамилия)

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.

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 в выполнении комплекса работ по обеспечению информационной безопасности предприятия;

– получение практических навыков в оформлении нормативных документов, регламентирующих деятельность в сфере информационной безопасности;

– 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.).

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. Практика относится к рекомендуемым ФГОС типам практики.

Практика проводится во 2 семестре при очной и очно-заочной формах обучения, базируется на учебных дисциплинах: «Методология исследовательской деятельности в информационной безопасности», «Системы радиомониторинга и выявления негласного съема информации», «Защищенные информационные системы», «Научный семинар», «Управление информационной безопасностью», «Методы и средства защиты информации», «Технологии обеспечения информационной безопасности», «Организационно-правовые механизмы обеспечения информационной безопасности»,

«Математическое моделирование и прогнозирование информационных угроз», «Противодействие техническим разведкам и основы радиоэлектронной борьбы», «Актуальные вопросы противодействия информационным угрозам» / «Управление инцидентами информационной безопасности», «Организация и профессиональная подготовка сотрудников службы информационной безопасности», «Физические основы технических средств защиты информации (практикум)», «Технологии массовых коммуникаций в информационном противоборстве» и является основой для преддипломной практики, а также для подготовки к процедуре защиты и защиты выпускной квалификационной работы.

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 - эксплуатационная.

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 при очной и очно-заочной формах обучения во 2 семестре – концентрированная.

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, 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 эксплуатационной практики в учебном процессе определяет ее важную роль в подготовке магистрантов к практическому внедрению научных результатов - важному этапу инновационной деятельности. Выполняемые в рамках эксплуатационной практики

проектные работы составляют основу соответствующих разделов выпускной квалификационной работы специалиста. Выполнение эксплуатационной 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-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 зашиты 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 информационной системы.
ПК-2 – Способен разрабатывать системы и комплексы обеспечения информационной безопасности	**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-5 – Способен принимать значимость информационной безопасности, как системообразующего фактора сфер жизни современного общества, ее влияния на состояние экономической, политической, оборонной и других составляющих национальной безопасности	**Знать:** - направления и тенденции развития современных вычислительных и информационно-коммуникационных средств и систем, средств обеспечения информационной 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 съёма 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 съёма 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 съёма информации, используемых техническими разведками; - навыками применения методов и средств противодействия техническим разведкам.

6 Структура и содержание практики

Эксплуатационная практика 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 эксплуатационной практики; итоговая конференция; защита по результатам прохождения практики; выставление оценок.

6.1. Структура практики

Трудоемкость практики составляет при всех формах обучения 6 зачетных единиц (216 часов), 4 недели.

Таблица 6.1.

№ п/п	Разделы (этапы) практики	Виды учебной деятельности на практике, включая самостоятельную работу студентов и трудоемкость (в часах)		Формы текущего контроля
		ОФО	ОЗФО	
	Подготовительный этап	**4**	**4**	
1	Установочная конференция	2	2	Отчет
2	Предварительный инструктаж	2	2	Отчет
	Производственный этап	**142**	**142**	
3	Изучение структуры и органов защиты информации организации	16	16	Отчет
4	Изучение видов угроз безопасности информации, характерных для организации	16	16	Отчет
5	Изучение способов, средств и методов защиты информации, применяемых в организации	24	24	Отчет
6	Практическое выполнение обязанностей на различных должностях в зависимости от возможностей организации	70	70	Отчет
7	Изучение перспектив и направлений развития средств защиты информации	16	16	Отчет

	в организации			
	Обработка и анализ полученной информации	**70**	**70**	
8	Выполнение индивидуального задания.	40	40	Отчет
9	Подготовка отчета о выполнении эксплуатационной практики	24	24	Отчет
10	Итоговая конференция	6	6	
	Итого	**216**	**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 эксплуатационной 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 эксплуатационной 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 эксплуатационной 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, реферат 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
A	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
B	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
C	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	69-74	удовлетворительно

Оценка ECTS	Определение оценки в системе ECTS	Оценка по 100-балльной шкале	Оценка по национальной шкале
	большей части технической документации; обучающийся проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов.		
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 10.04.01 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 учебной практики в распоряжение студентов предоставлены компьютерные классы кафедры «Информационная безопасность», укомплектованные современным вычислительным оборудованием и периферией, специализированные учебные и научно-исследовательские лаборатории различного профиля.

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

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

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

Приложение 1
Пример оформления дневника практики

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

ДНЕВНИК ПРАКТИКИ

Производственная (эксплуатационная) 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

№ п/п	Вопросы, подлежащие изучению	Источник информации
	(перечень вопросов заполняет руководитель практики от Университета)	

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

№ п/п	Дата	Наименование работ	Отметка о выполнении
		(заполняет руководитель практики от университета)	

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.

Рабочие записи во время практики

Отзыв (характеристика)

_____

(фамилия, имя, отчество обучающегося)

Руководитель практики от профильной организации

_____ _____

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

«____» _____ 20___ г.

Сведения об уровне усвоения обучающимся 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-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
4.	**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)

Приложение 2

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.

Приложение 3

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 (эксплуатационной) практике
(вид практики) (тип практики)

в _____
(наименование организации)

Выполнил _____
(Фамилия И.О. обучающегося)

_____
(шифр группы)

Направление 10.04.01
Информационная безопасность
(код, наименование)

Руководитель практики от Университета

_____
(должность)

_____
(Фамилия И.О. руководителя)

Севастополь
20__ г.