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

«10» 04 2024 г.

М.П.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика
(вид практики)

Б2.В.02(П) Научно-исследовательская работа
(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» от «10» апреля 2024 г., протокол № 11.

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

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

Рецензент:
Начальник Управления защиты государственной тайны и мобилизационной работы Правительства г. Севастополя _____ (подпись) В.С. Кобизской (И.О. Фамилия)
(должность, ученая степень, ученое звание)

1 Цели практики

Целью выполнения научно-исследовательской работы (далее - НИР) является подготовка материалов по теме магистерской диссертации.

2 Задачи практики

Задачами НИР являются:

– определение вида и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов, целей и задач деятельности данного объекта обследования;

– выполнение работ по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации на конкретных объектах информатизации;

– по теме магистерской диссертации описать вид и форму информации, подверженной угрозам, возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов, целей и задач деятельности заданного объекта обследования;

– выполнение работ по оформлению магистерской диссертации и разработке ее презентации.

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. НИР относится к части, формируемой участниками образовательных отношений блока Б2 учебного плана ООП.

НИР проводится в 1, 2 и 3 семестрах при очной и очно-заочной формах обучения, базируется на всех изученных ранее учебных дисциплинах и является основой подготовки выпускной квалификационной работы.

Приступая к выполнению НИР, 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 педагогической деятельности; использовать на практике методы гуманитарных, социальных и экономических наук в различных видах профессиональной и социальной деятельности;

- ***владеть*** (быть в состоянии продемонстрировать): навыками научного анализа социально-значимые 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 деятельности и работы различных коллективов.

4 Тип практики, способ и форма ее проведения

Тип практики – научно-исследовательская работа.

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) или выездная (по договорам на предприятиях, в учреждениях, организациях, расположенных за пределами г. Севастополя).

Форма проведения практики – рассредоточенная практика.

НИР представляет собой вид учебных занятий, непосредственно ориентированных на профессионально-практическую подготовку обучающихся. В период прохождения практики у студентов формируются практические навыки работы по направлению подготовки, умения принимать самостоятельные решения на конкретных участках работы в реальных условиях, целостное представление о содержании, видах и формах профессиональной деятельности.

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 подготовке и оформлении выпускной квалификационной работы (магистерской диссертации).

Практика проводится в 1, 2 и 3 семестрах 1 и 2 годов обучения (курсов) и является базовой для преддипломной практики, а также 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-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

Формируемые в результате освоения ООП компетенции	Планируемые результаты обучения при прохождении практики
	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

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	**Знать:** - международные и отечественные стандарты и

Формируемые в результате освоения ООП компетенции	Планируемые результаты обучения при прохождении практики
комплексы обеспечения информационной безопасности	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.

6 Структура и содержание практики

НИР 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 производственной практики; итоговая конференция; защита по результатам прохождения практики; выставление оценок.

6.1. Структура практики

Общая трудоемкость НИР составляет 18 зачетных единиц (648 часов) (по 6 з.е. в каждом семестре).

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	**12**	
1	Установочная конференция	6	отчет
2	Предварительный инструктаж	6	отчет
	Основной этап	**606**	
3	Изучение структуры организации и органов защиты информации	54	отчет
4	Изучение видов угроз безопасности информации, характерных для организации	54	отчет
5	Изучение способов, средств и методов защиты информации, применяемых в организации	90	отчет
6	Изучение и подбор материала по теме выпускной квалификационной работы	198	отчет
7	Написание статьи совместно с руководителем дипломной работы	60	отчет
8	Выполнение индивидуального задания по теме выпускной квалификационной работы	150	отчет
	Обработка и анализ полученной информации	**30**	
9	Подготовка отчета о выполнении производственной практики	24	отчет
10	Итоговая конференция	6	отчет
	Итого	**648**	**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. Основной этап*:** рассматриваются более детально основные вопросы, вынесенные на практику.

- изучение структуры и органов защиты информации организации;
- изучение видов угроз безопасности информации, характерных для организации;
- изучение способов, средств и методов защиты информации, применяемых в организации;
- изучение и подбор материала по теме выпускной квалификационной работы;
- написание статьи совместно с руководителем дипломной работы;
- выполнение индивидуального задания по теме выпускной квалификационной работы, которое он должен выполнить в виде реферата (20-25 страниц печатного текста).

6.2.3. Обработка и анализ полученной информации:

- подготовка отчета о выполнении производственной 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 выполнения НИР 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 НИР 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, 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	82-89	хорошо

	литературе и предоставленной на практике документации.		
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 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

Приложение 1
Пример оформления дневника практики

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

ДНЕВНИК ПРАКТИКИ

Производственная практика (научно-исследовательская работа)
(вид и тип практики)

обучающегося
(Фамилия, Имя, Отчество)

Институт информационных технологий

Кафедра (департамент) «Информационная безопасность»

Уровень образования бакалавриат

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.	**УК-2** – способность управлять проектом на всех этапах его жизненного цикла	освоена / освоена частично / не освоена	освоена / освоена частично / не освоена
2.	**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
3.	**ПК-2** – способность разрабатывать системы и комплексы обеспечения информационной безопасности	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 практике (научно-исследовательской работе)
(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.