МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

13.02.2024 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ/НИР

ПРОИЗВОДСТВЕННАЯ - ПРЕДДИПЛОМНАЯ ПРАКТИКА

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	6
Семестр	11

Магнитогорск
2024 год

Программа практики/НИР составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Программа практики/НИР рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2024 протокол №4

Зав. кафедрой _____ И.И. Баранкова

Программа практики/НИР одобрена методической комиссией ИЭиАС
13.02.2024 г. Протокол № 4

Председатель _____ В.Р. Храмшин

Программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Кузьмина

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО) ,
_____ М.М. Близнецов

Лист актуализации программы

Программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели практики/НИР

Целями производственной преддипломной практики для специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются: закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин базовой и вариативной части ОП, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника; изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты; изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.

2 Задачи практики/НИР

Задачами производственной преддипломной практики являются закрепление, расширение, углубление и систематизацию знаний, полученных при изучении дисциплин базовой и вариативной части, на основе изучения деятельности конкретной организации, приобретение практического опыта, а также обобщение и систематизация разделов выпускной квалификационной работы.

Программа практики по специальности обеспечивает обоснованную последовательность формирования у обучающихся единой системы профессиональных умений и навыков в соответствии с профилем деятельности специалиста. При организации и проведении практики заложен модульный принцип, который осуществляет привязку задания к конкретному предприятию, обеспечивающему его выполнение.

3 Место практики/НИР в структуре образовательной программы

Для прохождения практики/НИР необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Информатика

Управление информационной безопасностью

Анализ рисков информационной безопасности

Форензика

Методы проектирования систем защиты распределенных информационных систем

Защита электронного документооборота

Защита программного обеспечения

Аттестация АИС

Тестирование систем защиты информации автоматизированных систем

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Моделирование систем защиты информации

Организация ЭВМ и вычислительных систем

Знания (умения, владения), полученные в процессе прохождения практики/НИР будут необходимы для изучения дисциплин/практик:

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

4 Место проведения практики/НИР

Производственная практика по получению профессиональных умений и опыта профессиональной деятельности проводится на базе кафедры «Информатики и информационной безопасности», в лабораториях технических средств защиты информации, защищенных автоматизированных систем, программно-аппаратных средств обеспечения информационной безопасности, сетей и систем передачи информации, безопасности сетей ЭВМ ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», ООО «ММК-Информсервис», ПАО «Магнитогорский металлургический комбинат», и других предприятиях г. Магнитогорска, а также Управление ФСТЭК России по УрФО, г. Екатеринбург.

Способ проведения практики/НИР: нет

Практика/НИР осуществляется дискретно

5 Компетенции обучающегося, формируемые в результате прохождения практики/НИР и планируемые результаты обучения

В результате прохождения практики/НИР обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-1 Способен проводить анализ безопасности компьютерных систем	
ПК-1.1	Оценивает эффективность защиты информации
ПК-1.2	Применяет разработанные методики оценки защищенности программно-аппаратных средств защиты информации
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	
ПК-2.1	Разрабатывает профили защиты компьютерных систем
ПК-2.2	Формирует политики безопасности компьютерных систем и сетей
ПК-3 Способен анализировать причины возникновения компьютерных инцидентов	
ПК-3.1	Определяет причину и условия изменения программного обеспечения
ПК-3.2	Определяет принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой
ПК-3.3	Прогнозирует возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	
ПК-4.1	Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем
ПК-4.2	Применяет методы анализа защищенности компьютерных систем и сетей
ПК-5 Способен проводить аттестацию объектов на соответствие требованиям по защите информации	
ПК-5.1	Проводит аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации
ПК-5.2	Оформляет материалы аттестационных испытаний на соответствие требованиям по защите информации
ПК-5.3	Оформляет аттестат соответствия объектов вычислительной техники требованиям по защите информации

ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	
ПК-6.1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

6. Структура и содержание практики/НИР

Общая трудоемкость практики/НИР составляет 6 зачетных единиц 216 акад. часов, в том числе:
– контактная работа – 2,5 акад. часов:
– самостоятельная работа – 213,5 акад. часов;
– в форме практической подготовки – 216 акад. часов.

№ п/п	Разделы (этапы) и содержание практики	Семестр	Виды работ на практике, включая самостоятельную работу	Код компетенции
1.	Подготовительный (ознакомительный)	11	Инструктаж по технике безопасности. Прослушивание вводного инструктажа по охране труда и изучение спецкурса в рамках образовательной программы. Получение индивидуальных заданий. Изучение требования по оформлению отчетности и защиты отчетов по практике.	ПК-2.2, ПК-3.1, ПК-3.2, ПК-4.2
2.	Экспериментально-исследовательский	11	Сбор фактического и литературного материала	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-5.1, ПК-5.2, ПК-5.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
3.	Обработка и анализ полученной информации.	11	Обработка и систематизация фактического и литературного материала.	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.2, ПК-5.2, ПК-5.3, ПК-6.4, ПК-7.1, ПК-7.4
4.	Отчетный	11	Подготовка итогового отчета	ПК-1.2, ПК-2.1, ПК-2.2, ПК-3.1, ПК-3.2, ПК-3.3, ПК-5.1, ПК-5.2, ПК-5.3, ПК-1.1, ПК-4.1, ПК-4.2, ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4

7 Оценочные средства для проведения промежуточной аттестации по практике/НИР

Представлены в приложении 1.

8 Учебно-методическое и информационное обеспечение практики/НИР

а) Основная литература:

1. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997108 (дата обращения: 31.01.2024)

2.Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 31.01.2024).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452430 (дата обращения: 31.01.2024).

4. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453063 (дата обращения: 31.01.2024).

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437163 (дата обращения: 31.01.2024).

6. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва : Издательство Юрайт, 2019. — 220 с. — (Университеты России). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437667 (дата обращения: 31.01.2024).

7. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 31.01.2024)

б) Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 31.01.2024).

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 31.01.2024)

МАКРООБЪЕКТЫ:

3. Сетевая защита информации. Лабораторный практикум : учебное пособие

[для вузов] / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/2400. - ISBN 978-5-9967-1605-0. - Текст : электронный*.

4. Развертывание и настройка виртуальных сетей : учебное пособие [для вузов] / [сост.: В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/2388. - ISBN 978-5-9967-1305-9. - Текст : электронный*.

5. Архитектура и принципы работы вычислительных систем : учебное пособие [для вузов] / В. В. Баранков, И. И. Баранкова, М. В. Коновалов, М. В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/2495. - ISBN 978-5-9967-1306-6. - Текст : электронный*.

6. Мазнин Д. Н. Администрирование компьютерных сетей : учебное пособие [для вузов] / Д. Н. Мазнин, Ю. А. Мазнина. - Магнитогорск : МГТУ им. Г. И. Носова, 2023. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/21027. - ISBN 978-5-9967-2906-7. - Текст : электронный*.

7.Баранкова И. И. Техническая защита информации. Лабораторный практикум : учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/1747. - Текст : электронный*.

8. Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/1858. - ISBN 978-5-9967-1031-7. - Текст : электронный*.

9. Организация обработки и защиты ПДН в вузе : учебное пособие [для вузов] / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, Д. А. Илларионова ; Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, Д. А. Илларионова ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/2690. - ISBN 978-5-9967-1736-1. - Текст : электронный.

10. Баранкова И. И. Системы контроля и управления доступом : практикум [для вузов] / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2020. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/2913. - Текст : электронный*.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронной библиотеки МГТУ им. Г. И. Носова https://host.megaprolib.net/MP0109/Web.

2. Произвести авторизацию на портале (логин: Фамилия на русском языке, пароль: номер читательского билета)

3. Активизировать гиперссылку макрообъекта.

в) Методические указания:

Методические указания по выполнению самостоятельных работ по производственной-практике (Приложение 2).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
Oracle Virtual Box	свободно распространяемое ПО	бессрочно
WordPress	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Visual Studio	свободно распространяемое ПО	бессрочно
MS Visual Studio	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
MS Windows 10	К-79-21 от 22.11.2021	бессрочно
Браузер Mozilla	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Calculate Linux	свободно распространяемое ПО	бессрочно
MariaDB	свободно распространяемое ПО	бессрочно
PostgreSQL	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
VIP Net Client	Д-946-14 от 22.07.2014	бессрочно
VIP Net	Д-946-14 от 22.07.2014	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View	https://dlib.eastview.com/
Национальная информационно-аналитическая система	URL:
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Федеральное государственное бюджетное учреждение	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers
Электронные ресурсы библиотеки МГТУ им. Г.И.	https://host.megaprolib.net/M
Федеральный образовательный портал – Экономика.	http://ecsocman.hse.ru/
Международная база полнотекстовых журналов	http://link.springer.com/
Международная реферативная и полнотекстовая	https://www.nature.com/sitein
Архив научных журналов «Национальный	https://arch.neicon.ru/xmlui/
база данных патентного поиска - база данных Orbit	https://www.orbit.com/
Информационная система - Нормативные правовые	https://fstec.ru/tekhnicheskaya
Информационная система - Банк данных угроз	https://bdu.fstec.ru/?

9 Материально-техническое обеспечение практики/НИР

необходимой для выполнения задания по практике и написанию отчета.

Организации, учреждения и предприятия, а также учебно-научные подразделения Университета должны обеспечить рабочее место обучающегося компьютерным оборудованием в объемах, достаточных для достижения целей практики.

Аудитории для самостоятельной работы (компьютерные классы; читальные залы библиотеки) оснащены персональными компьютерами с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета».

Материально-техническое обеспечение учебной практики по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности включает:

Комплекс радиомониторинга «Касандра К-6».

Комплекс радиомониторинга «Касандра К-21».

Анализатор спектра «АКС-1301».

Комплект оборудования для мониторинга информационной безопасности.

Комплект оборудования контроля доступа.

Комплект оборудования для построения сети ZigBee.

Комплект оборудования SECURITY-CISCO-3M.

Портативный поисковый комплекс амплитудной пеленгации «Касандра С6»

Система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) Сигурд

Программно-аппаратный комплекс для измерения параметров волоконно-оптических систем передачи и оценки защищенности оптических линий связи Лазурит

Фильтр сетевой помехоподавляющий «ЛФС-100-3Ф»

Генератор шума ГШ-1000М.

Соната-АВ (модель 3М) система виброакустической и акустической защиты (Центральный ГШ): Генераторный блок (Модель 3М) + Аудиоизлучатель АИ-3М + «Тяжелый» виброизлучатель ВИ-3М + «Легкий» виброизлучатель ПИ-3М.

Устройство защиты Прокруст 2000.

Устройство КРИПТОН-ЗАМОК/У (АПМДЗ-У, М-526Б).

Устройства для защиты линий электропитания и заземления от утечки информации «Соната-РС2» исп. 208.

Комплект оборудования «Беспроводные компьютерные сети ЭВМ».

Модуль «Низкоуровневый контроллер Ethernet»

Комплект коммуникационного оборудования с сервером для моделирования облачного сервиса

Электронные ключи Guardant, eToken.

Комплект оборудования пользовательского сегмента системы GPS.

Комплект оборудования ТЛС-1.

Комплект оборудования VOIP.

Комплект оборудования «Кодирование и модуляция информации в системах связи».

Комплект оборудования «Исследование дистанционной передачи информации»

ПРИЛОЖЕНИЕ 1

Оценочные средства для проведения промежуточной аттестации по практике/НИР

Промежуточная аттестация по практике имеет целью определить степень достижения запланированных результатов обучения и проводиться в форме зачета с оценкой.

Обязательной формой отчетности обучающегося по практике является письменный отчет. Цель отчета – сформировать и закрепить компетенции, приобретенные обучающимся в результате освоения теоретических курсов и полученные им при прохождении практики. Отчеты обучающихся по практикам позволяют руководителям образовательных программ создавать механизмы обратной связи для внесения корректив в образовательный процесс.

Примерная структура и содержание раздела:

Промежуточная аттестация по производственной практике по получению профессиональных умений и опыта профессиональной деятельности имеет целью определить степень достижения запланированных результатов обучения и проводиться в форме зачета с оценкой.

Зачет с оценкой выставляется обучающемуся за подготовку и защиту отчета по практике.

Подготовка отчета выполняется обучающимся самостоятельно под руководством преподавателя. При написании отчета обучающийся должен показать свое умение работать с нормативным материалом и литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

Содержание отчета определяется индивидуальным заданием, выданным руководителем практики. В процессе написания отчета обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

На протяжении всего периода прохождения практики обучающийся должен вести дневник по практике, который будет являться приложением к отчету.

Примерное содержание отчета должно включать следующие разделы:

1. Титульный лист.
2. Аннотация.
3. Содержание.
4. Раздел 1.
5. Раздел 2.
6. Заключение.
7. Список использованных источников.

Титульный лист отчета оформляется в соответствии с СМК-О-ПВД-01-16. Аннотация отчета по производственной практике должна содержать краткую характеристику отчета. В разделе 1 должен включать краткое описание учреждения, где проходила практика, основы организации его деятельности, вопросы информационной безопасности и техники безопасности. В разделе 2 описывается тема индивидуального задания.

Готовый отчет сдается на проверку преподавателю не позднее 3-х дней до окончания практики. Преподаватель, проверив отчет, может возвратить его для доработки вместе с письменными замечаниями. Обучающийся должен устранить полученные замечания и публично защитить отчет.

Примерное индивидуальное задание на производственную преддипломную практику:

Цель прохождения практики:

– закрепление и углубление теоретических знаний, полученных обучающимися при изучении дисциплин обще-профессионального цикла и дисциплин специализации, приобретение и развитие необходимых практических умений и навыков в соответствии с требованиями к уровню подготовки выпускника;

– изучение обязанностей должностных лиц предприятия, обеспечивающих решение проблем защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств ее обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;

– изучение источников информации и системы оценок эффективности применяемых мер обеспечения защиты информации.

Задачи практики:

– ознакомиться с нормативно-правовой документацией организации;

– изучить структуру организации;

– изучить и провести анализ должностных инструкций сотрудников организации;

– изучить и провести анализ решений по обеспечению ИБ предприятия;

– изучить и провести анализ методов контроля за исполнением принятых решений;

– проведение статистических исследований;

– изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;

Вопросы, подлежащие изучению:

1) Род деятельности предприятия, на котором проходила практика.
2) Какие способы защиты информации используются на предприятии?
3) Какие программные средства используются для обеспечения информационной безопасности на предприятии?
4) Какие аппаратно-технические средства используются для обеспечения информационной безопасности?
5) Какая топология используется в локальных сетях на предприятии?
6) Как обеспечивается безопасность беспроводных сетей?
7) Как обеспечивается безопасность по виброакустическим каналам передачи информации?
8) Охарактеризуйте должностные обязанности лиц ответственных за обеспечение информационной безопасности на предприятии.
9) Какие нормативные акты и законы РФ используются лицами ответственными за обеспечение информационной безопасности на предприятии при выполнении свои обязанностей.
10) Опишите способы контроля трафика по локальным сетям предприятия.
11) При помощи, каких программно-аппаратных средств ограничивается доступ персонала предприятия в глобальную сеть.
12) Как обеспечивается защита локальной сети предприятия от угроз из глобальной сети?
13) При помощи, каких программных средств осуществляется администрирование

ПК персонала предприятия?

14) Какие операционные системы используются на ПК персонала предприятия?
15) Какие операционные системы используются на серверах предприятия?
16) Понятие и виды защищаемой информации по законодательству РФ.
17) Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
18) Принципы, механизмы и процедура отнесения сведений к государственной тайне. Реквизиты носителей сведений, составляющих государственную тайну.
19) Конфиденциальная информация и ее виды. Правовые режимы конфиденциальной информации: содержание и особенности.
20) Виды деятельности в информационной сфере, подлежащие лицензированию и участники лицензионных отношений в сфере защиты информации.
21) Правовая регламентация сертификатной деятельности в области защиты информации. Режимы и объекты сертификации.
22) Понятие интеллектуальной собственности. Объекты и субъекты авторского и смежного права.
23) Организационная структура отдела (службы) безопасности и основные обязанности сотрудников по защите информации предприятия (организации).
24) Основное содержание разработки Политики безопасности предприятия (организации).
25) Принципы, основные задачи и функции обеспечения информационной безопасности.
26) Раскрыть содержание правовых основ защиты информации. Законодательные источники права на доступ к информации.
27) Основные уровни доступа к информации с точки зрения законодательства. Меры по обеспечению сохранности сведений, составляющих государственную тайну.
28) Ответственность за нарушение законодательства в информационной сфере.
29) Основные мероприятия по защите информации при проведении совещаний и переговоров.
30) Защита права на личную информацию с ограниченным доступом (классификация, обработка, правовая охрана персональных данных).
31) Виды компьютерных преступлений. Классификация компьютерных злоумышленников.
32) Раскрыть основные правовые аспекты применения электронной цифровой подписи (ЭЦП).
33) Раскрыть основной порядок проведения аттестации и контроля объектов информатизации.
34) Сформулировать основные правила безопасной работы в компьютерной системе.
35) Привести архитектуру СЗИ. Раскрыть особенности функционирования подсистем, систем и модулей защиты от НСД.
36) Перечислить виды атак на пароль. Раскрыть их особенности. Привести модели оценки стойкости парольной защиты.
37) Привести и охарактеризовать основные приемы отладки злоумышленником программного обеспечения. Указать методы противодействия отладчикам.
38) Привести и охарактеризовать основные приемы дизассемблирования программного обеспечения. Указать методы противодействия дизассемблированию программного обеспечения.
39) Классифицировать программно-аппаратные средства защиты информации. Сформулировать основные их характеристики.
40) Рассмотреть особенности разграничения доступа и аудита в СЗИ
41) Особенности реализации метода «разграничения доступа» в системах защиты информации от несанкционированного доступа.

42) Раскрыть особенности образования электромагнитных каналов утечки информации.
43) Раскрыть особенности образования и съема информации по электрическим каналам утечки информации.
44) Сформулировать основные особенности построения периметровой охраны особо важных объектов

Планируемые результаты практики:

– подготовка рекомендаций по устранению или минимизации выявленных проблем (рекомендации должны быть обоснованными, т.е. сопровождаться ссылками на соответствующие НПА или авторитетное мнение специалистов в сфере деятельности, исследователей, конкурентов, потребителей и т.п.);

– подготовка выводов о деятельности предприятий или организаций, востребованности их продуктов на соответствующих рынках, а также практических рекомендаций по совершенствованию организационных и экономических аспектов их деятельности;

– оценка эффективности проектов и программ, внедряемых на предприятиях;

– оценка качества решений по обеспечению ИБ предприятия;

– публичная защита своих выводов и отчета по практике;

– систематизация и обобщение материала для написания выпускной квалификационной работы.

Показатели и критерии оценивания:

– на оценку **«отлично»** (5 баллов) – обучающийся представляет отчет, в котором в полном объеме раскрыто содержание задания; текст излагается последовательно и логично с применением актуальных нормативных документов; в отчете дана всесторонняя оценка практического материала; используется творческий подход к решению проблемы; сформулированы экономически обоснованные выводы и предложения. Отчет соответствует предъявляемым требованиям к оформлению.

На публичной защите обучающийся демонстрирует системность и глубину знаний, полученных при прохождении практики; стилистически грамотно, логически правильно излагает ответы на вопросы; дает исчерпывающие ответы на дополнительные вопросы преподавателя; способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры.

– на оценку **«хорошо»** (4 балла) – обучающийся представляет отчет, в котором содержание раскрыто достаточно полно, материал излагается с применением актуальных нормативных документов, основные положения хорошо проанализированы, имеются выводы и экономически обоснованные предложения. Отчет в основном соответствует предъявляемым требованиям к оформлению.

На публичной защите обучающийся демонстрирует достаточную полноту знаний в объеме программы практики, при наличии лишь несущественных неточностей в изложении содержания основных и дополнительных ответов; владеет необходимой для ответа терминологией; недостаточно полно раскрывает сущность вопроса; отсутствуют иллюстрирующие примеры, обобщающее мнение обучающегося недостаточно четко выражено.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся представляет отчет, в котором содержание раскрыты слабо и в неполном объеме, выводы правильные, но предложения являются необоснованными. Материал излагается на основе неполного перечня нормативных документов. Имеются нарушения в оформлении отчета.

На публичной защите обучающийся демонстрирует недостаточно последовательные знания по вопросам программы практики; использует специальную терминологию, но допускает ошибки в определении основных понятий, которые затрудняется исправить самостоятельно; демонстрирует способность самостоятельно, но не глубоко, анализировать материал, раскрывает сущность решаемой проблемы только при наводящих вопросах преподавателя; отсутствуют иллюстрирующие примеры, отсутствуют выводы.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся представляет отчет, в котором содержание раскрыты слабо и в неполном объеме, выводы и предложения являются необоснованными. Материал излагается на основе неполного перечня нормативных документов. Имеются нарушения в оформлении отчета. Отчет с замечаниями преподавателя возвращается обучающемуся на доработку, и условно допускается до публичной защиты.

На публичной защите обучающийся демонстрирует фрагментарные знания в рамках программы практики; не владеет минимально необходимой терминологией; допускает грубые логические ошибки, отвечая на вопросы преподавателя, которые не может исправить самостоятельно.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся представляет отчет, в котором очень слабо рассмотрены практические вопросы задания, применяются старые нормативные документы и отчетность. Отчет выполнен с нарушениями основных требований к оформлению. Отчет с замечаниями преподавателя возвращается обучающемуся на доработку, и не допускается до публичной защиты.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.