Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО

На заседании педагогического совета
от 27.05.2025
протокол № 4

Принято с учётом
согласования с
организацией -партнёром
IT Студия «Северный ветер»
25.05.2025

УТВЕРЖДАЮ

Директор СПб ГБПОУ «АУГСГиП»

_____А.М. Кривоносов

ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

специальности
10.02.01 «Организация и технология защиты информации»

На базе основного общего образования

Санкт-Петербург
2025 год

Программа преддипломной практики разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по профессии 10.02.01 «Организация и технология защиты информации», Утвержден приказом Минобрнауки России от 28.07.2014 № 805.

Рассмотрена на заседании методического совета СПб ГБПОУ «АУГСГиП»
от 16.04.2025 протокол № 3

Составил мастер производственного обучения Несин Д.Е.

Содержание

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Область применения программы производственной практики

Рабочая программа производственной практики (далее программа) - является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности **10.02.01. «Организация и технология защиты информации»** базовой подготовки, в части освоения основного вида профессиональной деятельности (ВПД): организация и проведение работ по техническому обслуживанию и обеспечению информационной безопасности телекоммуникационных сетей и систем в организациях различных структур и отраслевой направленности; обеспечивать защиту информации в сети с использованием программно-аппаратных средств; выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации и соответствующих общих (ОК) и профессиональных компетенций (ПК):

Производственная практика является частью учебного процесса и направлена на формирование у студентов общих и профессиональных компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество***ОК 3.*** Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10. Применять математический аппарат для решения профессиональных задач.
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.
ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.
ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей

конфиденциальной информации.
ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.
ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.
ПК 1.9. Участвовать в оценке качества защиты объекта
ПК 2.1. Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации.
ПК 2.2. Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации.
ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации.
ПК 2.4. Организовывать архивное хранение конфиденциальных документов.
ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.
ПК 2.6. Вести учет работ и объектов, подлежащих защите.
ПК 2.7. Подготавливать отчетную документацию, связанную эксплуатацией средств контроля и защиты информации.
ПК 2.8. Документировать ход и результаты служебного расследования.
ПК 2.9. Использовать нормативные правовые акты, нормативно- методические документы по защите информации.
ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.
ПК 3.3. Фиксировать отказы в работе средств защиты.
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.
ПК 4.1. Устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем

ПК 4.2. Выполнять ввод цифровой и аналоговой информации в персональный компьютер с различных носителей

ПК 4.3. Конвертировать файлы с цифровой информацией в различные форматы

ПК 4.4. Обрабатывать аудио и визуальный контент средствами звуковых, графических и видео-редакторов

ПК 4.5. Создавать и воспроизводить видеоролики, презентации, слайд-шоу и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов средствами персонального компьютера и мультимедийного оборудования

ПК 4.6. Формировать медиатеки для структурированного хранения и каталогизации цифровой информации

ПК 4.7. Управлять размещением цифровой информации на дисках персонального компьютера, а также дисковых хранилищах локальной и глобальной компьютерной сети.

ПК 4.8. Тиражировать мультимедиа контент на различных съемных носителях информации.

ПК 4.9. Публиковать мультимедиа контент в сети Интернет.

1.2. Цели и задачи производственной практики, требования к результатам освоения практики, формы отчётности

Цель практики

Целью практики является формирование у студентов умений, приобретение первоначального практического опыта в рамках профессиональных модулей ППССЗ (Профессиональное образование в области защиты информации и систем безопасности) по основным видам профессиональной деятельности, для последующего освоения ими общих и профессиональных компетенций по избранной специальности. Практика направлена на развитие у студентов практических навыков, необходимых для эффективного выполнения задач в области защиты информации, работы с конфиденциальными данными, а также для применения современных методов и технологий информационной безопасности в реальных рабочих условиях.

Задачи производственной практики

Основными задачами практики являются:

- Формирование у студентов целесообразного, необходимого и достаточного набора практических умений, которые позволят им успешно решать профессиональные задачи в дальнейшем. Практика должна стать основой для будущего профессионального роста, укрепляя уверенность студентов в их знаниях и навыках.
- Воспитание у студента осознанного осмысления и самооценки собственной деятельности, развития аналитических и критических способностей, а также ответственности за результаты своей работы.
- Развитие навыков работы в коллективе, взаимодействия с коллегами и руководством, умение эффективно работать с документацией и средствами защиты информации.

В ходе освоения профессионального модуля обучающийся должен:

Иметь практический опыт:

-Использование физических средств защиты объектов, таких как системы видеонаблюдения, средства физической блокировки доступа, системы сигнализации и т.д.
-Применение средств контроля доступа на объект, включая биометрические системы и системы с ключевыми картами.
-Ведение текущей работы с конфиденциальной информацией, включая её обработку, хранение, передачу и уничтожение, а также соблюдение всех нормативных актов по защите конфиденциальных данных.
-Участие в эксплуатации систем защиты информации, включая управление средствами защиты и выявление угроз.
-Применение технических средств защиты информации, таких как программные и аппаратные средства шифрования, средства защиты от вирусных угроз, системы защиты от утечек данных.
-Выявление возможных угроз информационной безопасности объектов защиты, проведение оценки рисков и внедрение мер по их снижению.

Уметь:

-Организовывать охрану персонала, территорий, зданий, помещений и продукции организаций, используя различные методы охраны и защиты.
-Пользоваться аппаратурой систем контроля доступа, таких как устройства для сканирования биометрических данных, контрольный пункт доступа, системы видеонаблюдения.

-Разрабатывать и реализовывать планы по выделению зон доступа, определять степень конфиденциальности выполняемых работ и методов доступа.
-Определять порядок организации и проведения рабочих совещаний по вопросам, связанным с защитой конфиденциальной информации, а также разрабатывать инструкции по защите данных в рамках мероприятий.
-Проводить инструктажи и тренировки персонала по вопросам организации работы с конфиденциальной информацией, включая обучение по соблюдению стандартов безопасности и предотвращению утечек данных.
-Контролировать соблюдение персоналом требований режима защиты информации, а также обеспечивать соблюдение нормативных актов и стандартов защиты данных.
-Работать с техническими средствами защиты информации, такими как системы шифрования, программные средства защиты, системы контроля доступа.
-Организовывать работу с электронным документооборотом, включая оформление, хранение, классификацию и передачу конфиденциальных документов.
-Осуществлять передачу данных по защищённым каналам связи, обеспечивая их целостность и конфиденциальность.
-Фиксировать и анализировать отказы в работе средств вычислительной техники, оперативно устранять технические неисправности.

Знать:

-Виды и способы охраны объектов, включая физическую защиту, защиту персонала, мониторинг и контроль на объектах.

-Основные направления и методы организации режима охраны объектов, включая разработки программ защиты.

-Принципы действия аппаратуры систем контроля доступа, а также биометрических систем безопасности, включая анализ и применение современных технологий защиты.

-Требования к оборудованию режимных помещений, включая установку средств защиты, соблюдение санитарных и безопасности норм.

-Основы правового регулирования в области информационной безопасности, в том числе законодательства о защите конфиденциальной информации.

-Правовые нормы, регулирующие доступ к конфиденциальной информации, лицензирование деятельности в сфере защиты информации.

-Требования к нормативным актам и методическим материалам Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю.

-Законодательство в области интеллектуальной собственности, защиты патентов, авторских прав и коммерческой тайны.

-Правовые основы защиты конфиденциальной информации по видам тайны, порядок классификации и распределения информации.

-Основные методы защиты информации, включая программные и аппаратные средства защиты, системы мониторинга безопасности.

-Процедуры разработки, учёта, хранения и уничтожения конфиденциальных документов, а также способы защиты их от утечек.

-Технологии работы с конфиденциальными данными, включая методы их классификации, безопасность передачи данных и защиту на всех этапах их обработки.

-Современные технологии работы с мультимедийными данными, включая видео- и аудио редакторы, системы управления мультимедиа контентом.

1.3 Организация практики

Для проведения производственной практики в Академии разработана следующая документация:

- положение о практике;
- рабочая программа производственной практики;
- договоры с предприятиями по проведению практики;
- приказ о распределении студентов по базам практики;

В основные обязанности руководителя практики от Академии входят:

- проведение практики в соответствии с содержанием тематического плана и содержания практики;
- установление связи с руководителями практики от организаций;
- разработка и согласование с организациями программы, содержания и планируемых результатов практики;
- осуществление руководства практикой;
- контролирование реализации программы и условий проведения практики организациями, в том числе требований охраны труда, безопасности жизнедеятельности и пожарной безопасности в соответствии с правилами и нормами, в том числе отраслевыми;
- формирование группы в случае применения групповых форм проведения практики;
- совместно с организациями, участвующими в организации и проведении практики, организация процедуры оценки общих и профессиональных компетенций студента, освоенных им в ходе прохождения практики;
- разработка и согласование с организациями формы отчетности и оценочного материала прохождения практики.

Студенты при прохождении производственной практики обязаны:

- полностью выполнять задания, предусмотренные программой производственной практики;
- соблюдать действующие в организациях правила внутреннего трудового распорядка;

изучать и строго соблюдать нормы охраны труда и правила пожарной безопасности

1.4. Количество часов на освоение программы:

Рабочая программа рассчитана на прохождение студентами практики в объёме – 144 часов. Распределение разделов и тем по часам приведено в тематическом плане. Производственная практика проводится на базе профильных организаций по специальности: **10.02.01 «Организация и технология защиты информации».** Имеющиеся базы практики обеспечивают возможность прохождения практики всеми студентами в соответствии с планом.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Объем производственной практики и виды учебной работы

Вид учебных занятий, обеспечивающих практико-ориентированную подготовку	Объем часов
Всего занятий	144
в том числе:	
Практические занятия	142
Итоговая аттестация	2

Тематический план и содержание профессионального модуля

Преддипломной практики

Наименование разделов, тем, выполнение обязанностей на рабочих местах в организации	Содержание учебного материала, лабораторные и практические работы, экскурсии, состав выполнения работ		Объем часов	Уровень освоения
Организационная часть	***Содержание учебного материала***			1
	1	Инструктаж по ОТ и ТБ, пожарной безопасности и электробезопасности. Знакомство с рабочим местом и трудовым распорядком.	4	
	2	Цели и задачи практики, требования. Постановка задач, определение видов работ		
Раздел 1. Правовые аспекты защиты информации	***Содержание учебного материала***			1,2
	Основные понятия и угрозы безопасности. Законодательство в области информационной безопасности. Методы и модели оценки уязвимости информации. Информационные системы и защита данных.		32	
Раздел 2. Организация защиты информации и делопроизводство	***Содержание учебного материала***			2
	Функции и задачи службы защиты информации Организация конфиденциального документооборота. Подбор и обучение сотрудников службы защиты информации. Управление службой защиты информации.		34	
Раздел 3. Технические методы и средства защиты информации	***Содержание учебного материала***			2,3
	Технические средства защиты информации. Инженерно-технические меры безопасности. Программно-аппаратные методы защиты данных. Контроль эффективности защиты информации.		36	

Раздел 4. Обработка цифровой информации и мультимедиа	Обработка цифровой информации в графических редакторах. Создание и обработка видеоконтента. Создание текстовых 3D эффектов, анимации и аудиомонтажа. Размещение и публикация цифровой информации. Организация медиатеки и тиражирование мультимедиа контента. Электронные системы управления документами.	36	
Зачет по практике		**2**	
Итоговое количество		**144**	

3.УСЛОВИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1 Требования к минимальному материально-техническому обеспечению

Производственная практика обучающихся производится в организациях на основе прямых договоров, заключаемых между ГБОУ «Академия управления городской средой, градостроительства и печати» и каждой организацией, куда направляются обучающиеся.

Организации предоставляют практикантам рабочее место, оборудованное компьютерами и устройствами, необходимыми для прохождения производственной практики, согласно заданию.

3.2 информационное обеспечение

Основная литература:

Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2022. — 592 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — 3-е изд. – Москва : РИОР : ИНФРА-М, 2024. — 400 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Казарин О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для СПО/ О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2024. — 325 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Гришина Н. В. Основы информационная безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2023. — 216 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Гугуева Т. А. Конфиденциальное делопроизводство : учебное пособие / Т.А. Гугуева. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2023. — 199 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. — 2-е изд., перераб. и доп. — Москва : Логос, 2020. — 500 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Информационное право : учебник / Н. Н. Ковалева [и др.] ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2024. — 353 с. — URL: https: // urait.ru. — Режим доступа: по подписке.

Щербак А. В. Информационная безопасность : учебник для СПО / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Щербак А. В. Информационная безопасность : учебник для СПО / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — 50 экз.

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2024. — 325 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Гугуева Т. А. Конфиденциальное делопроизводство : учебное пособие / Т.А. Гугуева. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2023. — 199 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Егоров В. П. Делопроизводство и режим секретности : учебник для СПО / В. П. Егоров, А. В. Слиньков. — 3-е изд., стер. — Санкт-Петербург : Лань, 2023. — 312 с. — (Среднее профессиональное образование). — URL: https://e.lanbook.com. — Режим доступа: по подписке.

Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. — 2-е изд., перераб. и доп. — Москва : Логос, 2020. — 500 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Кузнецов И. Н. Документационное обеспечение управления. Документооборот и делопроизводство : учебник и практикум для СПО / И. Н. Кузнецов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 545 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Кузнецов И. Н. **Документационное обеспечение управления. Документооборот и делопроизводство : учебник и практикум для СПО / И. Н. Кузнецов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 545 с. — (Профессиональное образование). — 25 экз**

Бачило И. Л. Информационное право : учебник / И. Л. Бачило. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 419 с. — URL: https: // urait.ru. — Режим доступа: по подписке.

Кузнецов И. Н. Документационное обеспечение управления. Документооборот и делопроизводство : учебник и практикум для СПО / И. Н. Кузнецов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 545 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Дополнительная литература

Гришина Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ФОРУМ : ИНФРА-М, 2023. — 216 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Москвитин Г. И. Комплексная защита информации в организации : монография / Г. И. Москвитин. — Москва : Русайнс, 2020. — 353 с. — URL: https://www.book.ru. — Режим доступа: по подписке.

Коваленко Ю.И. Методика защиты информации в организациях : монография / Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин. — Москва : Русайнс, 2020. — 162 с. — URL: https://www.book.ru. — Режим доступа: по подписке.

Баранова Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Бабаш А. В. Моделирование системы защиты информации. Практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2023. — 320 с. — URL: http://znanium.com. — Режим доступа: по подписке

Емельянова Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ИД ФОРУМ : НИЦ ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Васильков А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А. В. Васильков, И. А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2022. — 368 с. — (Среднее профессиональное образование). — URL: http://znanium.com. — Режим доступа: по подписке.

Внуков А. А. Основы информационной безопасности: защита информации : учебное пособие для СПО / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — URL: https: // urait.ru. — Режим доступа: по подписке.

Ищейнов В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2022. — 256 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Рассолов И. М. Информационное право : учебник и практикум / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 427 с. — URL: https: // urait.ru. — Режим доступа: по подписке.

Кабашов С. Ю. Электронное правительство. Электронный документооборот. Термины и определения : учебное пособие / С. Ю. Кабашов. — Москва : ИНФРА-М, 2024. — 320 с. — URL: http://znanium.com. — Режим доступа: по подписке.

Электронный документооборот и обеспечение безопасности стандартными средствами Windows **: учебное пособие / Л. М. Евдокимова, В. В. Корябкин, А. Н. Пылькин, О. Г. Швечкова. — Москва : КУРС, 2023. — 296 с. — URL: http://znanium.com. — Режим доступа: по подписке**

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Контроль и оценка результатов освоения производственной практики осуществляется преподавателем при проверке отчетов и сдаче обучающимися дифференцированного зачета.

Результат обучения (Приобретение практического опыта, освоение умения)	**Формы и методы контроля и оценка результатов обучения**
ПК 1.1. Участвовать в сборе и обработке материалов для выработки оптимальных решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. ***Приобретённый практический опыт:*** В сборе и обработке материалов для выработки оптимальных решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. ***Освоенные умения:*** • определение методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации; • выполнение анализа научной литературы; • обоснование выбора соответствующих решений по защите информации объекта; обоснование использованных методов обнаружения технических каналов утечки информации устройства, оборудование и компьютерную оргтехнику;	***Форма контроля обучения:*** 1. Наблюдение за работой практиканта на рабочем месте; 2. Контроль ведения дневника практики; 3. Заполнение образцов исполнительной документации (журналов и актов), как приложение к отчету. ***Форма оценки результативности обучения:*** Система отметок в балах за каждую выполненную работу, на основе которых выставляется итоговая отметка: 1. Оценка работы руководителя от предприятия (аттестационный лист); 2. Оценка руководителя практики от Академии (по результатам наблюдения за работой, при посещении студента и ведению дневника практики); 3. Оценка отчета по производственной практике (техническая грамотность, полнота освещения вопросов в отчете по практике, творческая самостоятельность и своевременность сдачи); 4. Оценка защиты отчета по практике (компетентность в освещении вопросов, профессионализм и самостоятельность в ответах).
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте ***Приобретённый практический опыт:*** Разработки программ и методик организации защиты информации на объекте ***Освоенные умения:*** • определение предложений по разработке программ защиты информации на объекте; • определение методик защиты информации на предприятии	

ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации ***Приобретённый практический опыт:*** Планирования и организации выполнения мероприятий по защите информации**.** ***Освоенные умения:*** • выполнение работ по защите конфиденциальной информацией; • определение качества защиты информации; • выполнение мероприятий по комплексной защите информации	
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности. ***Приобретённый практический опыт:*** Внедрения разработанных организационных решений на объектах профессиональной деятельности**.** ***Освоенные умения:*** • обоснование выбранных организационных решений на объектах информатизации; • обоснование мер по внедрению организационных решений предприятии;	
ПК 1.5 Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации ***Приобретённый практический опыт:*** Ведение учета, обработки, хранения, передачи, использование различных носителей конфиденциальной информации. ***Освоенные умения:*** • обоснование использования носителей конфиденциальной информации; • определение методики обработки и хранения защищаемой информации; • организация выполнения передачи конфиденциальной информации на различных носителях. • полнота и эффективность соблюдения правил использования но	
ПК 1.6. Обеспечивать технику безопасности при проведении организационнотехнических мероприятий ***Приобретённый практический опыт:***	

Обеспечения техники безопасности при проведении организационно-технических мероприятий **.** ***Освоенные умения:*** • определение правил техники безопасности при комплексной защите информации; • определение методики защиты информации при проведении организационно- технических мероприятий.	
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите**.** ***Приобретённый практический опыт:*** Участия в организации и проведении проверок объектов информатизации, подлежащих защите. ***Освоенные умения:*** • обоснование выбранных методов проверок организаций, информация которых подлежит защите; • проведение проверки объектов информатизации; • проведение проверки организаций, работающих с конфиденциальной информацией.	
ПК 1.8. Проводить контроль за соблюдением персоналом требований режима защиты информации ***Приобретённый практический опыт:*** Проведения контроля за соблюдением персоналом требований режима защиты информации. ***Освоенные умения:*** • определение методов и способов контроля персонала, работающего с конфиденциальной информацией; • определение последовательности действий при проведении проверок соблюдения персоналом требований режима защиты информации; • организация проведения контроля за работой персонала, задействованного в защите информации организации.	

ПК 1.9. Участвовать в оценке качества защиты объекта ***Приобретённый практический опыт:*** в оценке качества защиты объекта ***Освоенные умения:*** • выполнение оценки качества комплексной защиты информации организации; • выполнение оценки качества защиты объекта информатизации; определение и анализ недостатков качества защиты • информации на предприятии	
ПК 2.1. Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации. ***Приобретённый практический опыт:*** в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации. ***Освоенные умения:*** • Умение готовить организационные и распорядительные документы, регламентирующие работу по защите информации • выполнение анализа и обработки распорядительных документов; • проведение исследований работ документов, регламентирующих работу по защите информации	
ПК 2.2. Организовывать и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации ***Приобретённый практический опыт:*** Организации и обеспечения технологии ведения делопроизводства с учетом конфиденциальности информации. ***Освоенные умения:*** • выполнение требований ведения делопроизводства с учетом конфиденциальности информации; • выполнение требований нормативно-технической документации	
ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации ***Приобретённый практический опыт:*** Организации документооборота, в том числе электронный, с учетом	

конфиденциальности информации. ***Освоенные умения:*** • проектирование электронной передачи данных, конструктивно-технологических модулей с применением пакетов прикладных программ; • разработка комплекта документации.	
ПК 2.4. Организовывать архивное хранение конфиденциальных документов. ***Приобретённый практический опыт:*** Организации архивного хранения конфиденциальных документов. ***Освоенные умения:*** • определение показателей надежности и оценка качества хранения конфиденциальных документов на различных носителях.	
ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом ***Приобретённый практический опыт:*** Оформления документации по оперативному управлению средствами защиты информации и персоналом. ***Освоенные умения:*** • выполнение требований нормативно-технической документации; • разработка проектной документации с использованием современных пакетов прикладных программ в сфере профессиональной деятельности	
ПК 2.6. Вести учет работ и контроль объектов, подлежащих защите. ***Приобретённый практический опыт:*** ведения учета работ и контроль объектов, подлежащих защите. ***Освоенные умения:*** • использование инвентаризации объектов, подлежащих защите.	
ПК 2.7. Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации. ***Приобретённый практический опыт:*** Подготовки отчетной документации,	

связанную с эксплуатацией средств контроля и защиты информации ***Освоенные умения:*** • разработка отчетной документации, связанной с эксплуатацией средств контроля и защиты информации	
ПК 2.8. Документировать ход и результаты служебного расследования. ***Приобретённый практический опыт:*** . Документирования хода и результатов служебного расследования. ***Освоенные умения:*** • выполнение требований документирования служебного расследования	
ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы по защите информации. ***Приобретённый практический опыт:*** Использования нормативных правовых актов, нормативно-методических документов по защите информации. ***Освоенные умения:*** • выполнение требований нормативно-технической документации по защите информации;	
ПК 3.1 Применять программно-аппаратные и инженерно-технические средства защиты информации ***Приобретённый практический опыт:*** Применять программно-аппаратные и инженерно-технические средства защиты информации ***Освоенные умения:*** • обоснованность выбора технических и программно-аппаратных средств защиты информации; • грамотное применение технических и программно-аппаратных средств защиты информации; • правильность освоения возможностей работоспособности компонентов систем защиты информации.	
ПК.3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов. ***Приобретённый практический опыт:***	

Участия в эксплуатации систем и средств защиты информации защищаемых объектах. ***Освоенные умения:*** • умение решать частные технические задачи, возникающие при эксплуатации систем и средств защиты информации; • умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации.	
ПК 3.3. Фиксировать отказы в работе средств защиты. ***Приобретённый практический опыт:*** Организации документооборота, в том числе электронный, с учетом конфиденциальности информации. ***Освоенные умения:*** • точность и скорость диагностики нарушений эксплуатационных характеристик средств защиты; • качество анализа эксплуатационных свойств средств защиты; • проверка технического состояния средств защиты; • умения проводить техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность средств защиты	

ПК 4.1. Устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем ***Приобретённый практический опыт*** Установка и настройка аппаратного обеспечения ПК, серверов и сетевого оборудования. Обеспечение стабильного функционирования защищенных телекоммуникационных систем. Проведение тестирования работоспособности и диагностики аппаратных неисправностей. **Освоенные умения:** • Настройка операционных систем для оптимальной работы оборудования. • Проведение тестирования производительности персонального компьютера. • Использование специализированного ПО для диагностики аппаратных компонентов	
ПК 4.2. Выполнять ввод Цифровой и аналоговой информации в персональный компьютер с различных носителей **Приобретенный практический опыт:** Ввод и обработка информации с USB-накопителей, оптических дисков, карт памяти, сканеров и других носителей. Проверка и восстановление поврежденных данных. **Освоенные умения:** • Обеспечение точности ввода информации. • Систематизация информации на носителях в соответствии с установленными стандартами.	
ПК 4.3. Конвертировать файлы с цифровой информацией в различные форматы **Приобретенный практический опыт:** Использование программ-конвертеров для изменения форматов графики, аудио, видео и документов.Автоматизация процессов конвертации с помощью скриптов и пакетной обработки. **Освоенные умения:** • Выбор правильной технологии конвертирования файлов.	

• Обеспечение совместимости цифровых данных с различными устройствами и приложениями.	
ПК 4.4.Обрабатывать аудио и визуальный контент средствами звуковых, графических и видео-редакторов **Приобретенный практический опыт:** Обработка изображений, монтаж видео, редактирование аудиофайлов. **Освоенные умения:** • Подбор и правильное применение программного обеспечения для обработки контента. • Использование технологий обработки аудио и визуального контента.	
ПК 4.5. Создавать и воспроизводить видеоролики, презентации, слайд-шоу и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов средствами персонального компьютера и мультимедийного оборудования **Приобретенный практический опыт:** Создание мультимедийных проектов для образовательных, рекламных и корпоративных нужд. Монтаж и рендеринг видеороликов, подготовка слайд-шоу в PowerPoint, Canva. **Освоенные умения:** • Подготовка исходных материалов для мультимедийной продукции. • Применение технологий создания и воспроизведения мультимедиа-контента.	
ПК 4.6.Формировать медиатеки для структурированного хранения и каталогизации цифровой информации **Приобретенный практический опыт:** Организация библиотек цифрового контента с использованием систем управления медиаданными (DAM). Создание удобных структур каталогов на дисковых хранилищах. **Освоенные умения:**	

• Формирование медиатеки в зависимости от типа файлов. • Каталогизация информации с учетом удобства поиска и доступа.	
ПК 4.7. Управлять размещением цифровой информации на дисках персонального компьютера, а также дисковых хранилищах локальной и глобальной компьютерной сети. **Приобретенный практический опыт:** Администрирование локальных и облачных хранилищ. Управление файловыми системами, резервное копирование и восстановление данных. **Освоенные умения:** • Соблюдение технологий организации хранения данных. • Обеспечение надежности и безопасности хранения цифровой информации.	
ПК 4.8. Тиражировать мультимедиа контент на различных съемных носителях информации. **Приобретенный практический опыт:** Запись и копирование данных на CD/DVD, USB-накопители, внешние жесткие диски. Создание загрузочных носителей с мультимедийными данными. **Освоенные умения:** • Соблюдение технологий тиражирования мультимедиа-контента • Проверка качества записанных данных.	
ПК 4.9. Публиковать мультимедиа контент в сети Интернет. **Приобретенный практический опыт:** Загрузка и публикация контента в сети Интернет, социальные сети и веб-сайты. Оптимизация мультимедийных файлов для веб-просмотра. **Освоенные умения:** • Применение технологий публикации мультимедиа-контента в сети Интернет. • Учет требований к качеству и формату контента для онлайн-платформ.	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоение общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	• Высокие показатели производственной деятельности; • демонстрация интереса к будущей профессии. Это ОК проверяется с помощью портфолио.	***Формы контроля обучения:*** • наблюдение за работой практиканта на рабочем месте. • контроль ведения дневника практики; • заполнение образцов исполнительной документации (журналов и актов), как приложения к отчёту; • Экспертная оценка результатов деятельности обучающихся в процессе освоения образования. • Оценка работы руководителя от предприятия (аттестационный лист); • Оценка руководителя практики от Академии (по результатам наблюдения за работой при посещении студента и ведению дневника практик • Оценка отчёта (техническая грамотность, полнота освещения вопросов в отчёте по практике, творческая самостоятельность, своевременность сдачи);
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	• обоснование выбора и применения методов и способов решения профессиональных задач в области разработки технологических процессов; • демонстрация эффективности и качества выполнения профессиональных задач.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	• демонстрация способности принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	• нахождение и использование информации для эффективного выполнения профессиональных задач, профессионального и личностного развития	
ОК 5. Использовать информационно-коммуникационные технологии в	• демонстрация навыков использования информационно-коммуникационные технологии в профессиональной	

профессиональной деятельности.	деятельности;	• Оценка защиты отчёта по практике (компетентность в освещении вопросов, профессионализм и самостоятельность в ответах).
ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями	• взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий	• проявление ответственности за работу подчиненных, результат выполнения заданий	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	• планирование обучающимся повышения личностного и квалификационного уровня	
ОК 9. Быть готовым к смене технологий в профессиональной деятельности.	• проявление интереса к инновациям в области профессиональной деятельности	
ОК 10. Применять математический аппарат для решения профессиональных задач.	• применение средств математической логики для решения задач	
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности	• уметь оценивать документы, используемые в области защиты информации.	
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	• владение информацией о структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	

5. Приложение
5.1 Задание на практику

Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждения
«Академия управления городской средой, градостроительства и печати»

Задание
на прохождение преддипломной практики

По специальности 10.02.01 «Организация и технология защиты информации»

Студенту _____
Группы _____
Начало практики _____
Окончание практики _____

Наименование организации: _____

Ответственный руководитель по практике от академии: _____
Телефон: _____

В основу задания по производственной практике положена программа производственной практики.

Во время практики студент должен вести дневник-отчет о практике, записи в котором необходимо делать ежедневно.

Выполнить в срок, установленный учебным планом, следующее индивидуальное задание:

1	Провести анализ нормативно-правовых актов в области защиты информации и составить краткий отчет о ключевых требованиях.
2	Ознакомиться с внутренними регламентами организации по защите информации и подготовить предложения по их улучшению.
3	Разработать и оформить пакет документов для защиты конфиденциальной информации (например, политика безопасности, инструкции).
4	Проанализировать возможные угрозы информационной безопасности в организации и предложить меры по их устранению.
5	Провести тестирование системы защиты информации, выявить уязвимости и предложить варианты их устранения.
6.	Ознакомиться с работой систем контроля доступа и видеонаблюдения, подготовить отчет об их эффективности.
7.	Осуществить резервное копирование данных с использованием различных методов и составить инструкцию по восстановлению.
8.	Провести аудит защищенности локальной сети организации и подготовить отчет с рекомендациями по повышению безопасности.

9.	Разработать план реагирования на инциденты информационной безопасности и представить его в виде отчета.
10.	Создать презентацию о современных методах защиты информации, включая криптографические и аппаратные средства.
11.	Изучить принципы работы антивирусных программ, выполнить анализ их эффективности и составить сравнительную таблицу.
12.	Ознакомиться с основными методами шифрования данных, настроить шифрование файлов и подготовить отчет о проделанной работе.
13.	Провести мониторинг событий безопасности в организации
14.	Разработать рекомендации по защите мобильных устройств и персональных гаджетов сотрудников.
15.	Изучить способы защиты информации при работе в облачных сервисах и подготовить инструкцию по безопасному использованию.
16.	Ознакомиться с методами социальной инженерии, провести тестирование на устойчивость сотрудников к атакам (фишинг, вишинг) и составить отчет.
17.	Настроить и протестировать VPN для безопасного удаленного доступа к корпоративным ресурсам.
18.	Подготовить итоговый отчет о прохождении практики, отражающий все выполненные задания, их результаты и выводы.

По итогам практики сдать следующие отчетные документы:

1. Титульный лист.
2. Дневник практики.
3. Характеристика деятельности обучающегося.
4. Аттестационный лист по учебной практике с отметкой.
5. Итоговая оценка.

Задание выдал
Руководитель практики _____/ _____

« ____» _____20__ г.

5.2 Титульный лист отчета студента о прохождении практики

Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждения
«Академия управления городской средой, градостроительства и печати»»

ОТЧЁТ
по прохождению преддипломной практики
По специальности
10.02.01 «Организация и технология защиты информации»

_____

(Наименование организации и место прохождения практики)

Студента группы:_____

_____
(подпись, дата)

Руководитель практики от предприятия

_____

_____
м.п. *(занимаемая должность)*

_____
(подпись руководителя практики от предприятия)

"____" _____20___ г.

Руководитель практики от Академии

_____/ _____

ФИО

"_____" _____20___ г.

Оценка за пройденную практику по результатам защиты отчёта

_____
(подпись руководителя практики от Академии)

Санкт-Петербург

20__г.

5.3 Аттестационный лист

Аттестационный лист по преддипломной практике

_____

Ф.И.О.

Группа _____

Специальность: 10.02.01 «Организация и технология защиты информации»

Место проведения практики (организация), наименование, юридический адрес:

_____

Время проведения практики с _____ по _____

Компетенция	Основные показатели результата	Уровень		
		Высокий	Средний	Ниже среднего
ПК 1.1. Участвовать в сборе и обработке материалов для выработки оптимальных решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	определение методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации.			
	выполнение анализа научной литературы;			
	обоснование выбора соответствующих решений по защите информации			
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.	определение предложений по разработке программ защиты информации на объекте;			
	определение методик защиты информации на предприятии			
ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.	выполнение работ по защите конфиденциальной информацией;			
	определение качества защиты информации;			
	выполнение мероприятий по комплексной защите информации			
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах	обоснование выбранных организационных решений на объектах информатизации;			
	обоснование мер по			

профессиональной деятельности.	внедрению организационных решений предприятии;			
ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.	обоснование использования носителей конфиденциальной информации;			
	определение методики обработки и хранения защищаемой информации;			
	организация выполнения передачи конфиденциальной информации на различных носителях.			
	полнота и эффективность соблюдения правил использования но			
ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.	определение правил техники безопасности при комплексной защите информации;			
	определение методики защиты информации при проведении организационно-технических мероприятий.			
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.	обоснование выбранных методов проверок организаций, информация которых подлежит защите;			
	проведение проверки объектов информатизации;			
	проведение проверки организаций, работающих с конфиденциальной информацией.			
ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.	определение методов и способов контроля персонала, работающего с конфиденциальной информацией;			
	определение последовательности действий при проведении проверок соблюдения персоналом требований режима защиты информации;			
	организация проведения контроля за работой			

	персонала, задействованного в защите информации организации.			
ПК 1.9. Участвовать в оценке качества защиты объекта	выполнение оценки качества комплексной защиты информации организации;			
	выполнение оценки качества защиты объекта информатизации; определение и анализ недостатков качества защиты информации на предприятии			
ПК 2.1. Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации.	Умение готовить организационные и распорядительные документы, регламентирующие работу по защите информации			
	выполнение анализа и обработки распорядительных документов;			
	проведение исследований работ документов, регламентирующих работу по защите информации			
ПК 2.2. Организовывать и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации	выполнение требований ведения делопроизводства с учетом конфиденциальности информации;			
	выполнение требований нормативно-технической документации			
ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности	проектирование электронной передачи данных, конструктивно-технологических модулей с применением пакетов прикладных программ;			
	разработка комплекта			

информации	документации			
ПК 2.4. Организовывать архивное хранение конфиденциальных документов.	определение показателей надежности и оценка качества хранения конфиденциальных документов на различных носителях.			
ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом	выполнение требований нормативно-технической документации;			
	разработка проектной документации с использованием современных пакетов прикладных программ в сфере профессиональной деятельности			
ПК 2.6. Вести учет работ и контроль объектов, подлежащих защите.	использование инвентаризации объектов, подлежащих защите.			
ПК 2.7. Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.	разработка отчетной документации, связанной с эксплуатацией средств контроля и защиты информации			
ПК 2.8. Документировать ход и результаты служебного расследования.	выполнение требований документирования служебного расследования			
	Умение заполнять Акт служебного расследования;			
ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы по защите информации.	выполнение требований нормативно-технической документации по защите информации;			
	Знание законодательной и нормативно-правовой базы по защите информации			
	обоснованность выбора технических и программно-аппаратных средств защиты информации			

ПК 3.1 Применять программно-аппаратные и инженерно-технические средства защиты информации	грамотное применение технических и программно-аппаратных средств защиты информации;			
	правильность освоения возможностей работоспособности компонентов систем защиты информации.			
ПК.3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.	умение решать частные технические задачи, возникающие при эксплуатации систем и средств защиты информации;			
	умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации.			
ПК 3.3. Фиксировать отказы в работе средств защитя	точность и скорость диагностики нарушений эксплуатационных характеристик средств защиты;			
	качество анализа эксплуатационных свойств средств защиты;			
	Проверка технического состояния средств защиты;			
	умения проводить техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность средств защиты			
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	умение выявлять и анализировать возможные угрозы информационной безопасности объектов			

ПК 4.1. Устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем	- Нормальное функционирование аппаратного обеспечения. Тестирование производительности персонального компьютера			
ПК 4.2. Выполнять ввод цифровой и аналоговой информации в персональный компьютер с различных носителей	-Точность ввода информации. -Правильная систематизации информации на носителях			
ПК 4.3. Конвертировать файлы с цифровой информацией в различные форматы	-Правильность применения технологии конвертирования файлов с цифровой информацией.			
ПК 4.4. Обрабатывать аудио и визуальный контент средствами звуковых, графических и видео-редакторов	-Умение подобрать необходимое программное обеспечение и правильное применения технологии обработки аудио и визуального контента			
ПК 4.5. Создавать и воспроизводить видеоролики, презентации, слайд-шоу и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов средствами персонального компьютера и мультимедийного оборудования	-Понимание процесса подготовки необходимой информации для создания мультимедийной продукции. Правильное применение технологий создания и воспроизведения мультимедийной информации.			
ПК 4.6. Формировать медиатеки для структурированного хранения и каталогизации цифровой информации	-Правильное формирование медиатеки в зависимости от типов файлов; -Создание структурированного			

	каталога хранения цифровой информации			
ПК 4.7. Управлять размещением цифровой информации на дисках персонального компьютера, а также дисковых хранилищах локальной и глобальной компьютерной сети.	-Соблюдение технологии по размещению цифровой информации на дисках ПК; дисковых хранилищах различных сетей.			
ПК 4.8. Тиражировать мультимедиа контент на различных съемных носителях информации.	-Соблюдение технологии тиражирования мультимедиа контента на различных съемных носителях информации			
ПК 4.9. Публиковать мультимедиа контент в сети Интернет.	-Соблюдение технологии создания и публикации мультимедиа контента в сети Интернет			

Руководитель практики от предприятия

«_____ » _____ 202 г.

_____ / _____/
(подпись) *Ф И О*

М. П.

5.4 Характеристика деятельности обучающегося

Характеристика деятельности студента на преддипломной практике

_____

Ф.И.О.

Группа _____

Специальность: _____

Место проведения практики (организация), наименование, юридический адрес:

_____

Время проведения практики с _____по _____г.

Код	Общие компетенции	Основные показатели оценки результата	Уровень		
			Высокий	Выше среднего	Средний
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	выступления на научно-практических конференциях; участие во внеурочной деятельности связанной с будущей профессией/специальность ю (конкурсы профессионального мастерства, выставки и т.п.); высокие показатели производственной деятельности			
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества			
ОК 3.	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.	анализ профессиональн ых ситуации			
		решение стандартных и нестандартных профессиональных задач			
	Осуществлять поиск,	эффективный поиск необходимой информации			

ОК 4.	анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.	использование различных источников, включая электронны е при изучении теоретического материала и прохождении различных этапов производственной практики			
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.	использование в учебной и профессиональной деятельности различных видов программного обеспечения, в том числе специального, при оформлении и презентации всех видов работ			
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	взаимодействие: - с обучающимися при проведении деловых игр, выполнении коллективных заданий (проектов), - с потребителями и коллегами в ходе производственной практики			
ОК 7.	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.	самоанализ и коррекция результатов собственной деятельности при выполнении коллективных заданий (проектов)			
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	планирование и качественное выполнение заданий для самостоятельной работы при изучении теоретического материала и прохождении различных этапов производственной практики			

		определение этапов и содержания работы по реализации самообразования			
ОК 9.	Быть готовым к смене технологий в профессиональной деятельности.	проявление профессиональной маневренности при прохождении различных этапов практики			
ОК 10.	Применять математический аппарат для решения профессиональных задач.	применение средств математической логики для решения задач			
ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности	уметь оценивать документы, используемые в области защиты информации.			
ОК 12.	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность	владение информацией о структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность			

Деятельность студента по освоению компетенций на уровне: высокий, выше среднего, средний.
Руководитель практики от предприятия

«_____ » _____ 202 г.

_____ / _____/
(подпись) *Ф И О*

М. П.

5.5 Дневник практики

Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждения
«Академия управления городской средой, градостроительства и печати»

ДНЕВНИК
ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Студент_____
(фамилия, имя, отчество)

Группа _____

Специальность: 10.02.01 «Организация и технология защиты информации»

Руководитель от предприятия: _____

Место проведения практики (организация), наименование, юридический адрес:

_____

Время проведения практики с _____по _____г.

Дата	Содержание выполняемых работ	Кол-во часов	Отметка об освоении данного вида работ (освоен, не освоен)	Подпись руководителя практики от организации
1	2	3	4	5
	Инструктаж по ОТ и ТБ, пожарной безопасности и электробезопасности. Знакомство с рабочим местом и трудовым распорядком.			
	Цели и задачи практики, требования. Постановка задач, определение видов работ			

	Защита отчетов	2		
ИТОГО:		**144**		

Руководитель практики от предприятия

«_____ » _____ 202 г.

_____ / _____/

(подпись) *Ф И О*

М. П.

5.6 Итоговая оценка

ИТОГОВАЯ ОЦЕНКА ПО ПРЕДДИПЛОМНОЙ ПРАКТИКИ

_____

ФИО

Сроки прохождения: с _____по _____

Специальность: 10.02.01 «Организация и технология защиты информации»
Курс _____ группа: _____
Студент(ка)_____
Ф.И.О.

м.п.

Оценка за выступление на итоговой конференции_____

Оценка руководителя практики от организации _____

Оценка руководителя практики от Академии за отчет_____

Итоговая оценка_____

Руководитель практики от СПб ГБПОУ «АУГСГиП» _____
Должность

_____
подпись Фамилия, Имя, Отчество