Программа
практики (преддипломной)

ПДП.00 ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРЕДДИПЛОМНАЯ)

10.02.01 Организация и технология защиты информации

2020 г.

РАССМОТРЕНА

на заседании ЦМК
информационно-технических
и профессиональных
дисциплин
Протокол от
«25» мая 2020 года № 4

СОГЛАСОВАНО

Директор ООО «СКБ»
_____ П.Л. Закопайло
«29» мая 2020 года

УТВЕРЖДЕНА

Директор ОмЮК
_____ Ю.А. Бурдельная
«29» мая 2020 года

Программа практики «Производственная практика (преддипломная)» разработана в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.01 Организация и технология защиты информации.

Организация-разработчик: частное профессиональное образовательное учреждение «Омский юридический колледж»

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРАКТИКИ «ПДП.00 ПРОИЗВОДСТВЕННАЯ ПРАКТИКА (ПРЕДДИПЛОМНАЯ)»

1.1. Область применения программы

Программа практики является частью основной профессиональной образовательной программы (далее – ОПОП) в соответствии с ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации в части освоения видов профессиональной деятельности (далее – ВПД) и соответствующих профессиональных компетенций (далее – ПК).

1.2. Место практики в структуре ОПОП

«ПДП.00 Производственная практика (преддипломная)» входит в обязательную часть учебных циклов. Производственная практика (преддипломная) является завершающим этапом и проводится после освоения и сдачи обучающимися всех видов промежуточной аттестации, предусмотренных ФГОС СПО и ОПОП.

Практика реализуется в рамках профессиональных модулей: ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта, ПМ.02 Организация и технология работы с конфиденциальными документами, ПМ.03 Программно-аппаратные и технические средства защиты информации, ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

1.3. Цели и задачи программы практики

Цели практики:

– закрепление и углубление знаний, полученных обучающимися в процессе теоретического обучения;

– приобретение необходимых умений, навыков и опыта практической работы по получаемой специальности;

– формирование у обучающихся практических профессиональных умений в рамках модулей ОПОП СПО по основным видам профессиональной деятельности, обучение трудовым приемам, операциям и способам выполнения трудовых процессов, характерных для соответствующей профессии и необходимых для последующего освоения выпускниками общих и профессиональных компетенций по избранной профессии;

– подготовка студента к выполнению выпускной квалификационной работы.

Задачи практики:

– ознакомление со структурой подразделения, в котором проходит практика, его функциями и связями с другими подразделениями предприятия;

– изучение организации проектных работ;

– приобретение практических навыков на рабочем месте техника;

– ознакомление с видами документации, стандартами, нормалями и т.п.;

– закрепление знаний и выработка умений по организации и технологии защиты информации;

– выработка навыков творческого подхода к решению теоретических и практических задач по специальности;

– сбор материалов, необходимых для выполнения выпускной квалификационной работы;

– выработка умений оценки технических показателей выполняемого проекта в соответствии с действующими нормативно-техническими документами.

В результате прохождения практики обучающийся должен иметь практический опыт:

– использования физических средств защиты объекта;

– применения физических средств контроля доступа на объект;

– ведения текущей работы исполнителей с конфиденциальной информацией;

– ведения учета и оформления бумажных и машинных носителей конфиденциальной информации;

– работы с информационными системами электронного документооборота;

– участия в эксплуатации систем и средств защиты информации защищаемых объектов;

– применения технических средств защиты информации;

– выявления возможных угроз информационной безопасности объектов защиты;

– приема, регистрации, учета входящих документов;

– систематизации и хранения документов текущего архива;

– формирования справочного аппарата, обеспечивающего быстрый поиск документов;

– осуществления экспертизы документов, подготовки и передачи документов на хранение в архив;

уметь:

– организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;

– пользоваться аппаратурой систем контроля доступа;

– выделять зоны доступа по типу и степени конфиденциальности работ;

– определять порядок организации и проведения рабочих совещаний;

– использовать методы защиты информации в рекламной и выставочной деятельности;

– использовать критерии подбора и расстановки сотрудников подразделений защиты информации;

– организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;

– проводить инструктаж персонала по организации работы с конфиденциальной информацией;

– контролировать соблюдение персоналом требований режима защиты информации;

– использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;

– документировать ход и результаты служебного расследования;

– определять состав документируемой конфиденциальной информации;

– подготавливать, издавать и учитывать конфиденциальные документы;

– составлять номенклатуру конфиденциальных дел;

– формировать и оформлять конфиденциальные дела;

– организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;

– использовать системы электронного документооборота;

– работать с техническими средствами защиты информации;

– работать с защищенными автоматизированными системами;

– передавать информацию по защищенным каналам связи;

– фиксировать отказы в работе средств вычислительной техники;

– принимать, регистрировать, учитывать поступающие документы;

– проверять правильность оформления документов;

– вести картотеку учета прохождения документальных материалов;

– систематизировать и хранить документы текущего архива;

– формировать справочный аппарат, обеспечивающий быстрый поиск документов;

– осуществлять экспертизу документов, готовить и передавать документальные материалы на хранение в архив;

знать:

– виды и способы охраны объекта;

– особенности охраны персонала организации;

– основные направления и методы организации режима и охраны объекта;

– разрешительную систему доступа к конфиденциальной информации;

– принципы действия аппаратуры систем контроля доступа;

– принципы построения и функционирования биометрических систем безопасности;

– требования и особенности оборудования режимных помещений;

– требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;

– требования режима защиты информации при приеме в организации посетителей;

– организацию работы при осуществлении международного сотрудничества;

– требования режима защиты информации в процессе рекламной деятельности;

– требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;

– задачи, функции и структуру подразделений защиты информации;

– принципы, методы и технологию управления подразделений защиты информации;

– методы проверки персонала по защите информации;

– процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией;

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– правовые основы защиты конфиденциальной информации по видам тайны;

– порядок лицензирования деятельности по технической защите конфиденциальной информации;

– правовые основы деятельности подразделений защиты информации;

– правовую основу допуска и доступа персонала к защищаемым сведениям;

– правовое регулирование взаимоотношений администрации и персонала в области защиты информации;

– систему правовой ответственности за утечку информации и утрату носителей информации;

– правовые нормы в области защиты интеллектуальной собственности;

– порядок отнесения информации к разряду конфиденциальной информации;

– порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;

– организацию конфиденциального документооборота;

– технологию работы с конфиденциальными документами;

– организацию электронного документооборота;

– виды, источники и носители защищаемой информации;

– источники опасных сигналов;

– структуру, классификацию и основные характеристики технических каналов утечки информации;

– классификацию технических разведок и методы противодействия им;

– методы и средства технической защиты информации;

– методы скрытия информации;

– программно-аппаратные средства защиты информации;

– структуру подсистемы безопасности операционных систем и выполняемые ею функции;

– средства защиты в вычислительных сетях;

– средства обеспечения защиты информации в системах управления базами данных;

– критерии защищенности компьютерных систем;

– методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов;

– нормативные правовые акты, положения, инструкции, другие руководящие материалы и документы по ведению делопроизводства на предприятии;

– основные положения Единой государственной системы делопроизводства;

– структуру предприятия и его подразделений;

– стандарты унифицированной системы организационно распорядительной документации;

– порядок контроля за прохождением служебных документов и материалов;

– основы организации труда;

– правила эксплуатации вычислительной техники;

– основы законодательства о труде;

– правила внутреннего трудового распорядка;

– правила и нормы охраны труда.

1.4. Количество часов на освоение программы практики 144 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ

Результатом освоения программы является овладение обучающимися видом профессиональной деятельности: участие в планировании и организации работ по обеспечению защиты объекта, в том числе профессиональными (далее – ПК) и общими (далее – ОК) компетенциями:

Код	Наименование результата обучения
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 с 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 защищаемых объектах.
ПК 3.2.	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.
ПК 3.3.	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4.	Выявлять и анализировать возможные угрозы информационной безопасности объектов.
ПК 4.1.	Принимать и регистрировать поступающую корреспонденцию, направлять ее в структурные подразделения организации.
ПК 4.2.	Рассматривать документы и передавать их на исполнение с учетом резолюции руководителей организации.
ПК 4.3.	Оформлять регистрационные карточки и создавать банк материалов.
ПК 4.4.	Вести картотеку учета прохождения документов.
ПК 4.5.	Контролировать прохождение служебных документов и материалов.
ПК 4.6.	Отправлять исполненную документацию адресатам с применением современных видов организационной техники.
ПК 4.7.	Составлять и оформлять служебные документы, материалы с использованием формуляров конкретных документов.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

3.1. Этапы прохождения практики

Подготовительный этап предполагает выбор базы практики и планирование видов работ, которые необходимо выполнить во время практики.

В ходе подготовительного этапа оформляется ряд документов, необходимых для прохождения практики обучающемуся необходимо:

1. Встретиться со своим будущим руководителем практики от организации и обсудить возможность выполнения во время практики видов работ, предусмотренных программой. Ряд работ из обязательного перечня обучающийся выбирает самостоятельно, поэтому важно выяснить приоритеты организации и при выборе руководствоваться ими.

2. Встретиться с руководителем практики – преподавателем колледжа, и запланировать виды работ, вписав их в «Дневник практики». Объем работ определяется программой практики, а их конкретное содержание – спецификой базы практики. Руководитель, преподаватель, поможет обучающемуся правильно сориентироваться, как лучше адаптировать программу практики к реальным условиям прохождения практики.

3. Договориться с руководителем практики, преподавателем колледжа, о способе получения индивидуальных консультаций во время прохождения практики. Это может быть личная встреча, телефонная консультация или общение по электронной почте. Индивидуальные консультации необходимы в том случае, если:

– обучающийся сталкивается с затруднениями при выполнении тех или иных видов работ по практике;

– ему не совсем понятно, как приступить к выполнению того или иного задания;

– возникла необходимость заменить один из запланированных видов работ на другой, незапланированный;

– если требуется консультация по написанию и оформлению отчета по практике.

Таким образом, в конце подготовительного этапа обучающийся имеет четкое представление о том, где он будет проходить практику, что он должен сделать во время практики и каким образом он при необходимости может получить консультацию у своего руководителя.

Рабочий этап непосредственно связан с осуществлением программы практики.

По окончании прохождения практики на предприятии руководитель практики от организации заполняет в «Дневнике практики» характеристику работы обучающегося, оставляет свой контактный телефон, ставит печать и подпись.

Итоговый этап включает в себя подготовку отчета о практике, обсуждение с руководителем итогов практики и возможности использования собранного во время практики материала при написании выпускной квалификационной работы.

Руководитель практики от колледжа, на основании проверки отчета, дневника практики и характеристики выставляет итоговую оценку по практике.

3.2. Содержание практики

№ п/п	Наименования тем производственной практики	Количество часов
	8 семестр	**144**
1	**Инструктаж по прохождению практики, по технике безопасности.** Содержание практики, ее задачи, краткое содержание практики. Содержание отчета и его оформление. Порядок оформления на работу. Вводный инструктаж по ТБ. Инструктаж по общим вопросам, охраны труда и техники безопасности, по режиму работы предприятия, знакомство с производственно-хозяйственной деятельностью организации.	6
2	**Знакомство с профильной организацией.** Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия. Ознакомление с конструкторско-технологическим обеспечением. Ознакомление с эксплуатацией микропроцессорных систем. Ознакомление с методами защиты средств вычислительной техники, защиты информации. Обеспечение информационной и компьютерной безопасности на предприятии. Организация и технология работы с конфиденциальными документами. Правовая защита информации на предприятии. Ведение конфиденциального делопроизводства на предприятии. Организация и сопровождение электронного документооборота. Процедура создания документооборота организаций, учреждений и предприятий в рамках современного законодательства. Комплектование архива организации. Учет документов, проверка их наличия и состояния. Управление электронными архивными ресурсами. Планирование и организация работ по обеспечению защиты объекта. Обеспечение организации системы безопасности предприятия. Технические средства контроля доступа и безопасности. Основные критерии защищенности информационных автоматизированных систем.	18
3	**Изучение работы ведущих отделов** Функции, задачи, структура отдела и его взаимосвязь с другими подразделениями предприятия. Права и обязанности работника отдела. Организация работ подразделений защиты информации. Функциональные подразделения: их штатная структура. Организация управленческой и функциональной деятельности службы корпоративной безопасности. Организационно-штатная структура службы корпоративной безопасности. Основные функциональные цели и задачи службы корпоративной безопасности. Взаимодействие службы защиты корпоративных интересов с кадровыми службами.	18
4	**Работа техника по защите информации** Решение текущих производственных задач в соответствии с получаемым образованием.	36

5	Подборка материала, практических, статистических данных по теме выпускной квалификационной работы.	60
6	Оформление отчета по практике.	4
7	Защита отчета. **Дифференцированный зачёт.**	2
Всего		**144**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

4.1. Информационное обеспечение обучения

Основные источники:

1. Внуков А.А. Основы информационной безопасности: защита информации [Электронный ресурс]: учебное пособие для среднего профессионального образования / А.А. Внуков. — М., 2019. — 240 с. — Режим доступа: http://biblio-online.ru/bcode/431332

2. Дербин Е.А., Климов С.М. Организационные основы обеспечения информационной безопасности предприятия: учебное пособие. – М., 2013 – 266 с. – Режим доступа: http://elib.fa.ru/fbook/Elektr_uch._posobie_OOIB1.pdf/download/Elektr_uch._posobie_OOIB1.pdf

3. Документоведение [Текст]: учебник и практикум для СПО / под ред. Л.А. Дорониной. – М., 2016. – 309 с.

4. Документоведение [Электронный ресурс]: учеб.и практикум для СПО / под ред. Л.А. Дорониной. – М., 2018. – 309 с. Режим доступа: https://www.biblio-online.ru/book/802E2AB0-DB13-492E-8AA7-186AABD08F79

5. Исмаилова Н.П. Электронный документооборот: учебно-методическое пособие / Н.П. Исмаилова. – Махачкала, 2017. – 51 с. – Текст: электронный // URL: https://mkala.rpa-mu.ru/Media/mkala/UMP/kafedra-gumanitarn/Электронный%20документооборот.pdf

6. Казарин О.В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О.В.Казарин, И.Б. Шубинский. — Москва: Издательство Юрайт, 2019. — 342 с. — Текст: электронный // URL: http://biblio-online.ru/bcode/431080

7. Кузнецов И.Н. Документационное обеспечение управления персоналом [Текст]: учебник и практикум для СПО / И.Н. Кузнецов. – М., 2016. - 521 с.

8. Кузнецов И.Н. Документационное обеспечение управления. Документооборот и делопроизводство [Текст]: учебник для СПО / И.Н. Кузнецов. – М., 2016. - 477 с.

9. Кузнецов И.Н. Документационное обеспечение управления. Документооборот и делопроизводство [Электронный ресурс]: учебник и практикум для СПО / И.Н. Кузнецов. – М., 2018. – 462 с.- Режим доступа: https://www.biblio-online.ru/book/A7E915F2-DB9B-406C-9ABB-2405EC3AD7E1

10. Куняев Н.Н., 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 - М.: Логос, 2011. - 500 с. – Текст: электронный // URL: http://tmnlib.ru/jirbis/files/upload/jirbis_data/ibc/books/1.pdf

11. Мокрый В.Ю. Системы электронного документооборота: учебное пособие. – СПб.: Инфо-да, 2018. – 48 с. – Текст: электронный // URL: https://www.gup.ru/events/news/smi/Posobiye_DOU_Mokryy_V.Yu._2018.pdf

12. Основы информационной безопасности: учебное пособие / Е.В. Вострецова.— Екатеринбург, 2019.— 204 с. – Режим доступа: http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

13. Программно-аппаратные средства защиты информации: учебное пособие / Л.Х. Мифтахова, А.Р. Касимова, В.Н. Красильников и др. – СПб., 2018. – 408 с. –

Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=481123

14. Пшенко А.В. Документационное обеспечение управления [Текст]: практикум / А.В. Пшенко, Л. А. Доронина. М., 2014. - 160 с.

15. Раскин Д.И. Методика и практика архивоведения: учебник для среднего профессионального образования / Д.И. Раскин, А.Р. Соколов. — М., 2019. — 339 с.

16. Шувалова Н.Н. Основы делопроизводства [Текст]: учебник и практикум для СПО / Н.Н. Шувалова, А.Ю. Иванова; ред. Н. Н. Шувалова. – М., 2016. - 375 с.

Дополнительные источники:

1. Журнал «Защита информации. Инсайд»

2. Программно-аппаратные средства защиты компьютерной информации. Практический курс: учебное пособие / Е.И. Духан, Н.И. Синадский, Д. А. Хорьков; Екатеринбург: УрГУ, 2008, 240 с. – URL: http://elar.urfu.ru/bitstream/10995/1403/5/1331981_schoolbook.pdf

3. Методы и средства защиты компьютерной информации: учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов, 2006. – 196 с.– URL: https://www.tstu.ru/book/elib/pdf/2006/shamkin2.pdf

4. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. Под ред. А.П. Зайцева, А.А. Шелупанова. - 7-е изд., испр. - М., 2012. - 442 с. – URL: http://www.studentlibrary.ru/book/ISBN9785991202336.html

Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина - СПб, 2012. - 416 с.– URL: http://window.edu.ru/resource/565/78565

5. Смирнова Г.Н. Электронные системы управления документооборотом: учебное пособие / Г.Н. Смирнова. – М., 2002. – 167 с. – Текст: электронный // URL: http://shpora1.do.am/_ld/2/253____-_-.pdf

6. Белов С.П. Подготовка предприятий к внедрению систем электронного документооборота: монография. – М., 2016. – 210 с. – Текст: электронный // URL: http://izd-mn.com/PDF/19MNNPM15.pdf

Интернет-ресурсы:

1. Волков К.А. Документирование в управленческой деятельности: учеб. пособие / К.А. Волков, А.Н. Приходько и др. – СПб., 2009. – Электронный ресурс. – Режим доступа: http://www.aup.ru/books/m685/

2. Ларьков Н.С. Документоведение: учеб. пособие / Н.С. Ларьков. – Электронный ресурс. – Режим доступа: http://aleho.narod.ru/document/

3. Нормативные документы по делопроизводству. – Режим доступа: http://www.termika.ru/termika/dou/docs/docs.html

4. Фионова Л.Р. Организация и технология документационного обеспечения управления: конспект лекций / Л.Р. Филонова. – Пенза, 2008. – Электронный ресурс. – Режим доступа: http://www.aup.ru/books/m1314/

5. Информационно-правовой портал «Гарант» http://www.garant.ru/

6. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/

7. Федеральный портал «Российское образование» - http://www.edu.ru/

8. Интегральный каталог ресурсов Федерального портала «Российское образование» http://soip-catalog.informika.ru/

9. Федеральный фонд учебных курсов - http://www.ido.edu.ru/ffec/econ-index.html

10. Комплексная система защиты от утечек корпоративной информации -

http://www.securit.ru

11. Общественно-государственное объединение «Ассоциация документальной электросвязи» - http://www.rans.ru/

12. Федеральная служба по техническому и экспортному контролю - http://fstec.ru/

4.2. Общие требования к организации образовательного процесса

Практика является обязательным разделом ОПОП. Она представляет собой вид учебных занятий, обеспечивающих практико-ориентированную подготовку обучающихся. Производственная (преддипломная) практика проводится в организациях различных организационно-правовых форм на основе договоров между организацией, осуществляющей деятельность по образовательной программе соответствующего профиля, и колледжем.

Практика проводится в учреждениях, специфика работы которых связана с компьютерными информационными технологиями, в отделах информационной безопасности различных предприятий, научно-производственных предприятиях, занимающихся разработкой средств информационной безопасности. При выборе базы практики учитываются следующие факторы: оснащенность современными аппаратно-программными средствами, оснащённость необходимым оборудованием, наличие квалифицированного персонала.

Аттестация по итогам производственной (преддипломной) практики проводится в форме дифференцированного зачета на основании предоставленных отчетов и отзывов с мест прохождения практики.

4.3. Кадровое обеспечение образовательного процесса

Педагогические кадры, осуществляющие руководство практикой имеют опыт деятельности в организациях соответствующей профессиональной сферы. Организацию и руководство производственной практикой осуществляют руководители практики от колледжа и от организации.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
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.	– 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.	Оценка результатов деятельности обучающихся в процессе выполнения работ на различных этапах практики. Оценка защиты отчета по практике. Оценка портфолио. Дневник практики.
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 информации; – определение качества защиты информации; – выполнение мероприятий по комплексной защите информации.	
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.	– Обоснование выбранных организационных решений на объектах информатизации; – обоснование мер по внедрению организационных решений на 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 носителей секретной информации.	
ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.	– Демонстрация умений 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.	– Демонстрация умений подготавливать организационные и распорядительные документы; – грамотная организация сбора и обработки материалов; – эффективная организация работы с распорядительными документами, регламентирующими работу по защите информации.	Оценка результатов деятельности обучающихся в процессе выполнения работ на различных этапах практики. Оценка защиты отчета по практике. Оценка портфолио. Дневник практики.
ПК 2.2. Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации.	– Демонстрация умений обеспечивать технологию ведения делопроизводства; – правильность использования методик организации делопроизводства; – умение ведения делопроизводства с учетом конфиденциальной информации.	
ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации.	– Демонстрация умений организовывать документооборот, в том числе электронный; – грамотная организация электронного документооборота, с учетом конфиденциальности информации.	
ПК 2.4. Организовывать архивное хранение	– Демонстрация умений организовывать архивное хранение конфиденциальных	

конфиденциальных документов.	документов; – грамотная организация архивного хранения конфиденциальных документов.	
ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.	– Демонстрация умений оформлять документацию по оперативному управлению; – грамотное ведение учета, обработки, хранения, передачи, использования документации по оперативному управлению средствами защиты информации и персонала.	
ПК 2.6. Вести учет работ и объектов, подлежащих защите.	– Демонстрация умений вести учет работ и контроль объектов, подлежащих защит; – соблюдение правил охраны объектов, подлежащих защите; – грамотное ведение учета работ, подлежащих защите.	
ПК 2.7. Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.	– Демонстрация умений осуществлять подготовку отчетной документации; – грамотная организация и подготовка отчетов, связанных с эксплуатацией средств контроля и защиты информации.	
ПК 2.8. Документировать ход и результаты служебного расследования.	– Демонстрация умений документировать и оформлять результаты служебного расследования; – правильность проведения контроля соблюдения персоналом требований режима защиты информации; – грамотная организация служебного расследования.	
ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы по защите информации.	– Демонстрация умений использования нормативных правовых актов, нормативно-методических документов по защите информации; – грамотное использование нормативных правовых актов, нормативно-методических документов по защите информации.	
ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.	– 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.	Оценка результатов деятельности обучающихся в процессе выполнения работ на различных этапах практики.
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	Оценка защиты отчета по практике. Оценка портфолио.

	утечки информации.	Дневник практики.
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	– 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. Принимать и регистрировать поступающую корреспонденцию, направлять ее в структурные подразделения организации.	– Сбор данных по управленческому вопросу; – составление проекта распорядительного документа; – согласование проекта распорядительного документа; – подписание документа.	Оценка результатов деятельности обучающихся в процессе выполнения работ на различных этапах практики. Оценка защиты отчета по практике. Оценка портфолио. Дневник практики.
ПК 4.2. Рассматривать документы и передавать их на исполнение с учетом резолюции руководителей организации.	– Создание документов; – организация движения и учёта документов; – хранение документов.	
ПК 4.3. Оформлять регистрационные карточки и создавать банк материалов.	– Подготовка первичной документации; – обработка поступающих в организацию документов; – предварительное рассмотрение и распределение документов; – регистрация документов; – контроль исполнения; – информационно-справочная работа; – исполнение документов, их составление, согласование, оформление; – отправка или направление в дело.	
ПК 4.4. Вести картотеку учета прохождения документов.	– Составление и оформление номенклатуры дел; – формирование архива; – сроки хранения документов; – передача документов в архивные органы.	
ПК 4.5. Контролировать прохождение служебных документов и материалов.	– Составление и заполнение деловых бумаг; – контроль за движением документов; – учет и исполнение документов; – организация хранения.	
ПК 4.6. Отправлять	– Прием и регистрация документов;	

исполненную документацию адресатам с применением современных видов организационной техники.	– регистрация входящих документов; – передача документов адресату; – регистрация и отправление исходящих документов.	
ПК 4.7. Составлять и оформлять служебные документы, материалы с использованием формуляров конкретных документов.	– Качественное ведение делопроизводства; – правильное составление документов; – использование унифицированных форм в делопроизводстве; – организация хранения документов.	

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 (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	– Демонстрация интереса к будущей профессии.	Оценка на защите отчета по практике. Оценка портфолио. Характеристика с места прохождения практики. Дневник практики.
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 в области защиты информации; – оценка эффективности и качества выполнения.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– Решение стандартных и нестандартных профессиональных задач в области защиты информации.	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	– Эффективный поиск необходимой информации; – использование различных источников, включая электронные.	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	– Работа с профессиональными информационными системами.	

ОК 6. Работать в коллективе и 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.	– Самоанализ и коррекция результатов собственной работы.	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	– Организация самостоятельных занятий при изучении профессионального модуля.	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	– Анализ инноваций в области защиты информации.	
ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных знаний.	– Готовность к исполнению воинской обязанности с применением полученных профессиональных знаний.	
ОК 11. Применять математический аппарат для решения профессиональных задач.	– Уметь применять средства математической логики для решения задач.	
ОК 12. Оценивать значимость документов, применяемых в профессиональной деятельности.	– Уметь оценивать документы, используемые в области защиты информации.	