Программа
практики

УП.01 УЧЕБНАЯ ПРАКТИКА

Вид профессиональной деятельности: участие в планировании и организации работ по обеспечению защиты объекта

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 «Учебная практика» 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 «УП.01 УЧЕБНАЯ ПРАКТИКА» 4
1.1. Область применения программы 4
1.2. Место практики в структуре ОПОП 4
1.3. Цели и задачи программы практики – требования к результатам освоения профессионального модуля 4
1.4. Количество часов на освоение программы практики 5
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ 5
3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ 7
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ 9
4.1. Требования к минимальному материально-техническому обеспечению ... 9
4.2. Информационное обеспечение обучения 9
4.3. Общие требования к организации образовательного процесса 10
4.4. Кадровое обеспечение образовательного процесса 10
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ) 11

1. ПАСПОРТ ПРОГРАММЫ ПРАКТИКИ «УП.01 УЧЕБНАЯ ПРАКТИКА»

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 основного вида профессиональной деятельности (далее – ВПД): участие в планировании и организации работ по обеспечению защиты объекта.

1.2. Место практики в структуре ОПОП

«УП.01 Учебная практика» входит в профессиональный модуль «Участие в планировании и организации работ по обеспечению защиты объекта».

1.3. Цели и задачи программы практики – требования к результатам освоения профессионального модуля

С целью овладения указанным ВПД и соответствующими компетенциями обучающийся в ходе прохождения учебной практики должен:

иметь практический опыт:

– использования физических средств защиты объекта;

– применения физических средств контроля доступа на объект;

– ведения текущей работы исполнителей с конфиденциальной информацией;

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;

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.

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.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

Код и наименование дисциплины	Наименования тем учебной практики	Количество часов по темам
2	3	4
МДК.01.01. Обеспечение организации системы безопасности предприятия.	1. Разработка должностной инструкции охранника объекта. 2. Разработка должностной инструкции начальника охраны объекта. 3. Подготовка проекта установки камер внешнего видеонаблюдения объекта. 4. Подготовка проекта установки камер внутреннего видеонаблюдения объекта. 5. Составление технического регламента работы с конфиденциальной информацией для персонала, имеющего допуск к конфиденциальной информации. 6. Составление технического регламента о порядке оформления допуска лиц к конфиденциальным сведениям. 7. Составление технического регламента работы с системой внешнего видеонаблюдения. 8. Составление технического регламента работы с системой внутреннего видеонаблюдения. 9. Составление технического регламента организации и проведения рабочих совещаний. 10. Подготовка проекта выделения зон доступа по типу работ на объекте. 11. Подготовка проекта выделения зон доступа по конфиденциальности работ объекте. 12. Подготовка проекта установки СКУД на объекте. 13. Составление технического регламента работы с СКУД объекта. 14. Составление Положения об охране персонала объекта. 15. Составление Положения о режимных помещениях объекта. 16. Подготовка проекта оборудования режимного помещения объекта.	72
МДК.01.02. Организация работ подразделений защиты информации	1. Подготовка проекта структуры управления службой защиты информации. 2. Разработка мероприятий по контролю направлений деятельности службы защиты информации. 3. Разработка мероприятий по мониторингу направлений деятельности службы защиты информации. 4. Составление программы оценки эффективности работы службы защиты информации. 5. Разработка схемы взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации. 6. Составление карт организации трудового процесса.	36
МДК.01.03. Организация работы персонала с конфиденциальной информацией	1. Составление технического регламента организации и проведения совещаний по конфиденциальным вопросам. 2. Составление Положения о защите информации при приеме посетителей на объекте. 3. Составление Положения о процедуре служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.	36

	4. Составление Положения об организации работы при осуществлении международного сотрудничества. 5. Составление технического регламента контроля соблюдения персоналом требований режима защиты информации на объекте. 6. Проведение исследования о целесообразности внедрения биометрических систем безопасности на объекте. 7. Проведение технического аудита системы видеонаблюдения объекта. 8. Проведение технического аудита СКУД объекта. 9. Проведение технического аудита безопасности компьютерных систем объекта. 10. Составление Положения о подразделении защиты информации. 11. Составление Положения о проверке персонала по защите информации. 12. Составление технического регламента работы с компьютерными системами объекта. 13. Составление технического регламента защиты информации в процессе рекламной деятельности. 14. Проведение технического аудита организации охраны объекта. 15. Проведение исследования о соответствии подбора и расстановки сотрудников подразделений защиты информации.	
Всего часов		**144**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля требует наличия учебного кабинета информационной безопасности, лабораторий электронного документооборота и технических средств защиты информации.

Оборудование учебного кабинета:

– посадочные места по количеству обучающихся;

– рабочее место преподавателя;

– комплект учебно-методической документации;

– комплект учебно-наглядных пособий.

Технические средства обучения:

– компьютеры с лицензионным программным обеспечением;

– мультимедиапроектор;

– многофункциональные устройства.

4.2. 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. 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

3. 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

4. Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск, 2014. – 137 с. – Режим доступа: https://kbis.susu.ru/kb15/teor.pdf

Дополнительные источники:

Журнал «Защита информации. Инсайд»

Интернет-ресурсы:

1. Информационно-правовой портал «Гарант» http://www.garant.ru/
2. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
3. Федеральный портал «Российское образование» - http://www.edu.ru/
4. Интегральный каталог ресурсов Федерального портала «Российское образование» http://soip-catalog.informika.ru/
5. Федеральный фонд учебных курсов - http://www.ido.edu.ru/ffec/econ-index.html
6. Комплексная система защиты от утечек корпоративной информации - http://www.securit.ru

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

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

4.3. Общие требования к организации образовательного процесса

Практика является обязательным разделом ОПОП. Она представляет собой вид учебных занятий, обеспечивающих практико-ориентированную подготовку обучающихся. Учебная практика проводятся образовательной организацией при освоении обучающимися профессиональных компетенций в рамках профессиональных модулей и реализуется концентрированно.

Аттестация по итогам учебной практики проводится с учетом (или на основании) результатов, подтвержденных документами по результатам практики.

Реализация программы учебной практики предполагает наличие у образовательной организации базы социальных партнеров.

4.4. Кадровое обеспечение образовательного процесса

Учебная практика проводится преподавателями дисциплин профессионального цикла, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины (модуля). Организацию и руководство учебной практикой осуществляют руководители практики от колледжа и от организации.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

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 освоения образовательной программы: – на практических занятиях (при решении ситуационных задач, участии в деловых играх, при подготовке рефератов, докладов, компьютерных презентаций и т.д.); – при выполнении и защите практических и лабораторных работ; – при выполнении работ на различных этапах учебной и производственной практики; – при проведении тестирования, зачетов, экзаменов, квалификационного экзамена по модулю.
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 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.	

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 результатов деятельности обучающихся в процессе освоения образовательной программы: – на практических занятиях (при решении ситуационных задач, участии в деловых играх, при подготовке рефератов, докладов, – компьютерных презентаций и т.д.); – при выполнении и защите практических и лабораторных работ; – при выполнении работ на различных этапах производственной практики; – при проведении: тестирования, зачетов, экзаменов, квалификационного экзамена по модулю; – проверка выполнения самостоятельной работы; – защита работ на различных этапах производственной 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.	