

**Программа  
практики**

**УП.03 УЧЕБНАЯ ПРАКТИКА**

**Вид профессиональной деятельности: программно-  
аппаратные и технические средства защиты информации**

2019 г.

РАССМОТРЕНА

на заседании ЦМК  
информационно-технических  
и профессиональных  
дисциплин  
Протокол от  
«24» мая 2019 года № 4

СОГЛАСОВАНО

Директор ООО «СКБ»  
И.Л. Закопайло

« 28 » мая 2019 года



УТВЕРЖДЕНА

Директор ОмЮК  
Ю.А. Бурдельная

« 28 » мая 2019 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.03 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 .....	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ .....	5
3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ .....	6
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ .....	7
4.1. Требования к минимальному материально-техническому обеспечению ...	7
4.2. Информационное обеспечение обучения .....	7
4.3. Общие требования к организации образовательного процесса .....	8
4.4. Кадровое обеспечение образовательного процесса .....	8
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ) .....	9

# **1. ПАСПОРТ ПРОГРАММЫ ПРАКТИКИ «УП.03 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): программно-аппаратные и технические средства защиты информации.

## **1.2. Место практики в структуре ОПОП**

«УП.03 Учебная практика» входит в профессиональный модуль «Программно-аппаратные и технические средства защиты информации».

## **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:**

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

– применения технических средств защиты информации;

– выявления возможных угроз информационной безопасности объектов защиты;

### **уметь:**

– работать с техническими средствами защиты информации;

– работать с защищенными автоматизированными системами;

– передавать информацию по защищенным каналам связи;

– фиксировать отказы в работе средств вычислительной техники;

### **знать:**

– 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.

## **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 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.

### 3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

Код и наименование дисциплины	Наименования тем учебной практики	Количество часов по темам
2	3	4
МДК.03.01 Технические методы и средства, технологии защиты информации.	1. Создание защищённого канала передачи данных. 2. Настройка идентификации пользователей в автоматизированной системе. 3. Тестирование пожарно-охранной сигнализации. 4. Отслеживание журнала аудита. 5. Проверка системы на вирусы и несанкционированный доступ. 6. Анализ и оценка каналов утечки информации. 7. Исключения несанкционированного доступа к информационным ресурсам. 8. Приемы, методы и способы выявления неисправностей в компьютерах, компьютерных системах и сетях. 9. Описание (моделирование) объектов защиты; 10. Выявление демаскирующих признаков объектов защиты.	72
МДК.03.02 Программно-аппаратные средства защиты информации.	1. Использование диагностического оборудования для диагностики технического состояния инженерно-технических средств защиты информации. 2. Использование программно-аппаратных комплексов для диагностики технического состояния инженерно-технических средств защиты информации. 3. Осуществление работ с техническими средствами защиты информации. 4. Осуществление работ с защищенными автоматизированными системами. 5. Передача информации по защищенным каналам связи.	72
<b>Всего часов</b>		<b>144</b>

## 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.

Оборудование лабораторий электронного документооборота и технических средств защиты информации:

- посадочные места, рассчитанные на подгруппу;
- мультимедийные средства обучения;
- рабочее место преподавателя;
- компьютеры с лицензионным программным обеспечением;
- специализированное программное обеспечение;
- системы доступа;
- программно-аппаратные средства защиты информации.

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://bibli-online.ru/bcode/431332>

2. 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>

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/Elekt\\_r\\_uch.\\_posobie\\_OOIB1.pdf/download/Elekt\\_r\\_uch.\\_posobie\\_OOIB1.pdf](http://elib.fa.ru/fbook/Elekt_r_uch._posobie_OOIB1.pdf/download/Elekt_r_uch._posobie_OOIB1.pdf)

4. 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://bibli-online.ru/bcode/431080>

#### 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](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>

5. 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>

#### **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 проводится 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 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.	<ul style="list-style-type: none"> <li>– Обоснованность выбора технических и программно-аппаратных средств защиты информации;</li> <li>– грамотное применение технических и программно-аппаратных средств защиты информации;</li> <li>– правильность освоения возможностей работоспособности компонентов систем защиты информации.</li> </ul>	<p>Оценка результатов деятельности обучающихся в процессе освоения образовательной программы:</p> <ul style="list-style-type: none"> <li>– на практических занятиях (при</li> </ul>
ПК 3.2. Участвовать в эксплуатации систем средств защиты информации защищаемых объектов.	<ul style="list-style-type: none"> <li>– Умение решать частные технические задачи, возникающие при эксплуатации систем и средств защиты информации;</li> <li>– умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации.</li> </ul>	<p>решении ситуационных задач, участии в деловых играх, при подготовке рефератов, докладов, компьютерных презентаций и т.д.);</p> <ul style="list-style-type: none"> <li>– при выполнении и защите практических и лабораторных работ;</li> </ul>
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	<ul style="list-style-type: none"> <li>– Точность и скорость диагностики нарушений эксплуатационных характеристик средств защиты;</li> <li>– качество анализа эксплуатационных свойств средств защиты;</li> <li>– проверка технического состояния средств защиты;</li> <li>– умения проводить техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность средств защиты.</li> </ul>	<ul style="list-style-type: none"> <li>– при выполнении работ на различных этапах учебной и производственной практики;</li> </ul>
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	<ul style="list-style-type: none"> <li>– Умение выявлять и анализировать возможные угрозы информационной безопасности объектов.</li> </ul>	<ul style="list-style-type: none"> <li>– при проведении тестирования, зачетов, экзаменов, квалификационного экзамена по модулю.</li> </ul>

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.

<b>Результаты (освоенные общие компетенции)</b>	<b>Основные показатели оценки результата</b>	<b>Формы и методы контроля и оценки</b>
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:
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.	– на практических занятиях (при решении ситуационных задач, участии в деловых играх, при подготовке рефератов, докладов, – компьютерных презентаций и т.д.);
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– Решение стандартных и нестандартных профессиональных задач в области защиты информации.	– при выполнении и защите практических и лабораторных работ;
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.	– при выполнении работ на различных этапах производственной практики;
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	– Работа профессиональными информационными системами.	– при проведении: тестирования, зачетов, экзаменов, квалификационного экзамена по модулю;
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	– Взаимодействие обучающимися, преподавателями и мастерами в ходе обучения.	– проверка выполнения самостоятельной работы;
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	– Самоанализ и коррекция результатов собственной работы.	– защита работ на различных этапах производственной практики.

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.	