# ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ПРОФЕССИОНАЛЬНЫЙ ЦЕНТР ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ»

# (ООО «ПРОЦПБ»)

**УТВЕРЖДАЮ:**

Генеральный директор

ООО «ПроЦПБ»

\_\_\_\_\_\_\_\_\_А.И.Тихонов

**Учебно-тематический план программы повышения квалификации**

**«Информационная безопасность»**

**Код профессии: 26579**

**Категория:** руководители, специалисты и администраторы, ответственные за состояние информационной безопасности и организацию работ по созданию комплексных систем защиты информации в организации.

**Цель:** повышение квалификации ответственных лиц.

**Объем:** 72 часа.

**г. Пятигорск**

**2022 г.**

|  |
| --- |
|  |

**1. Пояснительная записка**

Целью изучения программы является повышение квалификации в сфере безопасности в информационном обществе и на этой основе формирование пониманий технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

К задачам дисциплины относятся:

- формирование общих представления о безопасности в информационном обществе;

- описать общие принципы технологий, применяемых в информационной безопасности;

- привить умения применять правила кибербезопасности во всех сферах деятельности

- освоение знаний, составляющих начала представлений об информационной картине мира и информационных процессах;

- овладение умением использовать компьютерную технику как практический инструмент для работы с информацией в повседневной жизни;

- развитие навыков ориентирования в информационных потоках;

В результате освоения программы профессиональной переподготовки слушателем будут приобретены следующие знания, навыки и умения:

**знать:**

- объекты компьютерных технологий, используемые в обеспечении кибербезопасности;

- понятийный аппарат информационных технологий и особенности терминологии кибербезопасности;

- базовые составляющие в области развития систем информационной безопасности

- объекты компьютерно-технической экспертизы;

**уметь:**

- ставить цели, формулировать задачи, связанные с обеспечением кибербезопасности;

- анализировать тенденции развития систем обеспечения кибербезопасности;

- применять знания о кибербезопасности в решении поставленных задач;

**владеть:**

**- знаниями о современных технологиях, применяемых в области кибербезопасности;**

методами проведения анализа в области обеспечения кибербезопасности.

Программа составлена с учетом знаний и навыков, полученных в общеобразовательных школах, профессионально-технических училищах, а также практических навыков обучающихся.

Форма организации обучения – очно-заочная, без отрыва от производства.

Срок обучения по программам профессиональной переподготовки и повышения квалификации составляет 72 часа. Количество часов, отводимое на изучение отдельных тем программы, последовательность их изучения в случае необходимости разрешается изменять при условии, что программы будут выполнены полностью по содержанию и общему количеству часов

Если аттестуемый, показывает знания и профессиональные умения выше установленной квалификационной характеристикой, ему может быть присвоена квалификация на разряд выше.

К концу обучения каждый рабочий должен уметь самостоятельно выполнять все работы, предусмотренные квалификационной характеристикой, в соответствии с техническими условиями и нормами, установленными на предприятии.

После теоретического обучения каждый учащийся сдает итоговое тестирование.

После окончания курса обучения и сдачи итогового тестирования слушателям выдается квалификационное свидетельство установленного образца.

**2. Тематический план**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование разделов, курсов, дисциплин, тем | Всего  часов | Всего | |
| теория | практика |
|  | Организация информационной защиты | 72 | 42 | 66 |
| 1 | Комплексная система обеспечения информационной безопасности в организации | 10 | 6 | 4 |
| 2 | Системы управления информационной безопасностью и управление рисками информационной безопасности организации | 10 | 6 | 4 |
| 3 | Безопасность удаленного доступа и межсетевого взаимодействия | 10 | 4 | 6 |
| 4 | Криптографическая защита конфиденциальной информации | 10 | 8 | 2 |
| 5 | Техническая защита конфиденциальной безопасности | 10 | 6 | 4 |
| 6 | Лицензирование в области защиты информации | 10 | 8 | 2 |
| 7 | Защита системы от вредноносных программ | 10 | 4 | 6 |
| 8 | Итоговое тестирование | 2 |  |  |
|  | Итого | 72 | 42 | 28 |

**3. Учебная программа**

**Раздел 1. Комплексная система обеспечения информационной безопасности в организации**

Предмет, цели и содержание дисциплины «Комплексная система обеспечения информационной безопасности в организации». Значение и место дисциплины в подготовке по профессии «Информационная безопасность». Актуальность проблемы обеспечения безопасности информационных технологий. Основные термины, понятия и определения в области информационной безопасности. Государственная система информационной безопасности Российской Федерации. Оценка защищенности конфиденциальной информации от ее утечки по техническим каналам. Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Способы и средства защиты защищаемых помещений от утечки акустической речевой информации по техническим каналам.

В результате обучаемый должен:

**знать:** актуальные проблемы в обеспечении безопасности информационных технологий; нормативно-правовую базу в сфере информационных технологий; способы и средства защиты информации от утечки.

**владеть:** основными терминами, определениями и понятиями в области информационных технологий;

**уметь:** оценивать защищенность конфиденциальной информации от утечки по техническим каналам.

**2. Системы управления информационной безопасностью и управление рисками информационной безопасности организации**

Основы построения комплексной системы обеспечения информационной безопасности в организации. Современные угрозы информационной безопасности автоматизированных систем. Основные компоненты комплексной системы обеспечения информационной безопасности в организации. Роль системы обеспечения информационной безопасности в системе обеспечения экономической безопасности организации. Расследование инцидентов информационной безопасности. Средства защиты информации.

В результате обучаемый должен:

**знать:** комплексные системы обеспечивания информационной безопасности в организации; основные компоненты комплексной системы обеспечения информационной безопасности в организации; средства защиты информации.

**владеть:** основными навыками для расследования инцидентов информационной безопасности.

**уметь:** оценивать основные угрозы информационной безопасности автоматизированных систем.

**3. Безопасность удаленного доступа и межсетевого взаимодействия**

Обзор компонент подсистем удалённого доступа, определяющих уровень защищённости; настройка на примере подсистемы терминального доступа; обзор механизмов защиты удалённого доступа; механизмы и технологии управлением удалённым доступом; механизмы и технологии межсетевого экранирования; механизмы и технологии построения виртуальных частных сетей; сценарии совместного применения механизмов защиты удалённого доступа.

В результате обучаемый должен:

**знать:** компоненты подсистем удаленного доступа; механизмы защиты удаленного доступа; механизмы и технологии управления удаленным доступом и межсетевым экранированием;

**владеть:** основными терминами, определениями и понятиями в области обеспечения удаленного доступа межсетевого взаимодействия;

**уметь:** строить виртуальные частные сети.

**4. Криптографическая защита конфиденциальной информации.**

Технологии криптографической защиты информации. Защита автоматизированных систем организации с использованием средства криптографической защиты. Система защиты информации «Vipnet». Система защиты информации «КриптоПро».

В результате обучаемый должен:

**знать:** актуальные проблемы в обеспечении криптографическо информации; системы защиты информации «КриптоПро» и «Vipnet».

**владеть:** основными терминами, определениями и понятиями для защиты автоматизированных систем организации с использованием средства криптографической защиты.

**уметь:** использовать средства криптографической защиты.

**5. Техническая защита конфиденциальной безопасности.**

Технические каналы утечки информации и их характеристики. Оценка защищенности конфиденциальной информации от ее утечки по техническим каналам. Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки по техническим каналам. Способы и средства защиты защищаемых помещений от утечки акустической речевой информации по техническим каналам.

В результате обучаемый должен:

**знать:** каналы утечки информации и их характеристики; способы и средства защиты информации, обрабатываемой техническими средствами, от утечки по техническим и акустическим каналам;

**владеть:** основными терминами, определениями и понятиями в области технической защиты информационных технологий;

**уметь:** оценивать защищенность конфиденциальной информации от утечки по техническим каналам.

**6. Лицензирование в области защиты информации.**

Лицензирование деятельности в области технической защиты конфиденциальной информации. Лицензирование деятельности в области шифрования информации

В результате обучаемый должен:

**знать:** актуальные проблемы в лицензировании в области технической защиты конфиденциальной информации и шифрования информации;

**владеть:** основными терминами, определениями и понятиями в области информационных технологий;

**уметь:** организовывать лицензионную защиту конфиденциальной информации.

**7. Защита системы от вредноносных программ.**

Классифицировать защищаемую ин­формацию по видам тайны и степеням кон­фиденциальности; применять основные правила и доку­менты сертификации Российской Федера­ции; классифицировать основные угрозы безопасности информации.

В результате обучаемый должен:

**знать:** нормативно-правовую документацию в сфере информационных технологий; основные каналы угрозы безопасности информации;

**владеть:** основными терминами, определениями и понятиями в области информационных технологий;

**уметь:** классифицировать защищаемую информацию по видам тайн и степеням конфиденциальности; применять основные правила и документы сертификации Российской Федерации.