Для служебного пользования
Экземпляр № 1

Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Информзащита»

СОГЛАСОВАНО

Начальник 1 Управления
ФСТЭК России

_____ / Мартинец Н.М. /
(подпись)

«__» апреля 2018 г.

М.П.

УТВЕРЖДАЮ

Директор АНО ДПО
«Учебный центр «Информзащита»

_____ / Степаненко А.А. /
(подпись)

«28» апреля 2018 г.

М.П.

ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ТЕХНИЧЕСКАЯ ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»

Сокращенное наименование:
«ТЗКИ»
Код: ПП03

Москва 2017

Выписка из Программы профессиональной переподготовки

Полный текст Программы имеет пометку «Для служебного пользования».

Предоставление копии Программы осуществляется только по письменному запросу в соответствии с положениями Постановления Правительства РФ от 03.11.1994 N 1233.

СОДЕРЖАНИЕ

1. Общие положения

Настоящая программа профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации» разработана с учетом положений:

- Федерального закона от 29 декабря 2012 г. № 273-03 «Об образовании в Российской Федерации»;
- приказа Минобрнауки России от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;
- приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 599н;
- профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Минтруда России от 3 ноября 2016 г. № 608н;
- профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 598н;
- профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 15 сентября 2016 г. № 522н;
- федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1515;
- федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратура), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1513;
- федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1512;
- федерального государственного образовательного стандарта высшего образования по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитета), утвержденного приказом Минобрнауки России от 16 ноября 2016 г. № 1426;
- федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1509;
- Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области

обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденных ФСТЭК России 4 апреля 2015 г.;

- Методических рекомендаций-разъяснений по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22 апреля 2015 г. № ВЖ-1032/06);
- примерной программы профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации», утвержденной ФСТЭК России 28 апреля 2017 г.

Программа профессиональной переподготовки позволяет формировать у слушателей (обучающихся) компетенции, необходимые им для решения задач при осуществлении следующих лицензируемых видов деятельности:

а) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам:

- в средствах и системах информатизации;
- в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;
- в помещениях со средствами (системами), подлежащими защите;
- в помещениях, предназначенных для ведения конфиденциальных переговоров;

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа (НСД) и ее модификации в средствах и системах информатизации;

в) услуги по мониторингу информационной безопасности средств и систем информатизации;

г) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации:

- средств и систем информатизации;
- помещений со средствами (системами), подлежащими защите;
- помещений, предназначенных для ведения конфиденциальных переговоров;

д) работы и услуги по проектированию в защищенном исполнении средств и систем информатизации (помещений со средствами (системами) информатизации, подлежащими защите, защищаемых помещений);

е) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

Плановая (нормативная) продолжительность освоения данной Программы составляет 360 аудиторных часов.

Программа разработана в инициативном порядке в соответствии с Приказом Директора АНО ДПО «Учебный центр «Информзащита» от 05 сентября 2016 г. №02/09/16.

Программа обсуждена и одобрена на заседании Методического совета АНО ДПО «Учебный центр «Информзащита» и утверждена Директором Учебного центра 03 июля 2017 г.

Разработчиками настоящей программы профессиональной подготовки являются:

- Ершов Дмитрий Вячеславович, заместитель директора по учебно-методической работе, кандидат технических наук;
- Бузов Геннадий Алексеевич, заведующий кафедрой защиты информации от утечки по техническим каналам, кандидат военных наук, старший научный сотрудник, доцент, академик Академии проблем безопасности, обороны и правопорядка;
- Лозовой Валерий Матвеевич, преподаватель кафедры защиты информации от утечки по техническим каналам, кандидат военных наук;
- Журавлев Владимир Владимирович, заведующий кафедрой юридических проблем защиты конфиденциальной информации;
- Лепихин Владимир Борисович, заведующий кафедрой сетевой безопасности.

2. Цель реализации программы профессиональной переподготовки

Целью реализации программы профессиональной переподготовки является формирование компетенций, необходимых специалистам для выполнения нового вида профессиональной деятельности «Техническая защита информации» в части защиты конфиденциальной информации.

Объектами профессиональной деятельности обучающихся по программе профессиональной переподготовки являются:

- автоматизированные (информационные) системы различного уровня и назначения, средства и системы информатизации, технические средства (системы), не обрабатывающие конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается, помещения со средствами (системами), подлежащими защите, помещения, предназначенные для ведения конфиденциальных переговоров (далее - объекты информатизации);
- технические каналы утечки информации (ТКУИ) на объектах информатизации и угрозы безопасности информации в автоматизированных (информационных) системах;
- способы обеспечения технической защиты конфиденциальной информации (далее - ТЗКИ), методы контроля защищенности конфиденциальной информации;
- технические средства защиты информации, защищенные технические средства обработки информации, технические средства контроля эффективности мер защиты информации, программные (программно- технические) средства защиты информации, защищенные программные (программно-технические) средства обработки информации, программные (программно-технические) средства контроля эффективности защиты информации (далее - средства ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации);

- система нормативных правовых актов, методических документов и национальных стандартов в области технической защиты информации (ТЗИ).

Обучающиеся по программе профессиональной переподготовки готовятся к осуществлению следующих видов деятельности:

- организационно-управленческая;
- проектная;
- эксплуатационная.

Обучающиеся по программе профессиональной переподготовки готовятся к решению следующих задач профессиональной деятельности:

а) в организационно-управленческой деятельности:

- планирование мероприятий, направленных на защиту информации, организация внедрения и применения политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;
- организация мероприятий по контролю (мониторингу) защищенности конфиденциальной информации на объектах информатизации;
- поддержка и совершенствование деятельности по обеспечению ТЗКИ на объектах информатизации;
- проведение аттестационных испытаний и аттестации объектов информатизации по требованиям безопасности информации;

б) в проектной деятельности:

- определение ТКУИ на объектах информатизации и угроз безопасности информации в автоматизированных (информационных) системах;
- формирование требований к обеспечению ТЗКИ на объектах информатизации (формирование требований к системе защиты информации объекта информатизации);
- проведение контроля (мониторинга) защищенности конфиденциальной информации на объектах информатизации, а также анализа применения политик (правил, процедур) по обеспечению ТЗКИ;
- разработка способов и средств для обеспечения ТЗКИ на объектах информатизации (разработка системы защиты информации объекта информатизации);
- внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрение системы защиты информации объекта информатизации);

в) в эксплуатационной деятельности:

- установка, монтаж, наладка, испытания, ремонт, техническое обслуживание средств защиты информации;
- обеспечение ТЗКИ в ходе эксплуатации объектов информатизации;
- обеспечение ТЗКИ при выводе из эксплуатации объектов информатизации.

3. Требования к квалификации поступающего на обучение

Уровень образования лица, поступающего на обучение - высшее образование, по направлению подготовки (специальности) в области математических и естественных наук,

инженерного дела, технологий и технических наук в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации, подтвержденное документом об образовании.

4. Планируемые результаты обучения

4.1 Приобретаемые профессиональные компетенции

Процесс освоения программы профессиональной переподготовки направлен на формирование у обучающихся следующих компетенций:

а) общепрофессиональных:

- способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ в своей профессиональной деятельности;
- способность определять виды и формы информации, подверженной угрозам, возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов организации, целей и задач деятельности объекта защиты;
- способность использовать достижения науки и техники в области ТЗИ, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

в организационно-управленческой деятельности:

- способность планировать мероприятия, направленные на защиту информации, организовывать внедрение и применение политик (правил, процедур) по обеспечению ТЗКИ на объектах информатизации;
- способность организовывать мероприятия по контролю (мониторингу) защищенности конфиденциальной информации на объектах информатизации;
- способность поддерживать и совершенствовать деятельность по обеспечению ТЗКИ на объектах информатизации;
- способность проводить аттестационные испытания и аттестацию объектов информатизации по требованиям безопасности информации;

в проектной деятельности:

- способность определять возможные ТКУИ и угрозы безопасности информации на основе анализа информационных процессов на объекте информатизации, целей и задач деятельности объекта защиты;
- способность формировать требования к обеспечению ТЗКИ на объектах информатизации (формировать требования к системе защиты информации объекта информатизации);
- способность проводить контроль (мониторинг) защищенности конфиденциальной информации на объектах информатизации, а также анализ применения политик (правил, процедур) по обеспечению ТЗКИ;

- способность организовывать разработку способов и средств для обеспечения ТЗКИ на объектах информатизации (разрабатывать систему защиты информации объекта информатизации);
- способность организовывать внедрение способов и средств для обеспечения ТЗКИ на объектах информатизации (внедрять систему защиты информации объекта информатизации);

в эксплуатационной деятельности:

- способность проводить работы по установке, монтажу, наладке и испытаниям средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- способность проводить работы по устранению неисправностей и ремонту (техническому обслуживанию) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- способность проводить анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей;
- способность проводить инструментальный мониторинг и анализ защищенности компьютерных систем и сетей с использованием сканеров безопасности;
- способность обеспечивать ТЗКИ в ходе эксплуатации объектов информатизации;
- способность обеспечивать ТЗКИ при выводе из эксплуатации объектов информатизации.

В результате освоения программы профессиональной переподготовки обучающийся должен получить знания, умения и навыки, которые позволят сформировать у него соответствующие компетенции для нового вида профессиональной деятельности и решения задач при осуществлении лицензируемых видов деятельности в области ТЗКИ, определенных постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (в ред. постановления Правительства Российской Федерации от 15 июня 2016 г. № 541).

4.2 Приобретаемые слушателями (обучающимися) знания, умения и навыки

Освоившие программу должны:

а) **знать:**

- нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗКИ;
- основы функционирования государственной системы противодействия иностранным техническим разведкам (ПДИТР) и ТЗИ, цели и задачи ТЗКИ;
- виды конфиденциальной информации, перечни сведений конфиденциального характера;
- возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;

- действующую систему сертификации средств защиты информации по требованиям безопасности информации;
- основы лицензирования деятельности по ТЗКИ;
- требования по ТЗКИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля (мониторинга) их выполнения);
- организацию и содержание проведения работ по ТЗКИ, состав и содержание необходимых документов;
- организацию и содержание работ по контролю (мониторингу) защищенности конфиденциальной информации, состав и содержание необходимых документов;
- правила разработки, утверждения, обновления и отмены действия документов в области ТЗКИ;
- типовую структуру, задачи и полномочия подразделения по ТЗИ;
- принципы работы основных компонентов современных технических средств информатизации;
- основы построения информационных систем и формирования информационных ресурсов, принципы построения и функционирования операционных систем, систем управления базами данных, локальных и глобальных компьютерных сетей, основные протоколы компьютерных сетей;
- типовые структуры управления, связи и автоматизации объектов информатизации, требования к их оснащенности техническими средствами;
- технические каналы утечки информации, возникающие при ее обработке техническими средствами и системами;
- способы (методы) и требования по ТЗКИ;
- подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты информации от утечки по техническим каналам, несанкционированных, непреднамеренных воздействий, контроля целостности информации;
- порядок осуществления аутентификации взаимодействующих объектов, проверки подлинности отправителя и целостности передаваемых данных;
- методы и методики контроля (мониторинга) защищенности конфиденциальной информации;
- порядок проведения контроля (мониторинга) информационной безопасности средств и систем информатизации;
- требования к средствам ТЗКИ и средствам контроля (мониторинга) эффективности мер защиты информации;
- средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации, порядок их применения, перспективы развития;
- порядок проведения аттестационных испытаний и аттестации объектов информатизации на соответствие требованиям по защите информации;
- порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным

требованиям, а также применяемую в этих целях контрольную аппаратуру и тестовые средства;

- программы и методики аттестационных испытаний и аттестации объекта информатизации на соответствие требованиям по защите информации;
- порядок установки, монтажа, испытаний средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- порядок устранения неисправностей и проведения ремонта (технического обслуживания) ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- архитектуру беспроводных сетей;
- архитектуру и принципы работы сканеров сетевого уровня;
- имеющиеся механизмы защиты, встроенные в оборудование для беспроводных сетей;
- методологию внедрения механизма анализа защищенности в корпоративной сети;
- дополнительные механизмы защиты беспроводных сетей;
- методы и методики контроля (мониторинга) защищенности конфиденциальной информации в беспроводных сетях;
- методы обработки данных мониторинга безопасности компьютерных систем и сетей;
- методы поиска уязвимостей, используемые в сканерах безопасности.
- методы сбора информации об объектах и ресурсах сети;
- механизмы реализации DDoS-атак на транспортном и прикладном уровнях;
- мотивы и цели DDoS-атак;
- особенности применения систем обнаружения атак и сканеров безопасности в беспроводных сетях;
- порядок проведения мониторинга информационной безопасности средств и систем информатизации;
- принципиальные особенности и разновидности инцидентов типа «отказов в обслуживании»;
- принципы построения систем обнаружения компьютерных атак;
- принципы работы сервисов и решений по защите от DDoS-атак;
- проблемы безопасности, связанные с применением Blurtooth-устройств;
- решения, применяемые для управления уязвимостями в крупных распределенных сетях;
- способы обнаружения и нейтрализации последствий вторжений в компьютерные системы;
- средства контроля (мониторинга) эффективности мер защиты информации;
- технологии управления «сетями-зомби»;

б) **уметь:**

- применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области ТЗКИ;
- разрабатывать необходимые документы в интересах проведения работ по ТЗКИ;
- определять возможные ТКУИ и угрозы безопасности информации в результате НСД и специальных воздействий;
- формировать требования по ТЗКИ;
- определять требования к средствам ТЗКИ на объектах информатизации;
- организовывать и проводить работы по ТЗКИ;
- организовывать и проводить работы по контролю (мониторингу) защищенности конфиденциальной информации, оформлять материалы по результатам контроля;
- применять на практике штатные средства ТЗКИ и средства контроля (мониторинга) эффективности мер защиты информации;
- проводить аттестационные испытания и аттестацию объектов информатизации на соответствие требованиям по защите информации, оформлять материалы аттестационных испытаний;
- разрабатывать программы и методики аттестационных испытаний и аттестации объектов информатизации;
- осуществлять аутентификацию взаимодействующих объектов, проверку подлинности отправителя и целостности передаваемых данных;
- проводить установку, монтаж, испытания и техническое обслуживание средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- устранять неисправности и проводить ремонт (техническое обслуживание) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- разрабатывать документы для получения лицензии на проведение работ и оказания услуг по ТЗКИ для их представления в лицензирующий орган;
- выбирать критерии фильтрации с целью блокировки трафика атаки;
- выявлять уязвимости с использованием различных средств анализа защищенности, в т.ч. Nessus, XSpider;
- задействовать базовые механизмы защиты данных в беспроводных сетях;
- использовать дополнительные механизмы защиты данных беспроводных сетей;
- использовать превентивный методы защиты сетевых ресурсов от DDoS-атак;
- использовать средства защиты периметра (межсетевые экраны, средства противодействия атакам);
- настраивать отчетность в программе MaxPatrol в соответствии с производственными необходимостями;

- настраивать централизованное обновление MaxPatrol в распределенных сетях;

- настраивать централизованное сканирование информационных систем программным комплексом MaxPatrol в распределенных сетях с учетом сдвигов часовых поясов;
- организовывать процессы управления уязвимостями;
- осуществлять мониторинг беспроводных сетей;
- планировать мероприятия по защите в случае распределенной атаки на канал или ресурс;
- повышать защищенность беспроводной сети, используя технологии VPN и IEEE802.1x;
- применять современные инструментальные средства проведения мониторинга защищенности компьютерных систем;
- проводить установку, применять современные инструментальные средства проведения мониторинга защищенности беспроводных компьютерных систем;
- работать с порталом отчетности MaxPatrol;
- работать с системой PT Tracker, предназначенной для взаимодействия отдела ИБ с отделом автоматизации;
- структурировать аналитическую информацию для включения в отчеты;
- устранять неисправности и проводить техническое обслуживание средств контроля (мониторинга) эффективности средств защиты информации;

в) **владеть навыками:**

- работы с действующей нормативной правовой и методической базой в области ТЗИ;
- выявления ТКУИ и определения угроз безопасности информации;
- определения задач, проведения организационных и технических мероприятий по ТЗКИ;
- определения задач, проведения организационных и технических мероприятий по контролю (мониторингу) защищенности конфиденциальной информации, подготовки материалов по результатам контроля;
- применения средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- работы в компьютерных сетях с учетом требований по безопасности информации;
- работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям, в том числе зарубежными информационными ресурсами;
- проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации, оформления материалов аттестационных испытаний;
- организации деятельности подразделений и специалистов в области ТЗКИ;
- проведения установки, монтажа, испытания средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;
- устранения неисправности и проведения ремонта (технического обслуживания) средств ТЗКИ и средств контроля (мониторинга) эффективности мер защиты информации;

- анализа защищенности приложений;
- анализа результатов работы сканеров уязвимостей;
- выполнять аудит безопасности беспроводных сетей;
- размещения средств анализа защищенности в корпоративной сети.

5. Условия реализации программы

Аудиторные занятия по дисциплинам (курсам, модулям) Программы включают лекции с демонстрацией презентаций на экране, семинары, практические работы с конкретными аппаратно-программными и техническими средствами защиты и контроля защищенности информации, а также лабораторные практикумы в специально оборудованных лабораториях.

Формирование профессиональных компетенций обеспечивается использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций), в сочетании с внеаудиторной самостоятельной работой.

Оснащение учебных аудиторий (лабораторий) для занятий по дисциплинам Программы:

- компьютер для преподавателя, компьютеры для слушателей (на каждого), оснащенные необходимым набором лицензионного общего и специального программного обеспечения;
- мультимедийный проектор, экран;
- изучаемые сертифицированные программные и аппаратные средства защиты и контроля защищенности информации (по соответствующим дисциплинам);
- оборудование для защиты от утечки по техническим каналам, контроля защищенности, стенды, приборы, позволяющие изучать и исследовать аппаратуру и процессы на объектах информатизации (по соответствующим дисциплинам в специальной «Лаборатории защиты информации от утечки по техническим каналам»).

Перечень используемого в Программе сертифицированных средств защиты, оборудования и измерительных приборов приведен в Приложении 1.

Все компьютеры учебных аудиторий и рабочие места преподавателей объединены в локальные вычислительные сети, технологически реконфигурируемые под требования соответствующих курсов (модулей, дисциплин). Сети учебных аудиторий, в свою очередь, объединены между собой и имеют выход в сеть Интернет через выделенные сервера-посредники прикладного уровня.

Лабораторные работы проводятся на компьютерных стендах, воссоздающих или эмулирующих реальные объекты информационных систем, или с реальными техническими средствами/приборами/установками/системами. Выполнение работ может проводится как под контролем преподавателя, так и самостоятельно (в том числе с программными средствами защиты на виртуальных машинах в центре обработки данных).

Специализированная лаборатория для практических занятий по технической защите конфиденциальной информации от утечки по техническим каналам оснащена необходимым контрольно-измерительным оборудованием, действующими стендами, позволяющими в полном объеме исследовать и оценить возможности по защите

конфиденциальной информации от утечки по техническим каналам, в лаборатории имеется комплект средств ТЗИ для демонстрации способов защиты информации от утечки по техническим каналам.

Специализированная лаборатория для практических занятий по технической защите конфиденциальной информации от несанкционированного доступа оснащена необходимыми средствами защиты информации и средствами инструментального контроля защищенности, действующими стендами, позволяющими изучать работу со специальным программным обеспечением.

Специализированная лаборатория для практических занятий по аттестации объектов информатизации по требованиям защиты информации оснащена необходимым контрольно-измерительным и испытательным оборудованием для проведения аттестационных испытаний, программными средствами контроля защищенности, действующими стендами, позволяющими в полном объеме отработать методики проведения аттестационных испытаний.

Занятия по темам и дисциплинам, связанным с изучением документов, содержащих служебную информацию ограниченного распространения, проводятся в учебных аудиториях и на средствах вычислительной техники, аттестованных в установленном порядке. Занятия по ряду тем и дисциплин, не связанных с изучением документов, содержащих служебную информацию ограниченного распространения, могут проводиться в учебных аудиториях и на средствах вычислительной техники, не прошедших аттестацию.

Предоставление доступа к основной и дополнительной литературе по учебным дисциплинам, управление обучением и тестированием реализуется с использованием системы управления обучением.

Реализация программы профессиональной переподготовки обеспечивается штатными преподавателями Учебного центра «Информзащита», а также специалистами высшего уровня квалификации в области ТЗИ, привлекаемыми к преподаванию из числа лиц, имеющих большой опыт практической работы в различных областях обеспечения информационной безопасности, включая проектирование, разработку, эксплуатацию и оценку средств, и аттестацию систем защиты информации.

Передача программы профессиональной переподготовки другой образовательной организации допускается при создании необходимых условий её реализации и соблюдении требований законодательства Российской Федерации о порядке обращения со служебной информацией ограниченного распространения и наличии разрешения федеральных государственных органов, в ведении которых находятся организации, осуществляющие образовательную деятельность.

Внесение изменений в настоящую программу профессиональной переподготовки осуществляются в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области образования, обеспечения безопасности и защиты информации и порядком обращения со служебной информацией ограниченного распространения.

Незначительные правки, вызванные изменениями в нормативной базе или в составе учебных дисциплин (модулей, курсов) вносятся в рабочем порядке.

Существенные изменения в программу рассматривается Методическим советом Учебного центра, а сама Программа повторно утверждается директором Учебного центра и проходит процедуру согласования в установленном порядке.

6. Формы аттестации и оценочные материалы

6.1 Оценка качества освоения программы

Система оценки качества освоения программы профессиональной переподготовки включает текущий контроль успеваемости (контроль посещаемости и активности на семинарах, опросы, контроль выполнения практических и лабораторных работ по учебным дисциплинам), промежуточные (по завершении освоения каждой учебной дисциплины (модуля, курса) программы) и итоговую аттестацию обучающихся.

Освоение каждой учебной дисциплины программы профессиональной переподготовки завершается зачетом, который принимает преподаватель, ведущий занятия по данному курсу. Зачет может проводиться в форме собеседования или в форме теста.

Тестирование при помощи контрольных вопросов, контрольных задач и заданий может быть организованно в устной или письменной форме, а также с использованием электронных методов и средств тестирования.

Для каждого теста разработана система оценки, параметрами которой являются количество вопросов, их сложность, полнота ответа на вопрос. По результатам ответа на вопрос испытуемому присваивается определенное системой оценки количество баллов. Итоговое решение о прохождении теста принимается на основании превышения суммарно набранного количества баллов по всем вопросам над определенным системой оценки пороговым значением.

Освоение настоящей программы профессиональной переподготовки завершается обязательной итоговой аттестацией обучающихся. Итоговая аттестация слушателей проводится в форме тестирования (обычно в электронном виде) по основным темам изученных базовых дисциплин профессионального цикла и заключительного собеседования с членами аттестационной комиссии. К собеседованию допускаются только успешно прошедшие тестирование слушатели.

Перечень вопросов Итоговой аттестации (для экзамена) формируется из перечней основных вопросов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным дисциплинам.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается Директором Учебного центра. В целях обеспечения объективного определения практической и теоретической подготовленности обучающихся к выполнению профессиональных задач по результатам обучения в состав аттестационной комиссии могут включаться представители ФСТЭК России (управлений ФСТЭК России по Центральному федеральному округу).

Лицам, успешно освоившим программу профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации», выполнившим все требования учебного плана и прошедшим итоговую аттестацию, по решению аттестационной комиссии выдается диплом о профессиональной переподготовке с указанием нового вида профессиональной деятельности «Техническая защита информации».

7. Учебный план программы профессиональной переподготовки «Информационная безопасность. Техническая защита конфиденциальной информации»

7.1 Категории обучающихся: специалисты, работающие в области ТЗКИ.
7.2 Формы обучения: очная или очно-заочная.
7.3 Продолжительность (трудоёмкость) обучения: 490 часов.
7.4 Режим занятий: 8 часов учебных (аудиторных) занятий с преподавателем и 1 час самостоятельной работы в день.

Продолжительность академического часа соответствует нормативным требованиям (45 мин).

7.5 План учебного процесса

№ п/п	Наименование учебных дисциплин	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1.1.	Организационно-правовые основы ТЗКИ	30	18	6	10	2	-	2	10	Зачет
1.2.	Средства и системы обработки информации	42	32	6	4	8	14	2	8	Зачет
1.3.	Способы и средства ТЗКИ от утечки по техническим каналам	60	46	12	4	6	24	2	12	Зачет
1.4.	Меры и средства ТЗКИ от НСД	60	46	6	4	10	26	2	12	Зачет
1.5.	ТЗКИ от специальных воздействий	10	6	2	2	2		2	2	Зачет
1.6.	Организация защиты конфиденциальной информации на объектах информатизации	52	38	6	6	26		2	12	Зачет
1.7.	Аттестация объектов информатизации по требованиям безопасности информации	48	36	6	4	14	12	2	10	Зачет
1.8.	Контроль состояния ТЗКИ	72	54	14	18	16	6	2	16	Зачет
1.9.	Инструментальный контроль защищенности компьютерных сетей	50	40	20		20		2	8	Зачет
1.10.	Безопасность беспроводных сетей	30	24	10		14		1	6	Зачет
1.11.	Организация защиты от DDoS-атак	20	16	9		7		1	2	Зачет
2.	**Итоговая аттестация**	**16**	**4**	**-**	**-**	**-**	**-**	**-**	**12**	**Экзамен**
Итого:		**490**	**360**	**97**	**52**	**125**	**82**	**20**	**110**	**-**

7.6 Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней / часов)			Распределение учебного времени (количество часов)					
Все-го	Из них		Всего часов учебных занятий	В том числе		Время на самостоя-тельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	Учебное время		Учебные занятия по расписанию	Практики			
77	22	55/490	490	376		110	4	

* по 9 час (8 час занятий + 1 час самоподготовки) в день

8. Календарный учебный график

Продолжительность обучения: **490** часов**, 11** недель**, 2,5** месяца.

Срок обучения по программе профессиональной переподготовки, месяцы	1				2				3		
Срок обучения по программе профессиональной переподготовки, недели	1	2	3	4	5	6	7	8	9	10	11
Виды занятий, предусмотренные программой профессиональной переподготовки	А	А	А	А	А	А	А	А	А	А	А,И

А - аудиторная и самостоятельная работа;
И - итоговая аттестация.