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

УТВЕРЖДАЮ

Директор АНО ДПО «Учебный центр «Информзащита»

_____ / Степаненко А.А. /
(подпись)

«22» февраля 2018 г.

М.П.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ПОСТРОЕНИЕ, ТОНКАЯ НАСТРОЙКА, ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ PKI И ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ НА ОСНОВЕ ПАК «КРИПТО ПРО УЦ» 2.0»

Сокращенное наименование: «ИОК-127»

Код: Т127

Москва
2019

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая программа повышения квалификации «Построение, тонкая настройка, техническое обслуживание PKI и использование электронной подписи на основе ПАК «Крипто Про УЦ» 2.0» (далее – «Программа») относится к дополнительным профессиональным программам в области информационной безопасности (далее - ИБ) и разработана с учетом положений:

- Федерального закона от 29 декабря 2012 г. № 273-03 «Об образовании в Российской Федерации»;
- Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам (утв. приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499);
- Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности (утв. приказом Министерства образования и науки РФ от 05 декабря 2013 г. № 1310);
- 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).

Программа сформирована с учётом видов профессиональной деятельности, трудовых функций и уровней квалификации, установленных в профессиональных стандартах:

- «Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 15 сентября 2016 г. № 522н;
- «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 598н;

При разработке содержания Программы учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего образования (ФГОС ВО) по направлению подготовки «Информационная безопасность», а именно:

- ФГОС ВО по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1512;

Программа повышения квалификации реализуется в АНО ДПО «Учебный центр «Информзащита».

Программа разработана в инициативном порядке в соответствии с Приказом Директора от «01» октября 2017 г. №01/10/17.

Программа обсуждена и одобрена на заседании Методического совета АНО ДПО «Учебный центр «Информзащита» «02» февраля 2018 г., протокол № 2 и утверждена Приказом Директора от «02» февраля 2018 г. № 01/02/18.

Разработчики:

- Артамошин Евгений Александрович, заведующий кафедрой безопасности электронных коммуникаций;
- Ершов Дмитрий Вячеславович, к.т.н., заместитель директора по учебно-методической работе.

Обучение по данной Программе направлено на решение следующих основных задач:

- получение и углубление профессиональных знаний и умений обучающимися по правовым основам защиты информации, организационным мерам и техническим средствам обеспечения безопасности при использовании современных информационных технологий на предприятиях и в организациях;
- удовлетворение потребности специалистов в получении знаний об актуальных нормативных требованиях к защите и о новейших достижениях в области защиты конфиденциальной информации и систем её обработки (в приобретении или комплексном обновлении их профессиональных компетенций, в рамках указанного вида профессиональной деятельности);
- популяризация передовых технологий, подходов, решений, методов и средств обеспечения защиты конфиденциальной информации предприятий (объединений), организаций и учреждений, распространение передового опыта по успешному решению задач обеспечения информационной безопасности;
- оказание помощи предприятиям (объединениям), организациям и учреждениям в повышении квалификации руководителей и инженерно-технических работников (специалистов) служб безопасности и подразделений защиты информации по вопросам построения и эффективного применения комплексных систем и средств защиты информации;
- повышение квалификации руководителей и инженерно-технических работников (специалистов по защите информации) предприятий и организаций, в соответствии с квалификационными требованиями к персоналу в штате у соискателя лицензии (лицензиата) на осуществление лицензируемых видов деятельности по направлениям ФСТЭК России.

2. ЦЕЛЬ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Целью реализации Программы является повышение профессионального уровня обучающихся (слушателей) в рамках имеющейся квалификации, формирование и (или) совершенствование у них компетенций, необходимых для выполнения трудовых функций (должностных обязанностей) в рамках профессиональной деятельности по обеспечению информационной безопасности автоматизированных систем и обеспечению защищенности объектов информатизации на базе компьютерных систем и сетей с применением средств криптографической защиты (средств электронной подписи в рамках инфраструктуры открытых ключей).

Программа направлена на формирование у слушателей знаний о базовых понятиях технологии инфраструктур открытых ключей, нормативно-правовых основах деятельности органа криптографической защиты, удостоверяющих центров и юридически значимого документооборота, а также формирование умений решения практических вопросов деятельности администраторов безопасности органа криптографической защиты, в том числе по автоматизации управления жизненным циклом сертификатов открытых ключей и ключевых носителей.

2.1 Характеристика вида профессиональной деятельности

а. **Область профессиональной деятельности** слушателей, обучающихся по Программе, включает сферы техники и технологий, охватывающие совокупность проблем, связанных с:
- защитой информации в автоматизированных системах управления и обеспечением их безопасности в условиях существования угроз в информационной сфере;
- эксплуатацией и администрированием средств и систем защиты информации компьютерных систем.

б. Объекты профессиональной деятельности:
- объекты информатизации, включающие автоматизированные информационные системы, входящие в них средства обработки, хранения и передачи информации и информационно-технологические ресурсы, подлежащие защите и функционирующие в условиях существования угроз в информационной сфере;
- угрозы безопасности и технологии обеспечения информационной безопасности автоматизированных систем;
- системы управления информационной безопасностью автоматизированных систем;
- методы и реализующие их средства защиты информации в компьютерных системах и сетях (включая средства криптографической защиты информации - СКЗИ);

- процессы, возникающие при защите информации, обрабатываемой в компьютерных системах;
- методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах;
- система нормативных правовых актов, методических документов и национальных стандартов в области информационной безопасности.

в. Виды профессиональной деятельности и решаемые задачи

Программа ориентирована на подготовку слушателей к следующим видам профессиональной деятельности:

- организационно-управленческая;
- проектная;
- эксплуатационная;
- контрольно-аналитическая.

Слушатели, успешно завершившие обучение по данной Программе, должны решать следующие задачи в соответствии с видами профессиональной деятельности:

- **в организационно-управленческой деятельности:**
  - планирование и управление информационной безопасностью объекта;
  - организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа;
  - участие в определении потребности в средствах защиты информации, контроль их поставки и эксплуатации;
  - внедрение методов и средств обеспечения безопасности объектов информатизации на основе компьютерных систем и сетей;
  - осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
  - разработка нормативных и методических документов, регламентирующих работу по защите информации и иных организационно-распорядительных документов.
- **в эксплуатационной деятельности:**
  - приемка и освоение программно-аппаратных средств криптографической защиты информации;
  - установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности (включая СКЗИ в составе ИОК);
  - администрирование подсистем информационной безопасности объекта;
  - обеспечение эффективного функционирования средств криптографической защиты информации с учетом требований по обеспечению защищенности компьютерной системы;
  - обеспечение восстановления работоспособности систем

криптографической защиты информации при возникновении нештатных ситуаций;
- составление инструкций по эксплуатации аппаратно-программных средств криптографической защиты информации.

– **в проектной деятельности:**
- сбор и анализ исходных данных для проектирования систем защиты информации с использованием ИОК и ЭП;
- определение угроз безопасности автоматизированных информационных систем на объектах информатизации и рисков от их реализации;
- формирование требований к обеспечению безопасности информации в автоматизированных информационных системах;
- разработка предложений по применению конкретных способов, методов и программно-аппаратных средств (включая СКЗИ) обеспечения безопасности информации и иных ресурсов в компьютерных системах;
- поиск рациональных решений при выборе средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения.

– **в контрольно-аналитическая деятельности:**
- проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средствах защиты информации;
- применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
- участие в обследовании объектов информатизации, их категорировании и аттестации по требованиям безопасности информации.

3. ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПОСТУПАЮЩЕГО НА ОБУЧЕНИЕ

Лица, желающие освоить Программу, должны иметь высшее образование, или получать высшее образование (проходить обучение в настоящее время), при условии, что они получат дипломы о первичном образовании в период прохождения обучения по Программе. Кандидаты на зачисление на обучение по данной Программе документально подтверждают свой уровень образования, предоставляя копии и предъявляя документы об образовании государственного или установленного образца.

Поступающим на обучение желательно иметь стаж работы (не менее 1 года), связанной с процессами обеспечения информационной безопасности в компаниях или организациях, или связанного с внедрением и эксплуатацией автоматизированных информационных систем и компьютерных сетей.

Слушатели должны иметь базовые знания и навыки работы в ОС Windows. Для лучшего освоения материала рекомендуется предварительно прослушать курсы «Разработка и управление инфраструктурой открытых ключей на базе Microsoft Windows»

и «Инфраструктура открытых ключей на Microsoft Windows Server 2008 R2».

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1 Приобретаемые профессиональные компетенции

Процесс освоения обучающимися данной Программы направлен на формирование и(или) совершенствование у них следующих компетенций[1]:

а) общепрофессиональных**:**

способность использовать нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации в своей профессиональной деятельности (ОПК-5);

способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности (ОПК-7);

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.

б) профессиональных:

В проектной деятельности:

способность разрабатывать модели угроз, формировать требования к обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации (ПСК-8.1);

способность осуществлять планирование инфраструктуры открытых ключей на основе ПАК «КриптоПро УЦ» 2.0 и обеспечение безопасности использования электронной подписи с применением программных и аппаратных решений;

способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);

способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-7);

способность участвовать в разработке подсистемы информационной безопасности компьютерной системы (ПК-8).

В организационно-управленческой деятельности:

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-15);

способность разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению информационной безопасности объектов информатизации

[1] Коды компетенций указаны в соответствии с ФГОС ВО 10.05.01

на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации (ПСК-8.5).

В эксплуатационной деятельности:

способность производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18);

способность осуществлять развертывание, эксплуатацию и техническое обслуживание инфраструктуры открытых ключей на основе ПАК «КриптоПро УЦ» 2.0 и обеспечение безопасности использования электронной подписи с применением программных и аппаратных решений различных производителей;

способностью выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций (ПК-20).

В контрольно-аналитической деятельности:

способность участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований к уровню защищенности компьютерной системы (ПК-9);

способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-10).

В результате освоения дисциплины обучающиеся должны получить знания, умения и навыки, которые позволят сформировать (совершенствовать) соответствующие компетенции для нового вида профессиональной деятельности.

Обучающиеся, освоившие Программу, должны:

знать:

- нормативно-правовые основы юридически значимого документооборота;
- основные нормативные правовые акты, а также нормативные методические документы ФСБ России в области защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, криптографическими методами;
- нормативно-правовые основы деятельности удостоверяющих центров, органов криптографической защиты, правовые основы применения ЭП/ЭЦП и СКЗИ в России;
- угрозы безопасности в системах электронного документооборота и способы снижения рисков при использовании технологии ЭП;
- принципы построения защищенного документооборота с использованием электронной подписи и виртуальных частных сетей;
- современные средства защиты от наиболее опасных атак системы дистанционного обслуживания;

- существующие криптографические алгоритмы, используемые для ЗИ, их назначение, основные характеристики;
- методы и основные схемы защиты информации с использованием СКЗИ;
- методы снижения рисков при использовании электронной цифровой подписи, а также простой, неквалифицированной и квалифицированной электронной подписи при применении их в системах электронного документооборота;
- концепцию, назначение, базовые понятия технологии, организационно-технические аспекты использования ЭП/ЭЦП и PKI (инфраструктуры открытых ключей);
- что представляют собой сертификаты открытых ключей, ключевые носители и средства ЭП/ЭЦП;
- назначение, место и роль удостоверяющих центров в управлении жизненным циклом сертификатов открытых ключей, организационно-технические аспекты использования ЭП/ЭЦП и PKI;
- особенности использования ЭП/ЭЦП и PKI в корпоративных информационных системах;
- требования по размещению технических средств с установленными СКЗИ;
- подходы и критерии выбора режимов работы компонентов УЦ в зависимости от характера и масштабов поставленных задач и требований к оказанию услуг;
- варианты настроек программных компонентов «КриптоПро УЦ 2.0» для реализации типовых регламентов оказания услуг;
- порядок планирования задач резервного копирования данных ПАК «КриптоПро УЦ 2.0»;
- порядок планирования задач восстановления ПАК «КриптоПро УЦ 2.0» после сбоя;
- порядок планирования работ по разрешению потенциальных нештатных ситуаций;
- порядок планирования задач по миграции на новые версии ПАК «КриптоПро УЦ 2.0» с предыдущий версий;
- порядок осуществления плановой и неплановой смены ключей ПАК «КриптоПро УЦ 2.0»;
- основы технологии защиты решений с применением электронной подписи в облачных сервисах;
- правовые нормы по лицензированию в области обеспечения защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, и сертификации средств защиты информации.

уметь:

- грамотно использовать в работе нормативные документы по защите информации с использованием СКЗИ;
- планировать и формировать инфраструктуру УЦ в зависимости от характера и

масштаба поставленных задач и требований по оказанию услуг;
- обоснованно выбирать необходимые программные и программно-аппаратные СКЗИ;
- применять различные программные и аппаратные средства ЭП/ЭЦП;
- оценивать риски, связанные с применением ЭП/ЭЦП и предлагать варианты их снижения;
- осуществлять настройку и использовать средства ЭП/ЭЦП и компоненты PKI в корпоративных информационных системах;
- использовать ЭП/ЭЦП в прикладных программах, интегрированных с PKI;
- обеспечивать безопасности функционирования рабочих мест с установленными средствами криптографической защиты;
- проводить информационные обследования, анализ и оценку рисков, связанных с применением ЭП/ЭЦП и предлагать варианты их снижения;
- решать прикладные задачи с использованием программно-аппаратных средств защиты различных производителей;
- осуществлять организацию контроля безопасности АРМ с установленным СКЗИ, выполнять требования эксплуатационной и технической документации на СКЗИ;
- выполнять все необходимые процедуры, определяемые регламентами оказания услуг органа криптографической защиты;
- разрабатывать организационно-распорядительные документы по вопросам защиты информации с использованием СКЗИ;
- организовывать обучение пользователей правилам работы с СКЗИ;
- применять различные программные и аппаратные средства ЭП/ЭЦП;
- формировать ключи и сертификаты с использованием различных средств ЭП/ЭЦП;
- осуществлять необходимые настройки программных компонентов «КриптоПро УЦ 2.0» и конфигурировать УЦ под заданные регламенты оказания услуг;
- проводить плановую и неплановую смену ключей ПАК «КриптоПро УЦ 2.0»;
- обеспечивать масштабирование «КриптоПро УЦ 2.0» и устойчивость его функционирования;
- проводить работы по резервному копированию данных и восстановлению ПАК «КриптоПро УЦ 2.0» после сбоя;
- проводить работы по миграции на новые версии ПАК «КриптоПро УЦ 2.0» с предыдущий версий;
- правильно действовать в нештатных ситуациях при работе с ПАК «КриптоПро УЦ».

в) **владеть навыками:**

- работы с действующей нормативной правовой и методической базой в области ЗИ в компьютерных системах и сетях.

5. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

5.1 Особенности организации учебного процесса

Обучение по Программе осуществляется единовременно (без разрывов), в порядке, определённом образовательной программой на основе договоров об обучении. Форма обучения и конкретные сроки освоения Программы определяются с учётом расписания курсов в Учебном центре и указываются в договоре об обучении.

При использовании дистанционных образовательных технологий (онлайн-вебинаров) слушатели из других часовых поясов должны учитывать, что занятия с онлайн-трансляцией (онлайн-вебинары) проводятся по рабочим дням с 10:00 до 17:30 по московскому времени. При наличии групп слушателей из удалённых регионов (одного или смежных часовых поясов) для них занятия могут быть проведены в иное, специально назначенное для этого, время (с учётом сдвига по времени).

Доступ к электронным учебным пособиям, к системе тестирования, а также к стендам (виртуальным машинам в центре обработки данных - ЦОД) для дистанционного выполнения лабораторных (практических) работ должен предоставляется слушателям круглосуточно.

Предоставление прав и реквизитов удалённого доступа обучающихся к их «личным кабинетам» и назначенным им курсам и тестам целесообразно осуществлять на весь период обучения по Программе. Контроль за прохождением этапов обучения слушателей должен вестись как лицами, ответственными за СДО и обеспечение проведения занятий с применением дистанционных технологий, и преподавателями, ведущими занятия, так и менеджерами, отвечающими за договора об обучении конкретных слушателей.

5.2 Порядок передачи Программы другой образовательной организации

Передача Учебным центром настоящей дополнительной профессиональной программы другим образовательным организациям не предусматривается.

Передача Программы повышения квалификации 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 органов управления, в ведении которых находятся организации, осуществляющие образовательную деятельность.

5.3 Порядок внесения изменений в Программу

Внесение изменений в настоящую дополнительную профессиональную программу осуществляются в соответствии с требованиями, установленными законодательными и иными нормативными правовыми актами Российской Федерации в области образования, защиты государственной тайны и информационной безопасности.

Перечень основной литературы может дополняться руководителями образовательных организаций при поступлении новых (уточненных) учебных пособий.

Перечень дополнительной литературы подлежит обновлению и (или) уточнению, с учетом введения в действие новых и утративших актуальность нормативных правовых актов и методических документов.

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 включает текущий контроль успеваемости (контроль посещаемости и активности на занятиях, опросы в начале очередного учебного дня, контроль выполнения практических и лабораторных работ), промежуточные по завершении освоения каждой учебной дисциплины (модуля, курса) Программы и итоговую аттестацию обучающихся.

Освоение каждой дисциплины (модуля, курса) Программы завершается зачетом (без оценки) в форме теста, который подразумевает ответы на контрольные вопросы по материалу курса. Зачет проводится с использованием электронной системы тестирования (основной вариант) или в бумажной форме (резервный вариант). Зачет принимает преподаватель, ведущий занятия по данной дисциплине.

Если краткосрочная программа повышения квалификации состоит только из одной учебной дисциплины (курса, модуля), то для неё промежуточная аттестация по дисциплине (курсу, модулю) является одновременно и итоговой по Программе.

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.

При использовании средств электронного тестирования, тесты для промежуточной аттестации по каждой учебной дисциплине (модулю, курсу) содержат от 10 до 30 вопросов. К каждому вопросу предлагается по четыре варианта ответов, только один из которых правильный (наиболее точный и полный). Проходной бал зачёта 2/3 правильных ответов.

Итоговая аттестация слушателей проводится в форме тестирования (обычно в электронном виде) по основным темам изученных дисциплин (модулей, курсов).

Тест итоговой аттестации для каждого слушателя формируется индивидуально и содержит 45 вопросов, выбираемых системой случайным образом из пула в 60 вопросов, сформированного из тестовых вопросов изучаемых дисциплин (модулей, курсов). Проходной бал зачёта 2/3 правильных ответов.

На прохождение теста отводится полтора часа (2 академических часа).

По результатам успешного тестирования и собеседования по каждому слушателю оформляется отдельное решение о прохождении (не прохождении) итоговой аттестации. В случае неуспешной попытки сдачи итогового теста, слушателю предоставляется время на самоподготовку и возможность повторно пройти тестирование.

Лицам, успешно освоившим Программу повышения квалификации, выполнившим все требования учебного плана и прошедшим итоговую аттестацию, выдается Удостоверение о повышении квалификации установленного образца.

Слушателям, не прошедшим итоговой аттестации или показавшим на итоговой аттестации неудовлетворительные результаты, а также слушателям, освоившим лишь часть Программы и/или отчисленным из организации, выдается справка об обучении (а также Свидетельства о прохождении обучения по отдельным модулям (курсам) Программы).

При освоении Программы слушателем параллельно с получением высшего образования Удостоверение о повышении квалификации выдаётся ему после получения соответствующего документа об основном образовании и о квалификации.

6.2 Оценочные материалы

Оценочные материалы по Программе включают наборы тестовых вопросов, используемые для контроля усвоения материала при проведении промежуточных аттестаций по каждой учебной дисциплине (курсу, модулю), а также скомпонованный из них пул тестов итоговой аттестации, реализуемые в рамках системы дистанционного тестирования на базе сервера управления обучением и тестированием Учебного центра.

Основные вопросы, включаемые в оценочные материалы промежуточных аттестаций приведены в соответствующих Рабочих программах по данным дисциплинам (модулям, курсам) в Приложении 1.

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

7. УЧЕБНЫЙ ПЛАН ПРОГРАММЫ

7.1 Категории обучающихся

Программа ориентирована на следующие категории обучающихся (слушателей):

- начальники служб безопасности, руководители подразделений обеспечения информационной безопасности (ОИБ), технической защиты (конфиденциальной) информации (ТЗИ, ТЗКИ), ответственные за состояние и обеспечение ИБ и организацию работ по созданию комплексных систем защиты конфиденциальной информации предприятий;
- аналитики подразделений ОИБ (ТЗКИ), отвечающие за анализ состояния информационной безопасности, определение требований к защищенности различных подсистем ИС и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- администраторы средств защиты и специалисты подразделений ОИБ (ТЗКИ), ответственные за защиту конфиденциальной информации техническими средствами.

7.2 Формы обучения

Программа реализуется в форме обучения с отрывом от основной работы при проведении обучения в очной форме, - с частичным отрывом от работы, при обучении с использованием дистанционных образовательных технологий (онлайн-вебинаров) и/или электронного обучения.

7.3 Продолжительность (трудоёмкость) обучения

Общий объём времени, отводимого на освоение данной Программы, составляет 96 часов, включая 80 академических часов аудиторных занятий (включая зачёты) и 16 академических часов самостоятельной учебной работы слушателя.

7.4 Режим занятий

Режим занятий: 8 академических часов учебных (аудиторных) занятий с преподавателем и 1 час самостоятельной работы в день.

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Учебные занятия организованы в одну смену. Время проведения очных занятий и онлайн-вебинаров - по рабочим дням с 10:00 до 17:30 по московскому времени. Доступ к электронным учебным пособиям и виртуальным стендам (в центре обработки данных - ЦОД) для дистанционного выполнения лабораторных работ предоставляется слушателям круглосуточно.

7.5 План учебного процесса

№№ п/п	Наименование учебных модулей, 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.	**МОДУЛЬ 1.** Использование электронной подписи и инфраструктур открытых ключей	**29**	**23**	**11**		**12**		**1**	**5**	Зачёт в форме тестирования
2.	**МОДУЛЬ 2.** Порядок развертывания и применения PKI на основе ПАК "КриптоПро УЦ" 2.0»	**19**	**15**	**8**		**7**		**1**	**3**	Зачёт в форме тестирования
3.	**МОДУЛЬ 3.** Практическая реализация регламентов деятельности удостоверяющего центра и настройка компонентов «КриптоПро УЦ 2.0»	**29**	**23**	**11**		**12**		**1**	**5**	Зачёт в форме тестирования
4.	**МОДУЛЬ 4.** Эксплуатация и техническое обслуживание PKI на основе ПАК «КриптоПро УЦ 2.0»	**18**	**15**	**8**		**7**			**3**	Зачёт в форме тестирования
	Итоговое тестирование	**1**						**1**		Зачёт в форме тестирования
	Итого:	**96**	**76**	**38**		**38**		**4**	**16**	

7.6 Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			Распределение учебного времени (количество часов)					
Всего	Из них		Всего часов учебных занятий	В том числе		Время на самостоятельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	Учебное время		Учебные занятия по расписанию	Практика			
12/96	**2**	**10/48**	**96**	**76**	**-**	**16**	**4**	**-**

8. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Срок обучения по программе повышения квалификации, месяцы	1	
Срок обучения по программе повышения квалификации, недели	2	
Виды занятий, предусмотренные программой повышения квалификации	А	И

А – аудиторная и самостоятельная работа

И – Итоговая аттестация

9. РАБОЧАЯ ПРОГРАММА УЧЕБНОГО КУРСА

9.1 Содержание учебных модулей (разделов)

Модуль 1. Использование электронной подписи и ИОК

Тема 1. Электронные документы

Тема 2. Электронная подпись. Электронная цифровая подпись

Тема 3. Криптографические методы защиты информации

Тема 4. Электронный сертификат

Тема 5. Криптопровайдеры

Тема 6. Создание электронной подписи

Тема 7. Электронные ключи eToken

Тема 8. Электронная подпись для Apple iOS

Тема 9. Электронные идентификаторы Рутокен

Тема 10. КриптоПро CSP

Тема 11. Проблемы безопасности при применении электронных подписей

Тема 12. Web-порталы и облачные сервисы

Тема 13. Компоненты PKI

Тема 14. Принципы доверия PKI

Тема 15. Эксплуатация PKI

Тема 16. Проверка подлинности цифровых сертификатов в Windows PKI

Тема 17. Процедуры аннулирования сертификатов в Windows PKI

Тема 18. КриптоПро OCSP Server

Тема 19. КриптоПро Revocation Provider

Тема 20. КриптоПро TSP Server

Тема 21. Усовершенствованная подпись КриптоПро

Промежуточный зачет (тест).

Модуль 2. Порядок развертывания и применения PKI на основе ПАК "КриптоПро УЦ" 2.0»

Тема 1. Назначение и основные возможности программно-аппаратного комплекса (ПАК) «Удостоверяющий центр «КриптоПро УЦ» версии 2.0.

Тема 2. Планирование развертывания ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 2.0.

Тема 3. Установка ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 2.0.

Тема 4. Функционирование УЦ с использованием Консоли управления ЦР.

Тема 5. Функционирование УЦ с использованием Веб-портала ЦР.

Тема 6. Установка УЦ для выпуска квалифицированных сертификатов.

Тема 7. Программный компонент УЦ «Консоль экспертизы ЭП» и АРМ Разбора конфликтных ситуаций.

Промежуточный зачет (тест).

Модуль 3. Практическая реализация регламентов деятельности удостоверяющего центра и настройка компонентов «КриптоПро УЦ 2.0»

Раздел 1. Угрозы и риски

Раздел 2. Составляющие инфраструктуры удостоверяющего центра «КриптоПро УЦ 2.0»

Раздел 3. Регламенты оказания услуг удостоверяющего центра в зависимости от форм и масштаба предприятий и организаций

Раздел 4. Техническая реализация регламента оказания услуг удостоверяющего центра настройками программных компонентов.

Раздел 5. Конфигурирование удостоверяющего центра «КриптоПро УЦ» для оказания услуг малым и средним предприятиям и организациям

Раздел 6. Конфигурирование «КриптоПро УЦ» для оказания услуг средним и крупным предприятиям и организациям.

Раздел 7. Конфигурирование «КриптоПро УЦ» для оказания услуг удаленным клиентам

Промежуточный зачет (тест).

Модуль 4. Эксплуатация и техническое обслуживание PKI на основе ПАК «КриптоПро УЦ 2.0»

Раздел 1. Техническое обслуживание ПАК «КРИПТОПРО УЦ 2.0»

Раздел 2. Проверка функционирования УЦ

Раздел 3. Поддержка процедур обеспечения непрерывности и восстановления деятельности Удостоверяющего центра

Раздел 4. Плановая смена ключей

Раздел 5. Внеплановая смена ключей

Раздел 6. Решение нештатных ситуаций связанных с эксплуатацией ПАК «КриптоПро УЦ 2.0»

Раздел 7. Обновление версии ПАК «КРИПТОПРО УЦ».

Итоговый зачет (тест).

Полдробные сведения о Модулях Программы приведены в приложении 1

9.2 Учебно-методическое и информационное обеспечение учебной дисциплины (модуля, курса)

Каждый обучающийся (слушатель) перед началом занятий по дисциплине (модулю, курсу) Программы обучения получает в постоянное пользование:

- оригинальное учебное пособие (руководство слушателя курса в печатном виде и возможность удалённого доступа к его электронному варианту на сервере СДО Учебного центра);
- справочные и вспомогательные материалы по изучаемым вопросам, а именно:
  - ссылки на тексты основных нормативных правовых актов и методических документов ФСТЭК России и ФСБ России;
  - примеры типовых организационно-распорядительные документов;
  - подборки профильных статей из периодических изданий в электронном виде;
  - перечни и ссылки на издания профильной литературы доступны слушателю в системе дистанционного обучения.

Обеспеченность слушателей учебной литературой – 100%.

а) основная литература:

1. Использование ЭП и PKI. Руководство слушателя курса КП06. - М.: УЦ Информзащита, 2019. – 639 с.
2. Порядок развертывания и применения PKI на основе ПАК «КриптоПро УЦ 2.0». Руководство слушателя курса Т012. - М.: УЦ Информзащита, 2019. – 469 с.
3. Практическая реализация регламентов деятельности удостоверяющего центра и настройка компонентов «КриптоПро УЦ 2.0». Руководство слушателя курса Т027. - М.: УЦ Информзащита, 2016. – 464 с.
4. Эксплуатация и техническое обслуживание ИОК (PKI) на основе ПАК «КриптоПро УЦ 2.0» . Руководство слушателя курса Т028. - М.: УЦ Информзащита, 2016. – 179 с.

б) дополнительная литература:

5. ФЗ от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи"
6. ФЗ от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Нормативные документы ФСБ России:

7. «Об утверждении Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены Приказом ФСБ Российской Федерации 21 февраля 2008г. № 149/54-144.
8. «Об утверждении типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены Приказом

ФСБ Российской Федерации 21 февраля 2008 г. N 149/6/6-622.

9. Приказ ФСБ Российской Федерации от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

10. Приказ ФАПСИ Российской Федерации от 13 июня 2001г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г. № 2848.

Стандарты:

11. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Москва, Стандартинформ, 2007, 11с.

12. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования». Москва, Стандартинформ, 2006, 8 с.

13. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Москва, ИПК Изд-во стандартов, 1989, 28 с.

14. ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Москва, Стандартинформ, 2012, 33 с.

15. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования». Москва, Стандартинформ, 2012, 35 с.

16. ГОСТ 29099-91. «Сети вычислительные локальные. Термины и определения». Москва, ИПК Изд-во стандартов, 1991, 27 с.

17. ГОСТ Р ИСО/МЭК 27002-2012. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Москва, Стандартинформ, 2014. 106 с.

18. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Москва, Стандартинформ, 2009, 40 с.

Учебные пособия:

19. Безопасность информационных технологий. Руководство слушателя курса БТ01. - М.: УЦ Информзащита, 2016. – 350 с.

20. Безопасность ОС Windows 7/8.1/10/2012 R2. Руководство слушателя курса БТ30. Москва, УЦ Информзащита, 2016, 588 с.

21. Безопасность компьютерных сетей. Руководство слушателя курса БТ03.-

Москва, УЦ Информзащита, 2016, 367 с.

22. Windows Server 2003 PKI Operations Guide: http://www.microsoft.com/en-us/download/details.aspx?id=6796

23. Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure: http://technet.microsoft.com/en-us/library/cc772670(WS.10).aspx

24. Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003: http://technet.microsoft.com/ru-ru/library/cc787237(v=ws.10).aspx

25. Troubleshooting Certificate Status and Revocation: http://technet.microsoft.com/en-us/library/cc700843.aspx

26. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://www.ietf.org/rfc/rfc3280.txt

27. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://www.ietf.org/rfc/rfc2527.txt

28. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP http://www.ietf.org/rfc/rfc2560.txt

29. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) http://www.ietf.org/rfc/rfc3161.txt

30. Cryptographic Message Syntax (CMS) http://www.ietf.org/rfc/rfc5652.txt

31. eToken PKI Client 5_1 SP1 Руководство администратора.

32. Java Card Platform Specification 2.2.1: http://java.sun.com/javacard/specs.html

33. Logistics of Smart Card Deployment: http://technet.microsoft.com/en-us/library/dd277379.aspx

34. ЖТЯИ.00050-02 90 02-01. Руководство администратора безопасности. Windows.

35. PKI Enhancements in Windows XP Professional and Windows Server 2003: http://technet.microsoft.com/en-us/library/bb457034.aspx

36. Инструкция по эксплуатации Rutoken.

37. Key Archival and Management in Windows Server 2003: http://technet.microsoft.com/en-us/library/cc755395(v=ws.10).aspx

38. Troubleshooting - Key Archival and Management in Windows Server 2003: http://technet.microsoft.com/en-us/library/cc787039(v=ws.10).aspx

39. КриптоПро OCSP Server. Руководство администратора.

40. КриптоПро TSP Server. Руководство администратора.

41. Komar, Brian.Windows Server 2008 PKI and Certificate Security. Microsoft Press ISBN-13:978-0-7356-2516-7, ISBN-10: 0-7356-2516-6. 2008

42. PKI Enhancements in Windows 7 and Windows Server 2008 R2: http://technet.microsoft.com/en-us/magazine/2009.05.pki.aspx?pr=blog

в) программное обеспечение:

43. Microsoft Office (2003 или новее), броузеры (программы просмотра гипертекстов)

г) базы данных, информационно-справочные и поисковые системы:

44. Система дистанционного обучения (СДО) Учебного центра «Информзащита». Режим доступа: https://sdo.itsecurity.ru/view_doc.html?mode=default
45. Сайт Учебного центра «Информзащита». Режим доступа: http://itsecurity.ru/
46. Электронный ресурс Yandex.ru. режим доступа: http://Yandex.ru
47. Электронный ресурс Google.com. Режим доступа: http://Google.com

9.3 Материально-техническое обеспечение учебного курса

Аудиторные занятия по дисциплине (модулю, курсу) включают лекции с демонстрацией презентаций на экране и практические работы (семинары) под руководством преподавателя.

Наименование специализированных аудиторий, кабинетов, лабораторий	**Вид занятий**	**Наименование оборудования, программного обеспечения**
1	2	3
Лаборатория для изучения дисциплин по теме «Управление информационной безопасностью»	Лекции, практические занятия (семинары)	Для преподавателя компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции (вебинара) Для слушателей (на каждого, не менее) компьютер: Процессор Core 2 Quad 2.50GHz Память 2 Gb Жесткий диск 500.0 Gb DVD-ROM Доступ в сеть интернет (сеть, броузер) Доступ к СДО (системе тестирования) Рассматриваемые аппаратно-программные средства защиты

Необходимое оснащение класса. Столы, стулья по количеству обучаемых, оборудование кондиционирования и вентиляции воздуха.

Для преподавателя: компьютер, мультимедийный проектор, экран, оборудование для on-line трансляции (вебинара).

В период очного обучения, каждому слушателю предоставляется компьютер с возможностью выхода в интернет, в том числе для доступа в «личный кабинет», где находится раздаточный материал по курсу (в электронном виде), а также к СДО Учебного центра для прохождения тестирования.

Тестирование слушателей в целях контроля усвоения материала по дисциплине (модулю, курсу), реализуется в системе дистанционного тестирования на базе сервера управления обучением и тестированием Учебного центра.

При использовании дистанционных образовательных технологий (онлайн-вебинаров) к компьютерам слушателей предъявляются такие же требования, как и

компьютерам в аудитории.

9.4 Методические рекомендации по организации изучения учебного курса

Используются традиционные образовательные технологии на основе объяснительно-иллюстративного метода обучения, в форме информационной лекции и практических занятий в компьютерных классах.

Формирование профессиональных компетенций обеспечивается использованием в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

9.5 Оценочные материалы

Оценочные материалы по Программы включают основные вопросы, выносимые на аттестацию (тестирование) по каждому входящему в Программу модулю (см. Рабочие программы Модулей).

10. Перечень сведений, составляющих государственную тайну, используемых в учебном процессе

В учебном процессе по данной программе повышения квалификации сведения, составляющие государственную тайну, не рассматриваются.