ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ПРИВОЛЖСКИЙ ИНСТИТУТ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ФЕДЕРАЛЬНОЙ НАЛОГОВОЙ СЛУЖБЫ», Г. НИЖНИЙ НОВГОРОД

УТВЕРЖДАЮ
Ректор Приволжского института повышения квалификации ФНС России
Н.Ф. Беляков
«30» января 2023 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«Оператор удостоверяющего центра. Электронная подпись»

(объем 102 часа)

Рассмотрена
на заседании кафедры ИБ
Протокол № 1 от 25.01.2023

Нижний Новгород – 2023

Оглавление

ВВЕДЕНИЕ

Настоящая программа повышения квалификации «Оператор удостоверяющего центра. Электронная подпись» разработана с учетом требований:

- Федерального закона от 29 декабря 2012года № 273-ФЗ «Об образовании в Российской Федерации»;

- Постановления Правительства Российской Федерации от 6 мая 2012 года № 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»;

- приказа Министерства науки и высшего образования Российской Федерации от 19 октября 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;

- приказа Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

- приказа Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 816 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Выбор тем программы и его основного содержания произведен с учетом обеспечения преемственности к государственному образовательному стандартам высшего профессионального образования направлений подготовки «Информационная безопасность» (уровень бакалавриат) - Приказ Минобрнауки России от 17.11.2020 №1427.

Цель реализации программы повышения квалификации

Целью реализации программы повышения квалификации является совершенствование компетенций, необходимых для повышения профессионального уровня в рамках имеющейся квалификации специалистов (включая государственных гражданских служащих), ответственных за обеспечение безопасности сетевых приложений и электронных коммуникаций, планирующих использование и внедрение электронной подписи (ЭП) и элементов инфраструктуры открытых ключей (PKI) в профессиональную деятельность.

Требования к квалификации поступающего на обучение

Уровень образования лица, поступающего на обучение – высшее образование по направлению подготовки (специальности) в области информационной безопасности или информационных технологий, или иное

высшее образование и стаж работы в области информационных технологий или защиты информации не менее 1 года.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Процесс освоения обучающимися программы повышения квалификации направлен на совершенствование следующих компетенций:

а) общепрофессиональных:

способность использовать нормативные правовые акты, методические документы, национальные и международные стандарты в области защиты информации и обеспечения безопасности информационных технологий в своей профессиональной деятельности;

способность определять виды и формы информации, подверженной угрозам, возможные методы и пути 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 защиты информации, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;

б) профессиональных:

-установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности, включая криптографические средства, с учетом установленных требований

-установка, настройка, эксплуатация и поддержание в работоспособном состоянии защищенных с использованием криптографических средств информационных систем с учетом установленных требований;

-использование нормативных правовых актов и нормативных методических документов для организации технологического процесса защиты конфиденциальной информации с использованием криптографических средств в информационных системах.

В результате освоения программы повышения квалификации, обучающиеся должны получить знания, умения и навыки, обеспечивающие совершенствование компетенций.

Обучающиеся должны:

а) знать:

- основные задачи и понятия криптографии;
- основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в информационных системах;
- типовые системы шифрования с открытыми ключами;
- принципы построения защищенного документооборота с использованием средств электронной подписи и виртуальных частных сетей;
- основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в информационных системах;
- основные критерии классификации, параметры и характеристики, которые необходимо оценивать при анализе вариантов реализации и выборе конкретных средств построения виртуальных частных сетей;

- цели, задачи, основные принципы организации, методы и средства контроля состояния защищенности информации на предприятии с использованием криптографических средств;

б) уметь:

- использовать криптографические методы и средства защиты информации в информационных системах;
- устанавливать, настраивать и эксплуатировать программные и программно-аппаратные средства защиты информации различных производителей (в том числе средства электронной подписи и программно-аппаратных компонентов PKI);
- формировать ключи и сертификаты с использованием различных средств электронной подписи.
- использовать криптографические средства защиты информации в информационных системах;
- администрировать системы, построенные с использованием программных и программно-аппаратных комплексов криптографической защиты информации различных производителей;
- эксплуатировать комплексы удостоверяющих центров, развернутых на базе программных комплексов различных производителей;
- администрировать программно-аппаратные компоненты PKI;
- проводить занятия с персоналом по работе с криптографическими средствами защиты информации информационной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне.
- использовать криптографические средства защиты информации в информационных системах;
- осуществлять организацию контроля безопасности автоматизированного рабочего мести с установленным СКЗИ;
- документировать процедуры и результаты контроля функционирования системы криптографической защиты информации информационной системы
- вырабатывать рекомендации для принятия решения о модернизации криптографических средств защиты информации информационной системы;
- проводить анализ недостатков в функционировании криптографических средств защиты информации информационной системы;
- устранять недостатки в функционировании криптографических средств защиты информации информационной системы.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы

по повышению квалификации федеральных государственных гражданских служащих Федеральной налоговой службы с отрывом от федеральной государственной гражданской службы

Цель: *Повышение квалификации по основным направлениям деятельности и компетенциям с учетом изменений в законодательстве, нормативных актах и программном обеспечении, используемом в ФНС России в целях совершенствования и (или) получения новой компетенции, необходимой для профессиональной деятельности, и (или) повышения профессионального уровня в*

рамках имеющейся квалификации по вопросам защиты персональных данных, обрабатываемых в информационных системах персональных данных

Категория, группа должностей: *ведущая, старшая, младшая группы должностей, категории: руководители, специалисты, обеспечивающие специалисты*

Продолжительность обучения: *102 часа*

Форма обучения: *очная с использованием дистанционных образовательных технологий в полном объеме с отрывом от исполнения служебных обязанностей по замещаемой должности государственной гражданской службы*

Режим занятий: *2-8 часов в день*

№	Наименование разделов и дисциплин	Количество часов			Форма промежуточной аттестации
		Всего	по видам занятий		
			лекции	практические занятие	
1	Криптографические методы и средства защиты. Электронная подпись	42	12	30	зачет
2	Инфраструктура открытых ключей.	42	18	24	зачет
3	Управление криптографическими ключами	16	0	16	зачет
	Итоговая аттестация	2		2	экзамен в форме тестирования
	ИТОГО	**102**	**30**	**72**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Срок обучения по программе повышения квалификации, недели	1					2					3		
Срок обучения по программе повышения квалификации, дни	1	2	3	4	5	6	7	8	9	10	11	12	13
Виды занятий, предусмотренные программой повышения квалификации	А	А	А	А	А	К	К	А	А	А	А	А	И

А- аудиторная и самостоятельная работа

И – итоговая аттестация

К – каникулы.

РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН (МОДУЛЕЙ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы и средства защиты. Электронная подпись

(наименование учебной дисциплины/раздела)

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Оператор удостоверяющего центра. Электронная подпись».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания правовых основ законодательства РФ, позволяющие специалисту по защите информации организовать мероприятия по обеспечению безопасности информации и применять в своей деятельности по должностным обязанностям программное обеспечение оператора удостоверяющего центра.

Цели, задачи и место учебной дисциплины в процессе повышения квалификации

Цель учебной дисциплины – совершенствование и (или) получение новых знаний, умений и навыков специалистами по вопросам организационно-правовых основ в области СКЗИ.

Задачи учебной дисциплины:

Актуализация знаний о целях, задачах криптографической защиты информации, основных понятиях, терминах и определениях криптографической защиты информации.

Совершенствование знаний о криптографических преобразованиях с симметричными ключами и с открытыми ключами, структуре электронного сертификата стандарта X.509

Закрепление знаний об СКЗИ КриптоПро CSP, КриптоАРМ, об электронных носителях (JaCarta, eToken, Рутокен и др.).

Учебная дисциплина является вводной в данную программу повышения квалификации. Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются при изучении последующих учебных дисциплин: «Инфраструктура открытых ключей», «Управление криптографическими ключами».

Требования к результатам освоения учебной дисциплины.

В результате освоения дисциплины обучающийся должен получить знания, умения и навыки, которые позволят сформировать соответствующие компетенции для его нового вида профессиональной деятельности. Перечень развиваемых и контролируемых в образовательном процессе знаний, умений и навыков формируется на основе нижеприведенного списка.

Обучающийся должен:

знать:

цели, задачи, основные принципы организации, методы и средства контроля состояния защищенности информации на предприятии с использованием криптографических средств;

основные задачи и понятия криптографии;

основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в информационных системах;

типовые системы шифрования с открытыми ключами;

уметь:

применять на практике требования нормативных правовых актов, методических документов, международных и национальных стандартов в области СКЗИ;

владеть навыками:

работы с действующей нормативной правовой и методической базой в области СКЗИ;

Объем учебной дисциплины и виды учебной работы

№ п/п	Наименование тем	Вид занятия
1.1	Основные понятия, термины и определения криптографической защиты информации. Криптография с симметричными ключами, с открытыми ключами	лекция практика
1.2	Структура электронного сертификата стандарта X.509. Проверка подлинности цифровых сертификатов. Отзыв сертификатов. Списки отозванных сертификатов.	Лекция практика
1.3	Средство криптографической защиты КриптоПро CSP: Назначение. Основные характеристики. Реализуемые алгоритмы. Ключевые носители. Функциональный ключевой носитель.	Лекция практика
1.4	Формирование электронной подписи. Настройка КриптоПро и КриптоАРМ.	Лекция практика
1.5	Работа с разными видами электронных носителей (JaCarta, eToken, Рутокен и др.)	лекция практика

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 42 часа (41% от всего объема программы).

Реферативное описание тем

Тема №1. Основные понятия, термины и определения криптографической защиты информации. Криптография с симметричными ключами, с открытыми ключами.

Законодательство Российской Федерации, нормативные правовые акты и нормативные методические документами ФСБ России по защите информации с использованием криптографических средств.

Криптографические методы защиты информации. Криптография с симметричными ключами. Криптография с открытыми ключами. Доверие к открытому ключу и цифровые сертификаты.

Тема №2. Структура электронного сертификата стандарта X.509. Проверка подлинности цифровых сертификатов. Отзыв сертификатов. Списки отозванных сертификатов.

Электронный сертификат. Структура сертификата. Сертификаты стандарта X.509. Основной контекст сертификата. Расширения сертификатов. Классы сертификатов. Хранилища сертификатов. Закрытые ключи, риски использования по умолчанию. КриптоАРМ. Создание самоподписанного сертификата. Анализ сертификата. Импорт и экспорт сертификатов.

Тема №3. Средство криптографической защиты КриптоПро CSP: Назначение. Основные характеристики. Реализуемые алгоритмы. Ключевые носители. Функциональный ключевой носитель.

Криптопровайдеры. Набор CSP (Cryptographic Service Provider) по умолчанию. Microsoft CSP.

КриптоПро CSP. Основные характеристики. Реализуемые алгоритмы. Установка. Настройка параметров. Получение сертификатов с использованием средства криптографической защиты «СКЗИ КриптоПро».

Тема №4. Формирование электронной подписи. Настройка КриптоПро и КриптоАРМ.

Электронная подпись. Виды электронной подписи. Правовые вопросы применения ЭП и СКЗИ в России. Особенности юридического определения ЭП. Федеральный закон «Об электронной подписи».

Создание электронной подписи. Установка и эксплуатация «КриптоАРМ».

Тема №5. Работа с разными видами электронных носителей (JaCarta, eToken, Рутокен и др.)

Электронные ключи eToken. Модели eToken. JaCarta. Российская криптография в JaCarta ГОСТ и eToken ГОСТ. Установка и настройка различных моделей eToken. Настройка параметров. Режимы работы. Получение сертификата с использованием электронных ключей eToken.

Электронные идентификаторы Рутокен. Модели Рутокен. Российская криптография в Рутокен ЭЦП. Рутокен Web. Установка и настройка различных моделей Рутокен. Настройка параметров. Режимы работы. Получение сертификата с использованием электронных ключей Рутокен.

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций и практических занятий, семинаров по данной дисциплине не предусмотрено. При проведении лекций обязательно наличие презентации.

При реализации дисциплины в рамках программы повышения квалификации приоритет отдается практической направленности обучения: практические аспекты применения законодательства и нормативных документов РФ; реализация требований нормативных документов при организации защиты информации с помощью СКЗИ на объекте защиты,

особенности подготовки локальных актов, регламентирующих использование средств защиты информации, а также, практические аспекты защиты информации с помощью СКЗИ.

Для проведения всех занятий по дисциплине рекомендуется применять современные формы и методы обучения, включая активные и интерактивные.

Для проведения лекционных занятий используются активные методы обучения, стимулирующие познавательную деятельность слушателей, опираясь на методические основы педагогической технологии «Развитие критического мышления».

Технологическую основу составляет базовая модель трех стадий «вызов – реализация смысла (осмысление) – рефлексия (размышление)», которая позволяет помочь слушателям самим определять цели обучения, осуществлять активный поиск информации и размышлять о том, что они узнали. На стадии вызова (evocation) в сознании слушателей происходит процесс актуализации имеющихся знаний и представлений о предмете изучения. Поскольку при этом сочетаются индивидуальная и групповая формы работы, участие слушателей в образовательном процессе активизируется, формируется познавательный интерес. Результатом данных процессов является самостоятельное определение ими цели дальнейшей учебной деятельности.

На стадии осмысления (realization) слушатель вступает в непосредственный контакт с новой информацией – носителем новых идей. Происходит ее систематизация. Стадия рефлексии (reflection) характеризуется тем, что слушатели закрепляют новые знания и активно перестраивают собственные представления с тем, чтобы включить в них новые понятия. Таким образом, происходит “присвоение” нового знания и формирование на его основе своего аргументированного представления об изучаемом объекте.

В ходе работы по такой модели обучающиеся овладевают различными способами интегрирования информации, учатся вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений, строить умозаключения и логические цепи доказательств, выражать свои мысли четко, понятно для других, уверенно и корректно по отношению к окружающим.

ПЛАНЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

тема «Установка, настройка и использование криптопровайдеров и сертифицированных программ шифрования и электронной подписи»

Цель: закрепить и углубить теоретические знания, приобрести практические навыки работы с сертифицированными ФСБ России СКЗИ, применяемыми в налоговых органах.

Программное и материальное обеспечение: персональные компьютеры, виртуальные машины Microsoft Hyper-V с операционной системой MS Windows, MS Word, программы криптографической защиты FileCrypt 32, Easy Crypt, BDV Data Hider, S-tools, TrueCrypt, PGP.

Учебные вопросы:

1. Установка, настройка и использование криптопровайдера КриптоПро CSP.

2. Особенности настройки сертифицированных СКЗИ.

3. Использование программного СКЗИ КриптоАРМ для шифрования и электронной подписи.

4. Использование программы МГК для формирования ключевой информации и запроса на сертификат. Получение сертификата открытого ключа от Удостоверяющего центра.

5. Настройка криптосистемы и использование защищённого почтового клиента DioPost.

Список литературы

а) основная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии». — М.: Гелиос АРВ, 2005.

2. Белов Е.Б, Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2006.

3. Введение в криптографию / Под общ. Ред. В.В. Ященко. – 4-е изд., доп. М.: МЦНМО, 2012. – 348 с.

Б) дополнительная литература, нормативные и методические документы:

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 9 сентября 2000 г. Пр-1895) – Российская газета. – 2000. – 28 сентября. – № 187.

2. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. От 27.07.2010) «Об информации, информационных технологиях и о защите информации». // Российская газета. –2006. – 29 июля. – № 165.

3. Федеральный закон от 10.04.2011 N 63-ФЗ (ред. От 01.07.2011) «Об электронной подписи». // Собрание законодательства РФ, 11.04.2011, N 15, ст. 2036.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Инфраструктура открытых ключей

(наименование учебной дисциплины/раздела)

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Оператор удостоверяющего центра. Электронная подпись».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания и приобретают практические навыки использования программного обеспечения удостоверяющего центра, позволяющие специалисту по защите информации выполнять мероприятия по обеспечению безопасности информации с использованием PKI.

Цели, задачи и место учебной дисциплины в процессе повышения квалификации

Цель учебной дисциплины – совершенствование и (или) получение новых знаний, умений и навыков специалистами по вопросам использования элементов удостоверяющего центра.

Задачи учебной дисциплины:

Изучение архитектуры, основных компонентов PKI, их функций и взаимодействие, центров сертификации, центров регистрации и клиентского ПО, моделей доверия.

Совершенствование умений и навыков формирования ключевой информации и управления жизненным циклом криптографических ключей, использования средств управления ключами.

Получение практических навыков использования отечественного программного обеспечения удостоверяющих центров.

Учебная дисциплина является основной и максимальной по объёму в данной программе повышения квалификации. Знания, умения и навыки, полученные в результате изучения данной учебной дисциплины, используются слушателями при изучении последующей учебной дисциплины «Управление криптографическими ключами» и в своей дальнейшей профессиональной деятельности.

Требования к результатам освоения учебной дисциплины.

В результате изучения данной дисциплины обучающиеся должны:

а) *знать*:

общие требования по построению PKI;

механизм взаимодействия компонентов PKI;

принципы управления ключевой информацией;

б) *уметь*:

использовать криптографические методы и средства защиты информации в информационных системах;

устанавливать, настраивать и эксплуатировать программные и программно-аппаратные средства защиты информации различных производителей (в том числе средства электронной подписи и программно-аппаратных компонентов PKI);

эксплуатировать комплексы удостоверяющих центров, развернутых на базе программных комплексов различных производителей;

администрировать программно-аппаратные компоненты PKI;

в) владеть навыками:

установки, первичной настройки компонентов PKI;

настройки и использования основных механизмов компонентов PKI;

Объем учебной дисциплины и виды учебной работы

№ п/п	Наименование тем	Вид занятия
1.1	Основные понятия и определения PKI. Назначение и взаимодействие элементов PKI.	лекция практика

	Состав PKI. Системы стандартов в области PKI. Протоколы, используемые в PKI. Основные группы приложений-потребителей услуг PKI.	
1.2	Законодательство РФ об организации работы УЦ	лекция практика
1.3	Требования к помещениям УЦ. Организация рабочего места оператора.	лекция практика
1.4	Организация работы УЦ: регламент, инструкция оператора	лекция
1.5	Дополнительные компоненты УЦ: КриптоПро OCSP, КриптоПро TSP	лекция практика
1.6	Интегрированное занятие - тренинг "Проверка достоверности сведений при обращении за сертификатом ключа проверки электронной подписи"	практика

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 42 часа (41% от всего объема программы).

Реферативное описание тем

Тема № 1. Основные понятия и определения PKI. Назначение и взаимодействие элементов PKI. Состав PKI. Системы стандартов в области PKI. Протоколы, используемые в PKI. Основные группы приложений-потребителей услуг PKI.

Основные понятия, термины и определения в области PKI. Архитектура, основные компоненты PKI, их функции и взаимодействие. Центры сертификации, центры регистрации, владельцы сертификатов, клиентское программное обеспечение, реестры сертификатов и др. Модели доверия – иерархическая, сетевая, гибридная. Цепочки сертификатов и пути сертификации.

Вопросы реализации PKI (организационные, технические). Основные стандарты PKI (PKCS, X.509, RFC). Необходимость унификации алгоритмов, схем, структур данных, протоколов и т.п. в PKI. Использование меток времени.

Протоколы PKI управления сертификатом. Требования к управлению PKI, операции управления PKI: инициализация конечного участника, начальная регистрация/сертификация, доказательство обладания закрытым ключом. Изменение ключа корневого CA. Кросс-сертификация. Запрос сертификата. Изменение ключа.

Тема №2. Законодательство РФ об организации работы УЦ.

Уполномоченный орган в сфере электронной подписи. Понятие удостоверяющего центра (УЦ). Статус и функции УЦ. Аккредитация УЦ.

Тема №3. Требования к помещениям УЦ. Организация рабочего места оператора.

Требования к персоналу, помещению, специальному оборудованию, охране. Порядок организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.

Тема №4. Организация работы УЦ: регламент, инструкция оператора.

Необходимые организационные мероприятия (назначение ответственных

лиц, разработка внутренних документов организации и т.д.). Типовой перечень внутренних организационно-распорядительных документов, регламентирующих применение средств криптографической защиты в организации.

Тема №5. Дополнительные компоненты УЦ: КриптоПро OCSP, КриптоПро TSP.

Жизненный цикл сертификатов. Генерирование ключей. Выпуск и подписание сертификатов. Распределение, использование и отзыв сертификатов. Возможные причины отзыва и приостановления действия сертификатов. Списки отозванных сертификатов (CRL) Разновидности CRL. Способы публикации CRL. Использование протокола OCSP для проверки статуса сертификата. Респондер OCSP и его настройка. Форматы сообщений протокола OCSP. Форматы подписанных данных: CMS, штампы времени TSP, формат CADES.

Тема №6. Интегрированное занятие - тренинг "Проверка достоверности сведений при обращении за сертификатом ключа проверки электронной подписи".

Нормативные документы, регламентирующие порядок получения сертификатом ключа проверки электронной подписи. Типичные ситуации, связанные с проведением проверки достоверности сведений при обращении за сертификатом ключа проверки электронной подписи. Интерактивный коучинг по составлению и проведению опроса «недобросовестных» лиц. Действия должностных лиц при выявлении нарушений.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Занятия по дисциплине проводятся в форме лекций, практических занятий, которые можно проводить в виде лабораторных работ. В процессе изучения учебной дисциплины значительное количество времени отведено на практические задания, в процессе выполнения которых слушатели получают практические навыки установки, настройки и использования компонентов PKI.

При реализации дисциплины в рамках программы повышения квалификации приоритет отдается практической направленности обучения: практические аспекты применения законодательства и нормативных документов РФ; реализация требований нормативных документов при построении PKI на объекте защиты, особенности настройки и использования отечественного программного обеспечения удостоверяющих центров.

Большинство занятий по данной дисциплине - практические и лабораторные работы, для проведения которых рекомендуется применять современные формы и методы обучения, включая активные и интерактивные.

Для проведения лекционных и практических занятий используются активные методы обучения, стимулирующие познавательную деятельность слушателей, опираясь на методические основы педагогической технологии «Развитие критического мышления».

Технологическую основу составляет базовая модель трех стадий «вызов – реализация смысла (осмысление) – рефлексия (размышление)», которая позволяет помочь слушателям самим определять цели обучения, осуществлять

активный поиск информации и размышлять о том, что они узнали. На стадии вызова (evocation) в сознании слушателей происходит процесс актуализации имеющихся знаний и представлений о предмете изучения. Поскольку при этом сочетаются индивидуальная и групповая формы работы, участие слушателей в образовательном процессе активизируется, формируется познавательный интерес. Результатом данных процессов является самостоятельное определение ими цели дальнейшей учебной деятельности.

На стадии осмысления (realization) слушатель вступает в непосредственный контакт с новой информацией – носителем новых идей. Происходит ее систематизация. Стадия рефлексии (reflection) характеризуется тем, что слушатели закрепляют новые знания и активно перестраивают собственные представления с тем, чтобы включить в них новые понятия. Таким образом, происходит “присвоение” нового знания и формирование на его основе своего аргументированного представления об изучаемом объекте.

В ходе работы по такой модели обучающиеся овладевают различными способами интегрирования информации, учатся вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений, строить умозаключения и логические цепи доказательств, выражать свои мысли четко, понятно для других, уверенно и корректно по отношению к окружающим.

ПЛАНЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. Рассчитайте количество центров регистрации для однорангового удостоверяющего центра.
2. Сколько центров сертификации должно быть в удостоверяющем центре?
3. Сколько требуется администраторов центра регистрации?
4. Какие функции выполняет администратор центра регистрации?
5. Какие функции не доступны оператору центра регистрации?
6. Каковы действия оператора в случае выявления «недобросовестных» лиц.

Список литературы

а) основная литература:

1. Варлатая, С.К. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая; соавт. М.В. Шаханова. - М.: Проспект, 2017. - 152 с.

2. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. Н.Г. Лабутин, О.И. Климченков. - Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2019. - 100 с.

3. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: ФОРУМ, 2017. - 352 с.: ил.- (Высшее образование).

4. Криптографические методы и средства защиты информации: Учебное

пособие / Н.Г. Бутакова, Н.В. Федоров. – СПб.: ИЦ «Интермедиа», 2019. – 384 с.

5. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И.Н. Васильева. — М.: Издательство Юрайт, 2016. — 349 с.

б) дополнительная литература:

1. Гатченко Н.А., Исаев А.С., Яковлев А.Д. «Криптографическая защита информации» – СПб: НИУ ИТМО, 2012. – 142с.

2. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников. - М.: Финансы и статистика, 2003.

3. Фороузан Б.А. Криптография и безопасность сетей. Учебное пособие. URSS. 2010. 784 с.

4. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

5. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

7. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

8. Постановление Правительства Российской Федерации от 6 ноября 2007 г. № 758 «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий».

9. Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (ПКЗ-2005). Утверждено приказом ФСБ России от 09 февраля 2005 г. № 66.

10. Приказ ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

11. Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

12. Приказ ФАПСИ от 13 июня 2001 г. № 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 содержащей сведений, составляющих государственную тайну»

13. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма

14. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хеширования

15. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление криптографическими ключами

(наименование учебной дисциплины/раздела)

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Оператор удостоверяющего центра. Электронная подпись».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания и приобретают практические навыки использования программного обеспечения удостоверяющего центра, позволяющие специалисту по защите информации выполнять мероприятия по обеспечению безопасности информации с использованием PKI.

Цели, задачи и место учебной дисциплины в процессе повышения квалификации

Цель учебной дисциплины – совершенствование и (или) получение новых знаний, умений и навыков специалистами по вопросам использования элементов удостоверяющего центра.

Задачи учебной дисциплины:

Изучение порядка работы с компонентами удостоверяющего центра КриптоПро УЦ.

Совершенствование умений и навыков формирования ключевой информации и управления жизненным циклом криптографических ключей, использования средств управления ключами.

Получение практических навыков использования отечественного программного обеспечения удостоверяющих центров.

Данная учебная дисциплина является итоговой учебной дисциплиной программы повышения квалификации.

Требования к результатам освоения учебной дисциплины.

В результате изучения данной дисциплины обучающиеся должны:

а) *знать*:

элементы управления центра сертификации, центра регистрации и АРМ оператора удостоверяющего центра;

механизм взаимодействия компонентов КриптоПро УЦ;

принципы управления ключевой информацией;

б) *уметь*:

использовать криптографические методы и средства защиты информации в информационных системах;

устанавливать, настраивать и эксплуатировать программные и программно-аппаратные средства защиты информации различных производителей (в том числе средства электронной подписи и программно-аппаратных компонентов КриптоПро УЦ);

эксплуатировать комплексы удостоверяющих центров, развернутых на базе программных комплексов различных производителей;

администрировать программно-аппаратные компоненты КриптоПро УЦ;

в) владеть навыками:

установки, первичной настройки компонентов КриптоПро УЦ;

настройки и использования основных механизмов компонентов КриптоПро УЦ;

Объем учебной дисциплины и виды учебной работы

№ п/п	Наименование тем	Вид занятия
1.1	ПАК «Удостоверяющий Центр «КриптоПро УЦ»: развертывание и настройка параметров компонентов Центра сертификации	практика
1.2	ПАК «Удостоверяющий Центр «КриптоПро УЦ»: развертывание и настройка параметров компонентов Центра регистрации	практика
1.3	Настройка рабочего места оператора УЦ	практика
1.4	Регистрация пользователя в УЦ и изготовление сертификата ключа подписи. Централизованная и распределенная схема обслуживания.	практика

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 16 часов (15,7% от всего объема программы).

Реферативное описание тем

Тема № 1. ПАК «Удостоверяющий Центр «КриптоПро УЦ»: развертывание и настройка параметров компонентов Центра сертификации.

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

Нормативно-правовое обеспечение деятельности УЦ. Назначение. Область применения. Основные функции. Логические компоненты. Технические средства. Электронный замок «Соболь». Смарт-карты и токены различных моделей eToken, Рутокен, JaCarta для защиты ключей ЭП. Функциональные роли.

Планирование развертывания ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 2.0. Типовые схемы публикации УЦ в сети Интернет. Лицензионные ограничения. Структура и режимы работы ЦР. Реализация ролевого администрирования. Политика PKI. Состав сертификатов ключей проверки ЭП и CRL. Дополнительные задачи УЦ.

Установка ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 2.0. Подготовка системы семейства Windows Server 2008 R2\ 2012 (R2). Настройка сервера ЦС. Настройка сервера ЦР.

Тема №2. ПАК «Удостоверяющий Центр «КриптоПро УЦ»: развертывание и настройка параметров компонентов Центра регистрации.

Настройка Консоли управления ЦР. Настройка Консоли управления ЦР.

Тема №3. Настройка рабочего места оператора УЦ.

Функционирование УЦ с использованием Консоли управления ЦР. Регистрация нового пользователя. Выпуск сертификата пользователю. Приостановление сертификата пользователя. Возобновление сертификата пользователя. Аннулирование сертификата пользователя.

Установка УЦ для выпуска квалифицированных сертификатов. Включение дополнительных полей в сертификат УЦ. Включение дополнительных полей в сертификат администратора ЦР.

Тема №4. Регистрация пользователя в УЦ и изготовление сертификата ключа подписи. Централизованная и распределенная схема обслуживания.

Функционирование УЦ с использованием Веб-портала ЦР. Отклонение запроса на регистрацию пользователя. Одобрение запроса на регистрацию пользователя. Одобрение запроса на сертификат. Установка и подтверждения установки сертификата. Проверка сертификата на подлинность. Одобрение запроса на приостановление. Одобрение запроса на восстановление.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Занятия по дисциплине проводятся в форме практических занятий и лабораторных работ, лекций по данной дисциплине не предусмотрено. В процессе изучения учебной дисциплины значительное количество времени отведено на лабораторные работы, в процессе выполнения которых слушатели получают практические навыки установки, настройки и использования компонентов КриптоПро УЦ.

При реализации дисциплины в рамках программы повышения квалификации приоритет отдается практической направленности обучения: практические аспекты применения законодательства и нормативных документов РФ; реализация требований нормативных документов при

построении КриптоПро УЦ на объекте защиты, особенности настройки и использования отечественного программного обеспечения удостоверяющих центров.

Все занятия по данной дисциплине - практические и лабораторные работы, для проведения которых рекомендуется применять современные формы и методы обучения, включая активные и интерактивные.

Для проведения практических занятий используются активные методы обучения, стимулирующие познавательную деятельность слушателей, опираясь на методические основы педагогической технологии «Развитие критического мышления».

Технологическую основу составляет базовая модель трех стадий «вызов – реализация смысла (осмысление) – рефлексия (размышление)», которая позволяет помочь слушателям самим определять цели обучения, осуществлять активный поиск информации и размышлять о том, что они узнали. На стадии вызова (evocation) в сознании слушателей происходит процесс актуализации имеющихся знаний и представлений о предмете изучения. Поскольку при этом сочетаются индивидуальная и групповая формы работы, участие слушателей в образовательном процессе активизируется, формируется познавательный интерес. Результатом данных процессов является самостоятельное определение ими цели дальнейшей учебной деятельности.

На стадии осмысления (realization) слушатель вступает в непосредственный контакт с новой информацией – носителем новых идей. Происходит ее систематизация. Стадия рефлексии (reflection) характеризуется тем, что слушатели закрепляют новые знания и активно перестраивают собственные представления с тем, чтобы включить в них новые понятия. Таким образом, происходит “присвоение” нового знания и формирование на его основе своего аргументированного представления об изучаемом объекте.

В ходе работы по такой модели обучающиеся овладевают различными способами интегрирования информации, учатся вырабатывать собственное мнение на основе осмысления различного опыта, идей и представлений, строить умозаключения и логические цепи доказательств, выражать свои мысли четко, понятно для других, уверенно и корректно по отношению к окружающим.

Для проведения практических занятий и лабораторных работ в Институте разработана среда виртуализации с виртуальными машинами, индивидуальными для каждого обучающегося. В виртуальных машинах установлены операционные системы и прикладное программное обеспечение, изучаемое слушателями на занятиях. При выполнении практических заданий применяется лицензионное программное обеспечение.

ПЛАНЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ И ЛАБОРАТОРНЫХ РАБОТ

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Практическое задание № 1. Установка сервера центра сертификации ПАК КриптоПро УЦ 2.0 на платформе MS Windows Server 2008 R2.

Практическое задание № 2. Настройка УЦ для выпуска квалифицированных сертификатов.

Практическое задание № 3. Установка сервера центра регистрации ПАК КриптоПро УЦ 2.0 на платформе MS Windows Server 2012 R2.

Практическое задание № 4. Установка консоли управления Центра регистрации КриптоПро УЦ 2.0 на платформе MS Windows 7.

Практическое задание № 5. Настройка удостоверяющего центра.

Практическое задание № 6. Регистрация пользователей в централизованном режиме в консоли управления УЦ

Практическое задание № 7. Регистрация пользователей и выпуск сертификатов через веб-портал центра регистрации.

Практическое задание № 8. Управление сертификатами пользователя через веб-портал ЦР.

Список литературы

а) основная литература:

6. Варлатая, С.К. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая; соавт. М.В. Шаханова. - М.: Проспект, 2017. - 152 с.

7. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. Н.Г. Лабутин, О.И. Климченков. - Н. Новгород: Приволжский ин-т повышения квалификации ФНС, 2019. - 100 с.

8. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: ФОРУМ, 2017. - 352 с.: ил.- (Высшее образование).

9. Криптографические методы и средства защиты информации: Учебное пособие / Н.Г. Бутакова, Н.В. Федоров. – СПб.: ИЦ «Интермедиа», 2019. – 384 с.

10. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И.Н. Васильева. — М.: Издательство Юрайт, 2016. — 349 с.

б) дополнительная литература:

16. Гатченко Н.А., Исаев А.С., Яковлев А.Д. «Криптографическая защита информации» – СПб: НИУ ИТМО, 2012. – 142с.

17. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников. - М.: Финансы и статистика, 2003.

18. Фороузан Б.А. Криптография и безопасность сетей. Учебное пособие. URSS. 2010. 784 с.

19. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

20. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

21. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

22. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

23. Постановление Правительства Российской Федерации от 6 ноября 2007 г. № 758 «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий».

24. Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (ПКЗ-2005). Утверждено приказом ФСБ России от 09 февраля 2005 г. № 66.

25. Приказ ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

26. Приказ ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

27. Приказ ФАПСИ от 13 июня 2001 г. № 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 содержащей сведений, составляющих государственную тайну»

28. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма

29. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хеширования

30. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Занятия проводятся в соответствии с методическими материалами, представленными в учебно-методическом комплексе, утвержденными на заседании кафедры Института. В содержании обучения приоритет отдается практической направленности обучения.

При проведении занятий обязательно учитывается распределение времени на лекционный материал и выполнение практических заданий в соответствии с утвержденным учебно-тематическим планом. При этом общее время на лекционный материал не превышает 30%. Практические задания предполагают разбор спорных и проблемных ситуаций из практической работы, подготовку распорядительно-организационных документов, решение практических вопросов из профессиональной деятельности обучающимися.

При выполнении лабораторных работ обучающиеся самостоятельно выполняют практические задания по установке и настройке программных средств защиты информации.

Практические задания предусматривают выполнение слушателями лабораторных работ по основным темам обучения с использованием необходимого специального программного обеспечения («ПАК "КриптоПро УЦ" 2.0») для формирования необходимых навыков его использования.

Основными видами самостоятельной работы обучающихся без участия преподавателей являются:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– подготовка к групповым занятиям по определенной теме дисциплины.

Каждый обучающийся на весь период обучения обеспечен индивидуальным неограниченным доступом к электронным учебным материалам, содержащим всю необходимую учебную и учебно-методическую информацию по изучаемым модулям. На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных правовых актов и практических действий. Часть лекций может излагаться проблемным методом с привлечением обучающихся для решения сформулированных преподавателем проблем.

На практические занятия и лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий отрабатываются задания, учитывающие специфику выполняемых функциональных обязанностей обучающихся по своему профессиональному предназначению, в том числе предусмотрены задания с проведением деловых игр (эпизодов) и созданием ситуаций, моделирующих типовые нарушения. В процессе практического обучения особое внимание уделяется формированию и развитию у обучающихся практических умений, навыков и компетенций.

Для проведения практических занятий используются методические разработки, позволяющие индивидуализировать задания обучающимся в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями объектов информатизации, и набором конкретных действий, существенных для определённых категорий обучающихся, объединённых в соответствующую подгруппу.

Институт имеет необходимый комплект лицензионного программного обеспечения и сертифицированных программных средств по защите информации. Для обучения по данной программе в институте используется специализированная лаборатория, оснащенная учебными лабораторными комплексами для обеспечения исследований специального программного обеспечения и программных средств криптографической защиты конфиденциальной информации в составе: программы симметричного и асимметричного шифрования и электронной подписи; защищённый почтовый клиент, криптопровайдер, программный комплекс для развёртывания защищённой сети организации, программное обеспечение удостоверяющего центра.

Формирование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых игр, разбора конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Реализация программы обеспечивается как штатными преподавателями специализированных кафедр Института, так и руководящими и научно-педагогическими работниками организаций и ведущих ВУЗов, а также высококвалифицированными специалистами в области информационной безопасности Управления Федеральной службы по техническому и экспортному контролю по Приволжскому федеральному округу, МВД России, Управления ФНС России по Нижегородской области, привлекаемыми к реализации программы на условиях гражданско-правового договора (контракта).

Для обеспечения учебной, учебно-методической, научной, справочной литературой, доступа к современным профессиональным базам данных, справочно-правовым системам и к глобальной сети Интернет, имеется библиотека.

ФОРМЫ АТТЕСТАЦИИ

Оценка качества освоения программы включает входной, текущий или промежуточный контроли, а также итоговую аттестацию обучающихся.

Входной контроль должен охватывать всех обучающихся и проводится в форме тестирования и последующего собеседования с ведущими преподавателями учебного заведения. Целью является определение уровня знаний обучающихся для корректировки и адаптации учебного процесса под конкретные потребности обучающихся, с учётом уровня освоения учебного

материала, изученного ими ранее в рамках получения базового образования или на курсах повышения квалификации.

Текущий контроль или промежуточный контроль предполагается проводить в форме зачётов по отдельным разделам и темам учебной программы. Для проведения промежуточного контроля разрабатываются тестовые задания, включающие вопросы по наиболее актуальным материалам, изучаемым обучающимися. Общее количество вопросов в тестах не должно превышать двадцати.

Конкретные формы и процедуры входного, текущего и промежуточного контроля знаний по каждому разделу и отдельным темам разрабатываются учебным заведением самостоятельно и доводятся до сведения обучающихся.

Итоговая аттестация обучающихся предусматривает проведение экзамена в форме тестирования.

Порядок проведения итоговой аттестации определен Положением об итоговой аттестации, утвержденным ректором Института.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается ректором Института.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Перечень вопросов, выносимых на экзамен

1. Основные понятия криптографии. Основная характеристика ключа шифрования.
2. Алгоритмы шифрования с симметричным ключом. Описание. Схема.
3. Алгоритмы шифрования с асимметричным ключом. Описание. Схема.
4. Архитектура открытых ключей PKI. Основные компоненты эффективной PKI.
5. Функции удостоверяющего центра. Основные обязанности удостоверяющего центра.
6. Электронная подпись: понятие по законодательству, способы применения.
7. Виды электронных подписей. Краткая характеристика.
8. Структура типового удостоверяющего центра.
9. Репозиторий. Основные требования к репозиторию. Центр регистрации.
10. Сертификат ключа проверки электронной подписи. Основные характеристики. Требования к сертификату.
11. Криптографические способы и средства защиты передаваемой по сетям информации: краткая характеристика.

Примеры тестовых вопросов

1. В функции центра регистрации может входить:

поддержка реестра всех изданных сертификатов
регистрация пользователей

выпуск сертификатов конечных субъектов
управление политика удостоверяющего центра

2. Корневой удостоверяющий центр в иерархической PKI действует как:

главный пункт доверия для подчиненных ему субъектов
начальный пункт связей PKI
пункт сертификации всех субъектов PKI
пункт управления сетью

3. Кросс-сертификацией называют процесс взаимного связывания:

одноранговых удостоверяющих центров
одноранговых головных удостоверяющих центров
вышестоящих и нижестоящих удостоверяющих центров
центров регистрации

4. В сетевой конфигурации PKI кросс-сертифицируются:

вышестоящие удостоверяющие центры с нижестоящими
все удостоверяющие центры
головные удостоверяющие центры
центры регистрации

Лицам, успешно освоившим дополнительную профессиональную программу повышения квалификации «Оператор удостоверяющего центра. Электронная подпись» и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

Проректор по учебной работе _____ И.В. Кожанова