ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «АКАДЕМИЯ ЛИДЕРСТВА И АДМИНИСТРИРОВАНИЯ БИЗНЕС-ПРОЦЕССОВ ФНС РОССИИ»

Утверждаю
Ректор «Академии ФНС ЛАБ»

_____ И.А. Ефремов
«26» января 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
«Эффективное взаимодействие при выдаче электронной подписи»

по повышению квалификации федеральных государственных гражданских служащих

(объем 48 часов)

Рассмотрена
на заседании кафедры
психологии профессиональной деятельности

Протокол № 1 от 03.02.2026

Рассмотрена
на заседании кафедры
информационной безопасности

Протокол № 1 от 29.01.2026

2026

Оглавление

ВВЕДЕНИЕ.....3
Цель реализации программы повышения квалификации 3
Требования к квалификации поступающего на обучение.....3
ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ 4
УЧЕБНЫЙ ПЛАН.....6
КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК.....7
РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН (МОДУЛЕЙ).....8
Криптографические методы и средства защиты. Электронная подпись. Инфраструктура открытых ключей 8
Введение.....8
Цели, задачи и место учебной дисциплины в процессе повышения квалификации 8
Планируемые результаты обучения 8
Реферативное описание тем 9
Практические задания.....10
Методические рекомендации.....10
Список литературы 11
Инфраструктура открытых ключей. Организация работы Удостоверяющего центра.12
Введение.....12
Цели, задачи и место учебной дисциплины в процессе повышения квалификации 12
Планируемые результаты обучения 13
Реферативное описание тем 14
Практические задания.....14
Методические рекомендации.....15
Список литературы 16
Психологическое обеспечение деятельности и работы с налогоплательщиками.....17
Введение.....17
Цели, задачи и место учебной дисциплины в процессе повышения квалификации 17
Планируемые результаты обучения 18
Реферативное описание тем 19
Практические задания.....20
Методические рекомендации.....22
Список литературы 23
ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ 24
ФОРМЫ АТТЕСТАЦИИ.....25
ОЦЕНОЧНЫЕ МАТЕРИАЛЫ.....26
Перечень вопросов, выносимых на экзамен.....26
Примеры тестовых вопросов 26

ВВЕДЕНИЕ

Программа повышения квалификации «Эффективное взаимодействие при выдаче электронной подписи» разработана и реализуется в соответствии со следующими нормативно-правовыми актами:

– Федеральный закон "Об образовании в Российской Федерации" от 29.12.2012 N 273-ФЗ (с изм. и доп.);

– Федеральный закон «О государственной гражданской службе Российской Федерации» от 27.07.2004 № 79-ФЗ (с изм. и доп.);

– Указ Президента Российской Федерации от 21.02.2019 № 68 «О профессиональном развитии государственных гражданских служащих Российской Федерации» (с изм. и доп.);

– Приказ Министерства науки и высшего образования Российской Федерации от 24.03.2025 N 266 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Программа реализуется в целях развития компетенции в области эффективного взаимодействия при выдаче электронной подписи.

В связи с этим цель программы повышения квалификации состоит в совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышения профессионального уровня в рамках имеющейся квалификации по вопросам управления криптографическими ключами и выдачи электронной подписи.

В рамках заявленной программы должны быть решены следующие задачи:

1. Сформировать целостное понимание правовых и криптографических основ функционирования инфраструктуры электронной подписи.

2. Отработать практические навыки работы со средствами криптографической защиты информации (СКЗИ) на всех этапах жизненного цикла сертификата.

3. Развить компетенции клиентоцентричности и эффективной деловой коммуникации при взаимодействии с налогоплательщиками.

В результате освоения данной программы слушатели обновят и углубят свои знания по вопросам управления криптографическими ключами и выдачи электронной подписи.

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:

Универсальные

- Системное и критическое мышление. Поиск, критический анализ и синтез информации, применение системного подхода для решения поставленных задач.
- Коммуникация. Деловая коммуникация в устной и письменной формах.
- Командная работа и лидерство. Социальное взаимодействие и реализация своей роли в команде.

Общепрофессиональные

- 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;

Профессиональные

- 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
- взаимодействие с налогоплательщиками и коллегами с учетом требований служебного поведения и профессиональной этики;
- реализация технологий предупреждения и урегулирования конфликтов;
- использование приемов саморегуляции и управления стрессом.

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;
– основные принципы клиентоцентричного взаимодействия с налогоплательщиками.

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, применяемые на рабочем месте оператора УЦ;
– психологически грамотно выстраивать взаимодействие с налогоплательщиками в условиях внедрения принципов человекоцентричности.

в) владеть навыками:
- работы с программными и программно-аппаратными средствами удостоверяющего центра на рабочем месте оператора УЦ;
- установки, настройки и эксплуатации средств криптографической защиты информации;
- проверки сведений, предоставляемых заявителем на ключевую информацию для использования электронной подписи;
- формирования ключевой информации с применением криптографических средств защиты информации в информационных системах;
– клиентоцентричного взаимодействия с налогоплательщиками;
– конструктивного поведения в сложных ситуациях;
– работы со стрессом.

УЧЕБНЫЙ ПЛАН

дополнительной профессиональной программы
«Эффективное взаимодействие при выдаче электронной подписи»

по повышению квалификации федеральных государственных гражданских служащих

Цель: *Совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, повышение профессионального уровня в рамках имеющейся квалификации по вопросам управления ключевой информацией и по вопросам клиентоцентричного взаимодействия с налогоплательщиками*

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

Форма обучения: *очная путем непосредственного взаимодействия педагогического работника с обучающимся с отрывом от исполнения должностных обязанностей по замещаемой должности государственной гражданской службы*

Продолжительность обучения: *48 часов*

Режим занятий: *6-8 часов в день*

№ п/п	Наименование разделов и дисциплин	Количество часов				Форма промежуточной аттестации
		Всего	по видам занятий			
			лекции	практические занятия		
				аудиторные	самостоятельная работа	
1	Криптографические методы и средства защиты. Электронная подпись. Инфраструктура открытых ключей	8	4	4	0	зачет
2	Инфраструктура открытых ключей. Организация работы Удостоверяющего центра	8	2	6	0	зачет
3	Психологическое обеспечение деятельности и работы с налогоплательщикам и	30	2	28	0	зачет
	Итоговая аттестация	2			2	экзамен в форме тестирования

	ИТОГО	**48**	**8**	**38**	**2**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Срок обучения по программе повышения квалификации, недели	1					2		
Срок обучения по программе повышения квалификации, дни	1	2	3	4	5	6	7	8
Виды занятий, предусмотренные программой повышения квалификации	А	А	А	А	А	АК	А	АИ

А- аудиторная и самостоятельная работа

И – итоговая аттестация

К – каникулы.

РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН (МОДУЛЕЙ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы и средства защиты. Электронная подпись. Инфраструктура открытых ключей

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Эффективное взаимодействие при выдаче электронной подписи».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания правовых основ законодательства РФ, а также принципов функционирования криптографических методов и средств защиты, включая электронной подписи и инфраструктуры открытых ключей, позволяющие специалисту квалифицированно 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 функционирования и использования СКЗИ.

Задачи 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 о 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.

Планируемые результаты обучения

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 использования СКЗИ;

№п/п	Наименование тем	Вид занятия
1.	Основные понятия, термины и определения криптографической защиты информации. Криптография с симметричными ключами, с открытыми ключами. Основные понятия и определения PKI	лекция
2.	Структура электронного сертификата стандарта X.509. Проверка подлинности цифровых сертификатов. Отзыв сертификатов. Списки отозванных сертификатов	лекция
3.	Средство криптографической защиты КриптоПро CSP: Назначение. Основные характеристики. Реализуемые алгоритмы. Ключевые носители. Функциональный ключевой носитель. Формирование электронной подписи. Настройка КриптоПро и КриптоАРМ	практика

Объем занятий по дисциплине – 8 часов (15% от всего объема программы).

Реферативное описание тем

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

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. Формирование электронной подписи. Настройка КриптоПро и КриптоАРМ.

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».

Создание электронной подписи. Установка и эксплуатация «КриптоАРМ».

Практические задания

1. Установите криптопровайдер КриптоПро CSP и СКЗИ КриптоАРМ.
2. Произведите настройки сертифицированных СКЗИ.
3. Создайте запрос на сертификат открытого ключа с использованием криптоалгоритма ГОСТ Р 34.10-2012.
4. Отправьте запрос на сертификат в удостоверяющий центр.
5. Получите от удостоверяющего центра необходимые сертификаты.
6. Установите сертификаты в СКЗИ.
7. С помощью программного СКЗИ КриптоАРМ исследуйте возможности по шифрованию файлов и электронной подписи.
8. С помощью программных СКЗИ сформируйте ключевую информацию и запрос на сертификат. Получите сертификат открытого ключа от Удостоверяющего центра.
9. Настройка криптосистемы и использование программных СКЗИ.

Методические рекомендации

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

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 от НСД на объекте защиты, особенности подготовки локальных актов, регламентирующих использование средств защиты информации, а также, практические аспекты защиты информации с использованием отечественного программного обучения.

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.

С целью определения качества усвоения материала проводится проверка знаний слушателей с использованием совокупности контрольных заданий и вопросов в виде текущего и итогового контроля.

Текущий контроль осуществляется на лекциях в самых разнообразных формах – опроса слушателей по изученным вопросам, диалога с преподавателем во время лекций, промежуточного тестирования, выполнения слушателями индивидуальных заданий по темам изучаемой дисциплины.

Список литературы

а) основная литература:

1. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. 7-е изд. Н.Г. Лабутин, О.И. Климченков. – Н.

Новгород: Приволжский ин-т повышения квалификации ФНС, 2024. – 106 с.

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

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

4. 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. 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.

2. 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.

3. Концепция информационной безопасности Федеральной налоговой службы (утверждена приказом Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6@)

4. Концепция системы управления информационной безопасностью ФНС России (утверждена приказом Федеральной налоговой службы от 25 февраля 2014 г. № ММВ-7-6/66@).

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Инфраструктура открытых ключей. Организация работы Удостоверяющего центра

Введение

Рабочая программа дисциплины разработана для программы повышения квалификации «Эффективное взаимодействие при выдаче электронной подписи».

В результате освоения данной дисциплины государственные гражданские служащие инспекций и управлений ФНС России совершенствуют свои знания по работе удостоверяющего центра ФНС России и приобретают практические навыки использования инструментов инфраструктуры открытых ключей.

Цели, задачи и место учебной дисциплины в процессе повышения квалификации

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.

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.

Планируемые результаты обучения

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

№п/п	Наименование тем	Вид занятия
1.	Законодательство РФ об организации работы УЦ. Требования к УЦ. Организация рабочего места оператора	лекция
2.	Организация работы УЦ: регламент, обязанности	практика
3.	Управление криптографическими ключами. Использование программного обеспечения для работы с УЦ	практика

Объем занятий по дисциплине – 8 часов (16,7% от всего объема программы).

Реферативное описание тем

Тема № 1. Законодательство РФ об организации работы УЦ. Требования к УЦ. Организация рабочего места оператора.

Положения Федерального закона РФ №63 по организации работы УЦ. Уполномоченный орган в сфере электронной подписи. Понятие удостоверяющего центра (УЦ). Статус и функции УЦ. Аккредитация УЦ.

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

Тема №2. Организация работы УЦ: регламент, обязанности.

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.

Порядок реализации Федеральной налоговой службой функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утверждённый приказом ФНС России от 30.12.2020 г. N ВД-7-24/982@ с изменениями и дополнениями от 11 августа 2023 г.

Тема №3. Управление криптографическими ключами. Использование программного обеспечения для работы с УЦ.

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.

Работа оператора УЦ с Единой цифровой платформой УЦ ФНС России.

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.
7. Установите СКЗИ КриптоПро CSP и КриптоАРМ на виртуальную машину с ОС Astra Linux.
8. С помощью КриптоАРМ сформируйте запрос на сертификат к удостоверяющему центру КриптоПро, развёрнутому в виртуальной сети по адресу 10.0.1.250. Получите от него сертификат своего открытого ключа, сертификат корневого удостоверяющего центра, список отозванных сертификатов (CRL); установите их в Криптопро CSP на своей рабочей станции.
9. Создайте документ произвольного содержания. С помощью программы КриптоАРМ подпишите этот документ своим сертификатом (закрытым ключом), сохраните его в виде файла.
10. Проверьте с помощью КриптоАРМ подпись на полученном документе и извлеките из подписанного файла исходный документ.
11. Создайте документ произвольного содержания. С помощью программы КриптоАРМ зашифруйте его сертификатом коллеги по группе. Зашифрованный файл отправьте в коллеге.

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций, практических занятий и лабораторных работ. При проведении лекций обязательно наличие презентации и использование мультимедийной техники.

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 от НСД на объекте защиты, особенности подготовки локальных актов, регламентирующих использование средств защиты информации, а также, практические аспекты защиты информации с использованием отечественного программного обучения.

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.

С целью определения качества усвоения материала проводится проверка знаний слушателей с использованием совокупности контрольных заданий и вопросов в виде текущего и итогового контроля.

Текущий контроль осуществляется на занятиях в самых разнообразных формах – опроса слушателей по изученным вопросам, диалога с преподавателем во время лекций, промежуточного тестирования, выполнения слушателями индивидуальных заданий по темам изучаемой дисциплины.

При проведении практических занятий и лабораторных работ рекомендовано использование лицензионного программного обеспечения.

Список литературы

а) основная литература:

1. Информационная безопасность в таблицах и схемах: учебно-методическое пособие. Н.Г. Лабутин, О.И. Климченков. Часть 1, 7-е изд. – Н. Новгород: «Академия ФНС ЛАБ-Волга», 2025. – 106 с.

1. Криптографические методы и средства защиты информации. Учебник СПО / А.В. Бабаш, Е.К. Баранова, М.: Кнорус, 2024. – 224 с.

2. Криптографические методы и средства защиты информации: Учебное пособие / Н.Г. Бутакова, Н.В. Федоров. – СПб.: ИЦ «Интермедиа», 2023. – 384 с.

3. Васильева, И.Н. Криптографические методы защиты информации: учебник и практикум для вузов / И.Н. Васильева. — Москва: Издательство Юрайт, 2024. — 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».

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Психологическое обеспечение деятельности и работы с налогоплательщиками

Введение

Налоговая деятельность протекает в области общественных отношений и отличается разнообразием решаемых задач и особенностью труда: напряженной многочасовой деятельностью при дефиците времени на обдумывание адекватных действий, работой с большими объемами информации, необходимостью быстрого переключения с одной проблемы на другую, несовпадением интересов с партнерами по деловому взаимодействию. Работа сотрудников структурного подразделения налогового органа, непосредственно взаимодействующих с налогоплательщиками, связана с решением возникающих проблем у налогоплательщиков всех категорий. Это требует от налогового инспектора профессиональных знаний не только в области налогообложения, но и психологии. Высокий уровень развития психологической и конфликтологической компетентности позволит сотруднику эффективно организовать взаимодействие с налогоплательщиками.

Цели, задачи и место учебной дисциплины в процессе повышения квалификации

Цель изучения данной дисциплины состоит в формировании новых и развитии ранее приобретенных профессиональных компетенций государственных гражданских служащих налоговых органов в части знаний закономерностей эффективного взаимодействия с налогоплательщиками, изучении психологических механизмов повышения эффективности их профессиональной деятельности.

В рамках заявленной темы должны быть решены следующие ***задачи***:

1) создание условий для трансформации учебно-познавательной деятельности слушателей в профессиональную деятельность служащих налоговых органов;

2) дополнение имеющихся базовых знаний по основным направлениям психологического обеспечения деятельности сотрудников налоговых органов и работы с налогоплательщиками, их закрепление, обобщение и систематизация;

3) обучение психологическому анализу сложных ситуаций взаимодействия.

В связи с тем, что структурные преобразования вносят значительные изменения в характер труда, предъявляя к сотрудникам, непосредственно взаимодействующих с налогоплательщиками, более высокие требования, увеличивая экономическую и социальную значимость результатов их деятельности, дисциплина «Психологическое обеспечение деятельности и работы с налогоплательщиками» занимает важное место в процессе обновления и закрепления профессиональных знаний, умений и навыков.

Планируемые результаты обучения

В результате освоения данной дисциплины государственный гражданский служащий должен

знать:

- закономерности и технологии эффективного взаимодействия с налогоплательщиками;
- приемы разрешения конфликтных ситуаций;
- виды и приемы психологического влияния;
- методы и приемы саморегуляции;

уметь:

- применять психологические знания для обеспечения эффективного взаимодействия с налогоплательщиками;
- применять основные закономерности клиентоцентричного поведения и делового общения в практике взаимодействия с налогоплательщиками;
- использовать приемы профилактики конфликта;
- использовать приемы влияния и защиты от манипуляций;
- анализировать и прогнозировать поведение человека на основе знаний типологии личности и профайлинга;

владеть навыками:

- делового общения и клиентоцентричного взаимодействия при личном приеме налогоплательщиков;
- установления контакта с налогоплательщиками, передачи информации эффективного слушания, аргументации и контраргументации;
- разрешения конфликта;
- убеждающего воздействия;

- управления стрессом.

№п/п	Наименование тем	Вид занятия
3.1	Тренинг-знакомство. Отработка навыков социальной коммуникации	практика
3.2	Традиционные российские духовно-нравственные ценности. Ценности человекоцентричности как основа внешних и внутренних коммуникаций	лекция
3.3	Тренинг развития компетенций клиентоцентричности	практика
3.4	Тренинг эффективного взаимодействия с налогоплательщиками	практика
3.5	Тренинг разрешения конфликтных ситуаций	практика
3.6	Профайлинг в работе налогового инспектора	практика
3.7	Психология влияния и противодействие манипуляциям (тренинг)	практика
3.8	Профилактика профессионального стресса и выгорания сотрудников	практика

Общий объем времени, отводимого на освоение учебной дисциплины, составляет 30 часов (62,5% от всего объёма программы).

Реферативное описание тем

3.1. Тренинг-знакомство. Отработка навыков социальной коммуникации

Знакомство. Социальная коммуникация, ее виды. Этапы делового общения и социальной коммуникации. Установление контакта: закономерности и приемы. Вербальное и невербальное общения. Барьеры в деловом общении. Деловая беседа, как основной вид делового общения. Этапы беседы. Отработка навыков социальной коммуникации.

3.2. Традиционные российские духовно-нравственные ценности. Ценности человекоцентричности как основа внешних и внутренних коммуникаций

Основные понятия и нормативная база. Ценности в профессиональной деятельности государственного гражданского служащего. Понятие и принципы человекоцентричности. Ценности человекоцентричности и их отражение в Декларации человекоцентричности и Манифесте ФНС России. Культура деловых коммуникаций и эмпатия. Технологии эффективной коммуникации при взаимодействии с сотрудниками и пользователями услуг.

3.3. Тренинг развития компетенций клиентоцентричности

Компетенция эффективной клиентоцентричности. Отработка приемов установления контакта с налогоплательщиком. Приемы снятия психоэмоционального напряжения. Овладение навыками эффективного

слушания. Навыки получения и передачи обратной связи. Вопросы налогоплательщика и ответы на них.

3.4. Тренинг эффективного взаимодействия с налогоплательщиками

Проблемы в организации эффективного взаимодействия с налогоплательщиками. Совершенствование стратегий клиентоцентричного поведения при взаимодействии. Развитие навыков коммуникации и эмпатии в процессе взаимодействия с налогоплательщиками.

3.5. Тренинг разрешения конфликтных ситуаций

Технологии управления конфликтами на государственной гражданской службе. Анализ и прогнозирование поведения налогоплательщиков. Овладение навыками эффективного поведения в конфликтной ситуации. Взаимодействие с конфликтными личностями. Развитие навыков разрешения конфликтных ситуаций.

3.6. Профайлинг в работе налогового инспектора

Психологические методы оценки и прогнозирования поведения человека. Невербальное поведение как индикатор личности. Речь как характеристика личности. Ведущая репрезентативная система и эффективное взаимодействие. Психотипы личности: диагностика и особенности коммуникации с налогоплательщиками.

3.7. Психология влияния и противодействие манипуляциям (тренинг)

Понятие и виды психологического влияния. Эффективные и неэффективные психологические приемы влияния на собеседника. Психотехнологии убеждающего воздействия. Отработка правил убеждения. Психологические приемы противодействия манипуляциям.

3.8. Профилактика профессионального стресса и выгорания сотрудников

Стресс и профессиональное выгорание: понятие и симптомы. Причины профессионального стресса и выгорания. Индивидуальные методы профилактики профессионального стресса и профессионального выгорания. Занятие в комнате психологической разгрузки.

Практические задания

Задание 1.

Ответьте на следующий вопрос: Какие приемы помогают мне создать первое впечатление и установить контакт с партнером по общению? Что мешает создать положительное впечатление и установить контакт?

Заполните таблицу:

Как произвести впечатление	
Положительное	*Отрицательное*

Задание 2.

Опишите, какие проблемы возникают у вас при взаимодействии с налогоплательщиками при выдаче электронной подписи. Определите докладчика. Регламент выступления 5 минут.

Поразмышляйте о том, как можно решить проблему взаимодействия «налогоплательщик-налоговый инспектор».

Задание 3.

Приведите примеры оценочных фраз, которые могут вызвать непонимание и желание защититься. Определите докладчика. Регламент выступления 3 минуты.

Во время выступлений групп отмечайте для себя (мысленно или письменно) то, что пополнит вашу личную «копилку» *неэффективных* оценочных фраз, которые лучше не использовать при общении с налогоплательщиком.

Задание 4.

В налоговую инспекцию пришел агрессивно настроенный налогоплательщик. На предложение сотрудника инспекции присесть, он ответил отказом и остался стоять, возвышаясь над ним. На повышенных тонах он начал выговаривать налоговому инспектору: «Я не намерен предоставлять Вам свою электронную подпись, я не собираюсь ее использовать в электронном виде, хочу подписывать документы только лично, без этого Вашего интернета, там одни мошенники?». Опишите психологически грамотные действия налогового инспектора в данной конфликтной ситуации с применением приемов снижения напряжения.

Задание 5.

При завершении контакта с налогоплательщиком рекомендуется сделать ему комплимент. 1. Приведите примеры комплиментов, которые можно использовать при взаимодействии с налогоплательщиком. 2. Приведите примеры комплиментов, которые нельзя использовать при общении с налогоплательщиком.

Задание 6.

Приведите 3 примера использования приемов манипулирования в ситуациях взаимодействия налогового инспектора с налогоплательщиком. Опишите способы защиты в данных ситуациях.

Методические рекомендации

Занятия по дисциплине проводятся в форме лекций и практических занятий.

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 контроля состояния технической защиты конфиденциальной информации на объекте защиты, особенности подготовки локальных актов, регламентирующих проведения контроля состояния технической защиты конфиденциальной информации.

Все занятия по данной дисциплине – лекционные и практические, 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.

С целью определения качества усвоения материала проводится проверка знаний слушателей с использованием совокупности контрольных заданий и вопросов в виде текущего и итогового контроля.

Текущий контроль осуществляется на занятиях в самых разнообразных формах – опроса слушателей по изученным вопросам, диалога с преподавателем во время лекций, промежуточного тестирования, выполнения слушателями индивидуальных заданий по темам изучаемой дисциплины.

При выполнении практических заданий рекомендуется применять лицензионное программное обеспечение.

Список литературы

1. Агаева, А.Ш. Деловая культура и психология общения: учебное пособие / А.Ш. Агаева; Ш.А. Идрисов. - М.: Инфра-Инженерия, 2022. - 232 с.

2. Биркенбиль, В. Тренинг уверенного общения. 56 упражнений, которые по-могут прокачать навыки коммуникации / В. Биркенбиль. - М.: ЭКСМО, 2022.- 288 с.

3. Воронина, Н.А. Взаимодействие с налогоплательщиками. Секреты эффективности: учебно-методическое пособие/ Н.А. Воронина; О.И. Суховеева; А.Ш. Широкова. - Н. Новгород, 2025. - 64 с.

4. Воронина Н.А. От стресса и выгорания к балансу: эффективные стратегии самопомощи: учебно-методическое пособие/ Н.А. Воронина; Н.А. Зимина, И.В. Кожанова. - Н. Новгород, 2025. - 60 с.

5. Каришина, И. Е. Тайм-менеджмент для всех. Секреты управления временем. Целеполагание: учебное пособие / И.Е. Каришина. - Н. Новгород: Академия ФНС ЛАБ- Волга, 2025. - 50 с.

6. Кожанова, И. В. Секреты эффективного делового общения: учебное пособие / И.В. Кожанова; А.Ш. Широкова. - Н. Новгород, 2025. - 56 с.

7. Кроль, Л. Жизнь без выгорания: Как сохранить устойчивость и позаботиться о себе / Л. Кроль. - М.: Альпина Паблишер, 2023. - 224 с.

8. Майорова, М. И. Сценарии конфликтов: Как без нервов улаживать споры и проблемы на работе и в жизни/ М.И. Майорова. - М.: Альпина Паблишер, 2021. - 139 с.

9. Мартьянова, Л.М. Профайлинг в действии. Характеристика собеседника за 10 минут / Л.М. Мартьянова. - М.: АСТ, 2023. - 256 с.

10. Резанова, Е. Работа, которая заряжает. Как не выгореть, занимаясь любимым делом/ Е. Резанова. - М.: Манн, Иванов и Фербер, 2022. - 240 с.

11. Рызов, И.Р. Психотрюки: 69 приемов в общении, которым не учат в школе / И.Р. Рызов. - М.: ЭКСМО, 2023. - 256 с.

12. Саймон, Дж. К. Манипулятор в овечьей шкуре: как не стать жертвой его уловок / Дж. К. Саймон. - М.: ЭКСМО, 2020. - 208 с.

13. Фесенко, О.П. Практикум по конфликтологии, или Учимся разрешать конфликты / О.П. Фесенко; соавт. С.В. Колесникова. - 3-е изд., стер. - М.: Флинта, 2018. - 128 с.

14. Шейнов, В. П. Как убедить, когда вас не слышат/ В.П. Шейнов. - СПб.: Питер, 2021. - 352 с.

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Повышение квалификации гражданских служащих осуществляется в очной форме путем непосредственного общения слушателя с преподавателем. В содержании обучения приоритет отдается практической направленности обучения.

При проведении занятий обязательно учитывается распределение времени на лекционный материал и выполнение практических занятий в соответствии с утвержденным учебно-тематическим планом.

Программа повышения квалификации предусматривает проведение занятий в соответствии с целевыми установками программы, которые обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются в основном проведением лекций, практических занятий и самостоятельной работы. Умения и навыки достигаются проведением ряда взаимосвязанных практических занятий, деловых и ролевых игр, разбором конкретных ситуаций, тренингов и др.

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий. Часть лекций может излагаться проблемным методом с привлечением слушателей для решения сформулированных преподавателем проблем.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматривать задания с проведением деловых игр (эпизодов) и созданием ситуаций, моделирующих типовые нарушения.

Для проведения практических занятий должны использоваться методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями информационных систем, и набором конкретных действий, существенных для определённых категорий обучаемых, объединённых в соответствующую подгруппу.

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

Учебная база Академии оснащена современными техническими средствами для обеспечения учебного процесса. Лекции и практические занятия проводятся в аудиториях, оснащенных компьютером, мультимедийным проектором, экраном и доской.

Компьютерные классы оборудованы автоматизированными рабочими местами для проведения занятий по учебным дисциплинам из расчёта одно рабочее место на одного обучающегося при проведении занятий в данных классах.

Для обеспечения учебной, учебно-методической, научной, справочной литературой, доступа к современным профессиональным базам данных, справочно-правовым системам и к глобальной сети Интернет, имеется библиотека. Каждому обучающемуся обеспечивается доступ к библиотечному фонду, укомплектованному печатными и электронными изданиями основной учебной литературы, изданными за последние 10 лет, из расчёта не менее одного экземпляра на 4-5 обучающихся.

Реализация программы обеспечивается как штатными преподавателями специализированных кафедр Академии, так и научно-педагогическими работниками организаций и ведущих ВУЗов, привлекаемыми к реализации программы на условиях гражданско-правового договора (контракта).

ФОРМЫ АТТЕСТАЦИИ

Оценка качества освоения программы включает входной, текущий или промежуточный контроль, 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 Академии.

Перечень вопросов, используемых для проведения экзамена, формируется на основе перечня основных вопросов (тестов), составляемых для контроля знаний обучающихся, при проведении промежуточного контроля знаний по учебным дисциплинам (модулям), представленных в рабочей программе повышения квалификации.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Перечень вопросов, выносимых на экзамен

Перечень основных вопросов, выносимых для контроля знаний, обучающихся по итогам изучения учебного курса:

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.
12. Назначение и структура УЦ ФНС России.
13. Роль и место оператора УЦ в структуре УЦ ФНС России.
14. Законодательное регулирование деятельности УЦ.
15. Порядок осуществления функций аккредитованного удостоверяющего центра УЦ ФНС России.
16. Основные задачи, обязанности и полномочия Оператора УЦ.
17. Порядок выполнения действий оператора УЦ по формированию и выдаче ключевых документов заявителям с использованием ЕЦП.
18. Традиционные российские духовно-нравственные ценности. Ценности человекоцентричности как основа внешних и внутренних коммуникаций.
19. Социальная коммуникация и ее виды.
20. Приемы организации эффективного взаимодействия с налогоплательщиками.
21. Принципы клиентоцентричной коммуникации.
22. Разрешение конфликтных ситуаций.
23. Развитие стрессоустойчивости и профилактика профессионального выгорания.

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

5. **С чего начинается психологическая культура обслуживания клиента?**
   - с подробного, четкого и эмоционального описания предоставляемой услуги
   - с прояснения цели пребывания клиента на территории инспекции
   - с доброжелательного приема
   - с создания благоприятного психологического климата и установления контакта

6. **Что необходимо делать сотруднику при первоначальном этапе работы с налогоплательщиком – установлении контакта?**
   - положительно отозваться о клиенте
   - выяснить цель пребывания клиента на территории инспекции

- расспросить о проблемах, возникающих при оформлении налоговой отчетности
- прокомментировать поведение клиента

7. Приятные слова и выражения, содержащие одобрение действий собеседника и подчеркивающие его положительные качества, это:

- комплимент
- лесть
- похвала
- критика

8. Психологически грамотным является следующий комплимент в отношении налогоплательщика:

- Вы прекрасно выглядите сегодня
- у Вас очень красивая сумочка, сразу видно не дешевая
- как приятно видеть человека, ответственно относящегося к оформлению документации
- Вы очень пунктуальны, не то, что мужчина, который был перед Вами

9. Наибольшее отрицательное влияние на взаимодействие с налогоплательщиком оказывает:

- отсутствие рукопожатия при приветствии
- безразличный тон или раздражение в голосе
- случайная оговорка, неправильное ударение
- неожиданный звонок мобильного телефона

10. Выберите наиболее эффективное приветствие сотрудником налогоплательщика для быстрого установления контакта:

- «Здравствуйте, Иван Петрович»
- «Добрый день»
- «Приветствую Вас»
- «Внимательно слушаю»

11. Действия сотрудника при первоначальном этапе работы с налогоплательщиком – установлении контакта

- доброжелательно поприветствовать, представиться
- при помощи наводящих вопросов убедиться, что именно Вы можете помочь налогоплательщику, а не другой специалист
- расспросить о проблемах, возникающих при оформлении налоговой отчетности
- четко указать на ошибки и исправить их

12. Если налогоплательщик начинает с Вами спорить, эффективной будет фраза

- «Вы ошибаетесь, на самом деле все обстоит не так»
- «Не нужно со мной спорить, я представитель власти»
- «Вы знаете, у меня другая информация, но возможно я ошибаюсь. Давайте лучше вместе проверим факты»
- «Успокойтесь, не нужно нервничать»

Лицам, успешно освоившим дополнительную профессиональную программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

Проректор по научному и инновационному развитию Е.А. Хицков