АНО ДПО «Учебный центр «Парадигма»
ИНН 7604200936 / КПП 760601001
ОГРН 1117600002178

**Автономная некоммерческая организация дополнительного профессионального образования
"Учебный центр "Парадигма"**

**«УТВЕРЖДАЮ»
Исполнительный директор
АНО ДПО "Учебный центр "Парадигма"**
Гребенкина А.В. _____
«11» мая 2022 г.

Дополнительная профессиональная программа,
программа повышения квалификации

«Электронная подпись. Организационно-правовые вопросы использования»

Трудоемкость - 44 часа
Форма обучения – заочная, с применением дистанционных образовательных технологий
Дополнительное профессиональное образование – повышение квалификации *«Электронная подпись. Организационно-правовые вопросы использования»*

Ярославль
2022 год

1. Общая характеристика программы

1.1. Общие положения

Настоящая дополнительная программа повышения квалификации «Электронная подпись. Организационно-правовые вопросы использования» (далее - Программа) разработана на основании Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», приказа Минобрнауки России от 5 декабря 2013 года № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности», приказа Минобрнауки России от 01.07.2013 года № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

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

1.2. Цели реализации программы

Целью реализации программы является:

- сформировать у слушателей профессиональные компетенции в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий;
- сформировать у слушателей профессиональные компетенции, необходимые для профессиональной деятельности в области обеспечения информационной безопасности на объектах информатизации;
- раскрыть основы правового регулирования отношений в области создания и применения электронной подписи;
- обеспечить освоение слушателями принципов использования электронной подписи и функций по созданию и выдаче квалифицированных сертификатов ключей проверки электронной подписи;
- обеспечить освоение правил безопасности в области защиты информации, персональных данных и электронных подписей.

В рамках данной программы рассматриваются основные принципы и правила выпуска электронной подписи и ее применения.

1.3. Категории слушателей

Программа предназначена для руководителей и специалистов структурных подразделений органов государственной власти, органов местного самоуправления, предприятий, учреждений и организаций, занимающихся вопросами формирования и применения квалифицированных сертификатов ключей проверки электронной подписи (далее - СКПЭП).

1.4. Планируемые результаты обучения

Слушатель, успешно освоивший Программу, должен

- Знать:
  основные законодательные акты, регламентирующие выпуск и применение квалифицированных СКПЭП;
  возможные угрозы безопасности информации при работе с персональными

данными;
порядок оформления и выдачи квалифицированных СКПЭП;
ответственность за нарушение деятельности Удостоверяющего центра;

- Уметь:
  определять сферы применения квалифицированных СКПЭП;
  защищать коммерческую, служебную, профессиональную тайну;
- Владеть:
  навыками определения порядка работы Удостоверяющего центра.

Все знания, умения и навыки, полученные в процессе обучения слушатель может применять в своей дальнейшей профессиональной деятельности.

1.5. Трудоемкость программы

Нормативная трудоемкость обучения по программе повышения квалификации – 44 часа.

1.6. Форма и сроки обучения

Обучение по Программе осуществляется в заочной форме (без отрыва от работы) с использованием дистанционных образовательных технологий.

Общая продолжительность обучения – 2 недели.

1.7. Режим занятий

Нагрузка устанавливается не более 24 часов в неделю.

Для занятий устанавливается академический час продолжительностью 45 минут.

2. Содержание программы

2.1. Тематический план учебной дисциплины

№ п/п	Наименование учебного модуля	Всего учебных (академ.) часов
1.	Введение: основные понятия и определения	6
2.	Электронная подпись	6
3.	Правовая основа деятельности Удостоверяющего центра, принципы и требования	7
4.	Работа с электронной подписью и обязанности Удостоверяющего центра	7
5.	Средства электронной подписи УЦ	6
6.	Риски и ответственность	6
7.	Доверенная третья сторона и «облака»	4
8.	Итоговая аттестация	2
	Итого:	**44**

Доступ слушателей к порталу Учебного центра, на котором расположена учебная программа в формате электронного обучения, осуществляется слушателями круглосуточно за исключением времени регламентных (профилактических) работ.

Обучение проводится по мере формирования групп, в установленные Учебным центром сроки.

2.2. Рабочая программа учебной дисциплины

Модуль 1. Введение: основные понятия и определения

Основные понятия и определения информационной безопасности.

Понятие угрозы безопасности информации. Виды угроз.

Защита персональных данных в РФ.

Защита коммерческой тайны в РФ.

Защита профессиональной и служебной тайны в РФ.

Модуль 2. Электронная подпись

Стандарт цифровой подписи ГОСТ Р 34.10-2012.

Правовая основа использования электронной подписи.

Электронная подпись. Общие понятия. Виды электронных подписей.

Сферы применения электронных подписей.

Электронные документы. Угрозы безопасности субъектам электронного документооборота.

Модуль 3. Правовая основа деятельности Удостоверяющего центра, принципы и требования

Удостоверяющий центр. Правовая основа деятельности, принципы и требования.

Федеральный государственный надзор в сфере электронной подписи.

Требования к аккредитации Удостоверяющего центра.

Требования к квалификации сотрудников Удостоверяющего центра.

Модуль 4. Работа с электронной подписью и обязанности Удостоверяющего центра

Порядок оформления и выдачи квалифицированного сертификата.

Признание электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами.

Способы идентификации заявителя при выдаче квалифицированного сертификата.

Порядок ознакомления с информацией, содержащейся в квалифицированном сертификате.

Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей.

Обязанности Удостоверяющего центра при обращении заявителя за получением квалифицированного сертификата.

Обязанности Удостоверяющего центра при выдаче квалифицированного сертификата.

Основания прекращения действия электронной подписи и аннулирования квалифицированных СКПЭП.

Модуль 5. Средства электронной подписи УЦ

Порядок выдачи квалифицированного сертификата.

Средства электронной подписи Удостоверяющего центра.

Порядок аннулирования СКПЭП.

Формирование реестров выданных и аннулированных СКПЭП.

Регистрация в ЕСИА.

Модуль 6. Риски и ответственность

Условия и требования для получения аккредитации Удостоверяющим центром.

Регламент Удостоверяющего центра.

Риски процедуры выдачи электронной подписи.

Мошеннические действия при оформлении электронной подписи.

Ответственность за нарушение деятельности Удостоверяющего центра.

Модуль 7. Доверенная третья сторона и «облака»

Доверенная третья сторона

Аккредитация для осуществления хранения ключа электронной подписи.

Порядок хранения и использования ключа электронной подписи по поручению владельца квалифицированного сертификата.

Итоговая аттестация

3. Условия реализации программы, организационно-педагогические условия

3.1. Требования к уровню подготовки поступающего на обучение

Лица, желающие освоить программу повышения квалификации, должны иметь высшее, средне-специальное или средне-техническое образование. Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

3.2. Требования к кадровым условиям реализации программы

Реализация программы обеспечивается руководящими и научно-педагогическими работниками организации, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора. Все научно-педагогические работники, участвующие в реализации программы, должны иметь образование, соответствующее профилю преподаваемой дисциплины (модуля), конкретный опыт реализации научно-прикладных разработок или иной формы практической деятельности в области обеспечения информационной безопасности на объектах информатизации.

Слушателям предоставляется возможность копирования материала для самоподготовки и подготовки к зачету.

3.3. Требования к материально-техническим условиям реализации программы

Каждый Слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (электронной библиотеке), содержащей обязательные и дополнительные издания учебной, учебно-методической и иной литературы. Перечисленной в рабочих программах дисциплин (модулей), с выполнением установленных требований по защите информации.

Библиотечный фонд Учебного центра укомплектован печатными изданиями. Фонд дополнительной литературы включает официальные, справочно-библиографические и специализированные отечественные и зарубежные периодические издания, в том числе, правовые нормативные акты и нормативные методические документы в области информационной безопасности.

Каждый слушатель может воспользоваться учебно-методическими материалами, помогающими организовать его самостоятельную работу при подготовке к итоговой аттестации. Все материалы доступны слушателям на электронных носителях.

4. Форма аттестации. Оценочные материалы

Оценка качества освоения слушателями программы повышения квалификации включает

итоговую аттестацию в форме экзамена. Итоговая аттестация проводится в форме электронного тестирования на портале Учебного центра.

Итоговая аттестация организуется и проводится в соответствии с «Положением об итоговой аттестации АНО ДПО «Учебный центр «Парадигма».

4.1 Критерии оценки

Оценка	Предмет оценки
Отлично 86-100 баллов.	86-100 баллов. Есть ответы на все вопросы. Допущены незначительные ошибки.
Хорошо 70-85 баллов.	70-85 баллов. Правильные ответы даны на более, чем 70% вопросов, но менее 86%.
Удовлетворительно 51-69 баллов.	Правильные ответы даны на более, чем 50% вопросов, но менее 70%
Неудовлетворительно 50 и менее баллов.	Менее 50% правильных ответов.

5. Нормативно-правовая база и Постановления Правительства Российской Федерации

5.1. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (в ред. от 08.06.2020) (с изм. и доп.., вступ. в силу с 01.07.2020);

5.2. Разъяснения регулятора Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации в части применения электронной подписи при оказании электронных услуг для граждан и бизнеса;

5.3. Федеральный закон от 27.12.2019 (в ред. 23.06.2020) № 476-ФЗ "О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля";

5.4. Приказ ФСБ РФ от 27.12.2011 № 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи";

5.5. Приказ Минкомсвязи России № 486 от 30.11.2015 «Об утверждении административных регламентов предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и исполнения Министерством связи и массовых коммуникаций Российской Федерации государственной функции по осуществлению государственного контроля и надзора за соблюдением аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом “Об электронной подписи” и на соответствие которым эти удостоверяющие центры были аккредитованы»;

5.6. Приказ ФАПСИ от 13.06.2001 № 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";

5.7. Федеральный закон от 27.07.2006 (ред. от 24.04.2020) № 152-ФЗ "О персональных

данных";

5.8. Типовой регламент КриптоПро;

5.9. Приказ Минкомсвязи России от 13.08.2018 № 397 "Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей";

5.10. Проект Приказа «Об утверждении Требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей»;

5.11. Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 № 195-ФЗ (ред. от 31.07.2020) (с изм. и доп., вступ. в силу с 11.08.2020);

5.12. Постановление Правительства РФ от 16.04.2012 (ред. от 10.07.2020) № 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)".