Правила организации работы

оператора первичного ввода заявлений на выпуск квалифицированных сертификатов и карт тахографов в ИС СПДн ИЗКТ

22.09.2022

СПРАВОЧНИК ТЕРМИНОВ

КТ – карта тахографа

КСЭП – квалифицированный сертификат ключа проверки ЭП

КиКСЭП – ключи электронной подписи и квалифицированный сертификат ключа проверки ЭП

ЭП – электронная подпись

СЗИ – средства защиты информации

ФЗ – Федеральный закон

ФСТЭК - Федеральная служба по техническому и экспортному контролю

ПО – программное обеспечение

ОС – операционная система

ПВК – пункт оформления заявлений на КТ и КиКСЭП, а также выдачи КТ с записанными на них КиКСЭП

СПРАВОЧНИК ТЕРМИНОВ

ИС – информационная система

СПДн – сбор персональных данных

ИЗКТ – ИС СПДн «Интерфейс заказов карт тахографа»

УЦ – удостоверяющий центр, выпускающий КиКСЭП для использования в картах тахографа и НКМ

ОИ – организация-изготовитель карт тахографа

АРМ – автоматизированное рабочее место

ПДн – персональные данные

Заявитель – заявитель на выпуск КТ, КиКСЭП, активизацию НКМ и КСЭП или представитель заявителя, чей сертификат будет использоваться в КТ или НКМ

Оператор ПВД – оператор первичного ввода данных

Оператор ПДн – организация, которая занимается обработкой персональных данных в информационной системе

НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

Федеральный закон от 10.12.1995 N 196-ФЗ (ред. от 02.07.2021) "О безопасности дорожного движения" (с изм. и доп., вступ. в силу с 22.08.2021) - https://legalacts.ru/doc/federalnyi-zakon-ot-10121995-n-196-fz-o/

Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) "О персональных данных" - https://legalacts.ru/doc/152_FZ-o-personalnyh-dannyh/

Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 11.06.2021) "Об электронной подписи" - https://legalacts.ru/doc/FZ-ob-jelektronnoj-podpisi/

Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации " - https://legalacts.ru/doc/FZ-ob-informacii-informacionnyh-tehnologijah-i-o-zawite-informacii/

НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

Приказ Минтранса России от 28.10.2020 N 440 "Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства« - https://legalacts.ru/doc/prikaz-mintransa-rossii-ot-28102020-n-440-ob-utverzhdenii/

Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" – https://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-01112012-n-1119

НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

Приказ Минкомсвязи России от 21.01.2019 N 10 "Об утверждении Программы профилактики нарушений обязательных требований, которые установлены Федеральным законом "Об электронной подписи", на 2019 год" - https://legalacts.ru/doc/prikaz-minkomsvjazi-rossii-ot-21012019-n-10-ob-utverzhdenii/

Приказ ФАПСИ от 13.06.2001 N 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» - https://legalacts.ru/doc/prikaz-fapsi-ot-13062001-n-152-ob/

НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера" - https://legalacts.ru/doc/ukaz-prezidenta-rf-ot-06031997-n-188/

Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» - https://legalacts.ru/doc/prikaz-fstek-rossii-ot-18022013-n-21/

Требования действующего законодательства к организациям, осуществляющим деятельность по приёму заявлений на выпуск и выдачу КиКСЭП и КТ, и активизации НКМ

ТРЕБОВАНИЯ К ПВК

Организации, занимающиеся приёмом документов на выпуск КиКСЭП и КТ, а также выдачу КТ с записанными на них КиКСЭП (ПВК) для выполнения работ должны:

- Соответствовать требованиям к Операторам ПДн.
- Иметь лицензию на работу с СКЗИ с соответствующими разрешёнными видами деятельности (в случае осуществления выдачи КТ).
- Быть действующим доверенным лицом УЦ.
- Иметь действующий агентский договор.
- Для организации информационного обмена с УЦ и ОИ у ПВК иметь действующую лицензию на ИЗКТ, а также подключение к ИЗКТ через защищённую сеть.

ТРЕБОВАНИЯ К МАСТЕРСКИМ

Для выполнения работ по активизации блоков СКЗИ тахографа организация (Мастерская) должна:

- Соответствовать требованиям к Операторам ПДн.
- Иметь лицензию на работу с СКЗИ с соответствующими разрешёнными видами деятельности.
- Быть действующим доверенным лицом УЦ.
- Иметь действующий агентский договор, по крайней мере, с одним центром технического обслуживания (ЦТО).
- Быть учтена в перечне сведений о мастерских, осуществляющих деятельность по установке, проверке, техническому обслуживанию и ремонту тахографов.
- Иметь действующие карты тахографа (мастерской).
- Для организации информационного обмена с УЦ и ЦТО у Мастерской иметь действующую лицензию на АРМ активизации, а также подключение к соответствующим серверам через защищённую сеть.

ТРЕБОВАНИЯ К ОПЕРАТОРУ ПДн

Согласно ст.3 ФЗ «О персональных данных», оператором ПДн является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

В случае обработки и передачи персональных данных оператор **обязан подать уведомление в Роскомнадзор, как оператор ПДн** (*Ст. 22. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"*).

ТРЕБОВАНИЯ К ОПЕРАТОРУ ПДн

Согласно ст.3 ФЗ «О персональных данных», оператором ПДн является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

В случае обработки и передачи персональных данных оператор **обязан подать уведомление в Роскомнадзор, как оператор ПДн** (*Ст. 22. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"*).

ТРЕБОВАНИЯ К ЗАЩИТЕ ПДн

Персональными данными являются сведениями о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Персональные данные в соответствии с *Указом Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера"* **являются конфиденциальными сведениями** и их защита осуществляется в соответствии с требованиями защиты конфиденциальной информации.

ТРЕБОВАНИЯ К ОПЕРАТОРУ ПДн

Оператор ПДн **обязан обеспечить техническую защиту обрабатываемых ПДн** и в соответствии с установленным уровнем защищенности (классом защиты), провести оценку эффективности принятых мер (*ФЗ от 27.07.2006 N 152-ФЗ "О персональных данных", Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"*).

ТРЕБОВАНИЯ К ОПЕРАТОРУ ПДн

Обеспечение технической защиты ПДн включает следующие этапы:

- моделирование угроз,
- определение уровня защищенности ПДн (утверждение Акта),
- проектирование системы защиты ПДн,
- выбор СЗИ,
- разработка эксплуатационной и организационно-распорядительной документации на СЗИ (ПДн),
- проведение оценки эффективности выбранных мер.

Организационные работы по технической защите ПДн выполнены оператором ИЗКТ, результаты представлены на сайте оператора ИЗКТ>>

ТРЕБОВАНИЯ К ОПЕРАТОРУ ПДн

В соответствии с определённым уровнем защищенности ПДн Оператор ПДн:

- Организует режим обеспечения безопасности помещений, в которых размещена ИС (перечень помещений хранения и обработки).
- Обеспечивает сохранность носителей ПДн.
- Определяет перечень лиц, допущенных к ПДн (приказ или распоряжение);
- Назначает ответственного за обеспечение безопасности ПДн в ИС (приказ или распоряжение);
- Определяет перечень лиц, допущенных к содержанию электронного журнала сообщений (приказ или распоряжение);
- Обеспечивает организацию автоматической регистрации в электронном журнале безопасности изменений полномочий сотрудника оператора ПДн по доступу к ПДн, содержащимся в ИС;
- Создаёт структурное подразделение, ответственное за обеспечение безопасности ПДн в ИС, либо возлагает на одно из структурных подразделений функции по обеспечению такой безопасности (приказ или распоряжение).

ТРЕБОВАНИЯ К ОПЕРАТОРУ ПДн

На основании ФЗ от 27.07.06 № 152-ФЗ «О персональных данных» Оператор ПДн должен внедрить организационные документы:

- Положения по обеспечению информационной безопасности персональных данных при их обработке.
- Политика в отношении обработки персональных данных.
- Регламент реагирования на запросы субъектов персональных данных.
- Приказ о назначении ответственного за организацию обработки персональных данных.
- Модель угроз безопасности (дублируется в ПП №1119).
- Журнал учета машинных носителей информации.
- Регламент проведения контрольных мероприятий.
- План внутренних мероприятий.
- Журнал учета внутренних проверок.
- Перечень нормативных документов о защите ПДн.

Шаблоны перечисленных выше документов представлены на сайте оператора ИЗКТ>>

ТРЕБОВАНИЯ К ПВК

Для приема заявлений на выдачу КиКСЭП с последующей их записью на КТ **Оператор ПДн обязан** получить статус **Доверенного лица УЦ**.

Для того, чтобы стать Доверенным лицом УЦ ПВК необходимо:

1) Подписать Соглашение о неразглашении конфиденциальной информации с УЦ.
2) Получить в УЦ Договор о присоединении на выполнение работ доверенного лица УЦ и Правила, в которых прописаны требования к доверенному лицу и процедурам взаимодействия доверенного лица с УЦ.
3) Информировать УЦ о присоединении к Договору.

ТРЕБОВАНИЯ К РАБОТЕ С СКЗИ

Карта тахографа и навигационный криптографический модуль (НКМ) являются средствами криптографической защиты информации (СКЗИ).

Согласно *Постановлению Правительства №313 от 16.04.2012г (ред. от 21.12.2020) "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств,…." (с изм. и доп., вступ. в силу с 01.01.2021)* **Оператор ПДн обязан иметь лицензии ФСБ России** на деятельность связанную со СКЗИ .

ТРЕБОВАНИЯ К РАБОТЕ С СКЗИ

Для работы с картами тахографа лицензированию подлежит:

- передача карт тахографа;

Применительно к тахографам со встроенным блоком СКЗИ тахографа лицензированию подлежит:

- передача блока СКЗИ тахографа, не установленного в тахограф;
- установка (монтаж) не активизированного блока СКЗИ тахографа в тахограф;
- активизация блока СКЗИ тахографа;
- активизация тахографа, поскольку она включает в себя работы по активизации блока СКЗИ тахографа;
- ремонт (сервисное обслуживание) тахографов с установкой/заменой блока СКЗИ тахографа, включая его активизацию.

ТРЕБОВАНИЯ К РАБОТЕ С СКЗИ

Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации **ПВК обязан создать орган криптографической защиты** (*п. 6 Приказ ФАПСИ от 13.06.2001 N 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*).

Функции органа криптографической защиты могут быть возложены на физическое лицо.

ТРЕБОВАНИЯ К РАБОТЕ СО СКЗИ

Орган криптографической защиты ведет:

- Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним (*форма журнала – Приложение к Приказу ФАПСИ от 13.07.2001 N 152*).
- Контроль за соблюдением правил пользования, хранения СКЗИ и условий их использования.
- Ведение на каждого пользователя СКЗИ лицевого счета (реестра СКЗИ эксплуатационной и технической документации к ним, ключевые документы).

Требования к лицензиату ИЗКТ, доверенному лицу УЦ, и агенту ОИ

ТРЕБОВАНИЯ К ЛИЦЕНЗИАТУ ИЗКТ

Лицензиат ИЗКТ должен:

- предоставить информацию о реквизитах организации, а также адреса и GPS-координаты офисов по приёму Заявителей;
- в случае изменения реквизитов организации или данных сотрудников, владельцев учётных записей, в 10-дневный срок внести соответствующие изменения в административном интерфейсе ИЗКТ;
- создавать учётные записи в ИЗКИ и допускать к работе в ИЗКТ исключительно своих сотрудников;
- передавать логин и пароль лично в руки сотрудникам, требовать от сотрудников соблюдения конфиденциальности пароля для учётной записи;
- информировать сотрудников о правилах обработки ПДн.

ПРОСТАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

Согласно Правилам пользования ИЗКТ Лицензиат признаёт, что логин является простой электронной подписью , подтверждающей факт совершения действий пользователем, которому присвоен логин. Информация, подписанная такой ЭП при работе с ИЗКТ в рамках Договора, признается Сторонами электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

В рамках Договора Лицензиат ИЗКТ обязуется признавать авторство Заявок, подписанных ЭП сотрудников Лицензиата.

ТРЕБОВАНИЯ К ДОВЕРЕННОМУ ЛИЦУ УЦ

Обязательная личная идентификация Заявителя при подаче заявления на получение КСЭП и КиКСЭП и при получении КСЭП и КиКСЭП.

Все Операторы ПВД должны иметь персональную усиленную квалифицированную электронную подпись.

Описание деловых процессов Оператора ПВД с использованием ИЗКТ

ТРЕБОВАНИЯ К ПВК

Список документов, которые ПВК должен предоставить Заявителю для ознакомлению:

- Порядок реализации функций аккредитованным УЦ.
- Договор оферты между ОИ и Заявителем.
- Правила пользования ИПФШ.467444.006ПП «Программно-аппаратные шифровальные (криптографические) средства защиты информации «Карта тахографа «Диамант-2».

Оператор ПВД обязан убедится в том, что Заявитель ознакомлен с вышеперечисленными документами, о чём отбирает расписку.

1. Этап - КОНСУЛЬТАЦИЯ

Оператор ПВД должен:

- Подготовить заявителя на КТ или его представителя к личной явке в офис.
- Проконсультировать по списку документов, которые необходимо предъявить для оформления карты тахографа.
- Записать заявителя или его представителя на приём в офис для оформления карты.

Пакет заявлений и документов для оформления карты тахограф СКЗИ

В обязательный пакет оригиналов документов водителя входят:

- Документ, удостоверяющий личность.
- Документ, подтверждающий регистрацию на территории РФ.
- Водительское удостоверение (в случае оформления КТ водителя).
- Документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учёта по форме АДИ-РЕГ или СНИЛС.
- Документ, подтверждающий идентификационный номер налогоплательщика РФ (ИНН).
- Нотариально заверенный перевод на русский язык необходимых документов только для иностранных граждан.
- Фотография заявителя (3,5х4,5см). Подробнее>>

Пакет заявлений и документов для оформления карты тахограф СКЗИ

При замене или обновлении ранее выданной карты необходимо предоставить дополнительный пакет документов. Подробнее>>

Пакет заявлений на изготовление карты тахографа:

- Заявление о выдаче (замене, обновлению) карты тахографа.
- Заявление на создание и выдачу ключей электронной подписи и квалифицированного сертификата ключа проверки электронной подписи в соответствии с регламентом УЦ.

2. Этап – СОЗДАНИЕ ЗАЯВКИ В ИС ИЗКТ

- Оператор ПВД оформляет электронную заявку на изготовление КТ и КиКСЭП только при личной явке Заявителя в офис и проводит идентификацию личности по предъявленному документу, удостоверяющему личность Заявителя.
- Оператор ПВД должен заверить копии документов, загрузить копии к электронной заявке и сформировать заявления на изготовление КТ и КиКСЭП.
- Заявитель должен лично подписать заявления на изготовление КТ и КиКСЭП.
- Оператор ПВД должен заверить заявление на КиКСЭП своей персональной усиленной квалифицированной ЭП.

3. Этап – ВЫДАЧА РАСПИСКИ И КВИТАНЦИИ

- Оператор ПВД должен распечатать для Заявителя расписку в получении документов, а также квитанцию для оплаты через банк или QR-код для оплаты через личный кабинет в публичной части ИЗКТ.
- Заявка на изготовление КТ и КиКСЭП будет передана в работу . В течение 5 рабочих дней принимается положительное или отрицательное решение УЦ об изготовлении КиКСЭП, а ОИ об изготовлении КТ.

4. Этап – ВЫДАЧА КТ И КиКСЭП

- Выдача КТ возможна только при личной явке Заявителя в офис.
- Заявитель должен будет подписать документы о получении КиКСЭП и КТ, ознакомлении с Правилами пользования и содержимым КСЭП.
- Оператор ПВД должен заверить расписку в получении Заявителем КиКСЭП своей персональной усиленной квалифицированной ЭП.
- Заявитель также получает бухгалтерские документы и акт выполненных работ.
- В случае неполучения КТ в течение заданного времени, Оператор отправляет КТ обратно ОИ.

Ответственность участников перечисленных бизнес процессов

ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА ПДн

Оператор ПДн несет ответственность согласно КоАП РФ Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных (в ред. Федерального закона от 07.02.2017 N 13-ФЗ).

Согласно статьи 13.11 предусмотрены штрафы от 1000 до 200 000 рублей в зависимости от степени нарушения.

Сотрудник Оператора ПДн несёт личную ответственность за внесение изменений в документы Заявителя, в том числе за подделку подписи в таких документах, согласно *УК РФ Статья 327. Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков*.

ОТВЕТСТВЕННОСТЬ ЛИЦЕНЗИАТА ИЗКТ

- Лицензиат ИЗКТ не имеет права передавать права использования ИС СПДн ИЗКТ (программ для ЭВМ «ИЗКТ 2.0») третьим лицам или предоставлять учётные записи лицам, не являющимся сотрудниками Лицензиата.
- При нарушении Лицензиатом требований, которые повлекли или могли бы повлечь за собой нарушение прав Лицензиара. Лицензиар вправе ограничить доступ к ИС СПДН ИЗКТ и взыскать с Лицензиата штраф в размере 1 000 000 (одного миллиона) рублей. При этом убытки возмещаются в полной сумме сверх штрафа.

ОТВЕТСТВЕННОСТЬ ДОВЕРЕННОГО ЛИЦА УЦ

- В случае нарушения правил и требований УЦ доверенное лицо может быть лишено своего статуса (быть исключено из реестра доверенных лиц УЦ). В этом случае доверенное лицо УЦ будет лишено возможности информационного взаимодействия с УЦ через ИЗКТ.
- В случае, если в результате деятельности доверенного лица УЦ, возникают издержки у УЦ, то такие издержки могут быть переложены на доверенное лицо, в результате деятельности которого они возникли.

ОТВЕТСТВЕННОСТЬ ДОВЕРЕННОГО ЛИЦА УЦ

Доверенное лицо УЦ несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных ФЗ “Об электронной подписи” и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей. (в ред. Федеральных законов от 30.12.2015 N 445-ФЗ, от 27.12.2019 N 476-ФЗ).

ОТВЕТСТВЕННОСТЬ ДОВЕРЕННОГО ЛИЦА УЦ

Гражданско-правовая ответственность заключается в том, что доверенное лицо УЦ возмещает вред, причиненный третьим лицам за неисполнение обязанностей, предусмотренных законом и договором, – ст. 15, гл. 59 ГК РФ.Так, если УЦ нарушит регламент и выдаст квалифицированный сертификат ключа проверки электронной подписи не владельцу, а неустановленному лицу, то в случае причинения ущерба владельцу убытки также могут быть взысканы с доверенного лица УЦ. Федеральным законом от 28.12.2016 № 471-ФЗ была введена ст. 13.33 в КоАП, которая устанавливает административную ответственность за нарушение ими обязанностей, предусмотренных законодательством в области электронной подписи.

ОТВЕТСТВЕННОСТЬ ДОВЕРЕННОГО ЛИЦА УЦ

Размеры административного штрафа варьируются в статье от 5 до 500 тыс. руб. и зависят от степени возможного причинения вреда. Так, за нарушение доверенным лицом УЦ порядка выдачи квалифицированного сертификата ключа проверки электронной подписи, установленного ст. 18 ФЗ "Об электронной подписи", штрафы могут быть от 10 до 30 тыс. руб.

За выдачу квалификационного сертификата, содержащего заведомо недостоверную информацию о его владельце, – от 200 до 250 тыс. руб., а если будут нарушены требования к его содержанию, то доверенному лицу УЦ придется заплатить от 50 до 150 тыс. руб.

За повторные нарушения штрафы взимаются в двухкратном размере.

Спасибо за внимание!

Подготовлено по заказу Ассоциации Тахоцентр

Настоящий материал доступен по ссылке
http://www.sovtehsnab.ru/?page_id=717