КАЗЕННОЕ УЧРЕЖДЕНИЕ ГОРОДА ОМСКА
«Управление по обеспечению деятельности Администрации города Омска»
(КУ г. Омска «Управление по обеспечению деятельности Администрации города Омска»)

ПРИКАЗ

«11» мая 2021 г. № 18 -ОД

г. Омск

Об организации работы с персональными данными и защиты информации

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудового кодекса Российской Федерации, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Администрации города Омска от 26.03.2021 № 188-п «Об обеспечении защиты информации, обрабатываемой в информационных системах Администрации города Омска», Постановления Администрации города Омска от 26.03.2021 № 189-п «Об утверждении Положения об информационно-телекоммуникационной сети Администрации города Омска», Соглашения на обработку персональных данных в муниципальной информационной системе «Система электронного документооборота и делопроизводства Администрации города Омска» заключенного между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска» и Казенным учреждением города Омска «Управление информационно-коммуникационных технологий», руководствуясь Уставом Казенного учреждения города Омска «Управление по обеспечению деятельности Администрации города Омска», утвержденным приказом Заместителя Мэра города Омска, управляющего делами Администрации города Омска от 31 января 2011 № 15,

ПРИКАЗЫВАЮ:

1. Утвердить:

1) Политику Казенного учреждения города Омска «Управление по обеспечению деятельности Администрации города Омска» в отношении обработки и защиты персональных данных (приложение № 1 к настоящему приказу);

2) Положение об обработке персональных данных (приложение № 2 к настоящему приказу);

3) Положение об обеспечении защиты информации, обрабатываемой в информационных системах (приложение № 3 к настоящему приказу);

4) Положение о системе межведомственного электронного взаимодействия (приложение № 4 к настоящему приказу);

5) Положение об осуществлении деятельности по созданию (замене) и выдаче простой электронной подписи с использованием сервисов Федеральной государственной информационной системы «Единая система идентификации и аутентификации инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА) (приложение № 5 к настоящему приказу).

2. Признать утратившими силу приказы директора:

1) от 17.08.2009 № 35-ОД «Об организации работы с персональными данными работников в Казенном учреждении города Омска «Управление по обеспечению деятельности Администрации города Омска»;

2) от 20.01.2010 № 3-ОД «Об обеспечении защиты информации в муниципальном учреждении «Управление по обеспечению деятельности Администрации города Омска»;

3) от 28.05.2010 № 23-ОД «О наделении отдельных сотрудников правом ЭЦП при осуществлении электронного документооборота с Управление Федерального казначейства по Омской области»;

4) от 15.12.2010 № 42-ОД «О создании комиссии по защите персональных данных работников казенного учреждения «Управление по обеспечению деятельности Администрации города Омска»;

5) от 03.06.2012 № 22-ОД «О наделении ответственных лиц правом электронной подписи при работе в системе межведомственного электронного взаимодействия»;

6) от 10.01.2013 № 2-ОД «О назначении ответственного лица в Казенном учреждении города Омска «Управление по обеспечению деятельности Администрации города Омска»;

7) от 15.01.2014 № 1-ОД «О внесении изменений и дополнений в некоторые распорядительные и иные документы»;

8) от 02.02.2015 № 3-ОД «Об организации работы с персональными данными и защиты информации»;

9) от 12.03.2019 № 9-ОД «О внесении изменений в приказы директора от 17.08.2009 № 35-ОД, от 02.02. 2015 № 3-ОД»;

10) от 15.07.2019 № 22-ОД «О внесении изменений в приказы директора от 02.02. 2015, от 12.12.2018 № 46-ОД».

3. Специалисту по охране труда Кумскову С.И. разместить настоящий приказ в сети «Интернет» на официальном сайте Администрации города Омска.

Директор А.А. Ложечкин

Приложение № 1 к приказу директора
от «11» 05 2021 №18-ОД

ПОЛИТИКА
Казенного учреждения города Омска «Управление по обеспечению деятельности Администрации города Омска» в отношении обработки и защиты персональных данных

1. Общие положения

1.1. Политика в отношении обработки и защиты персональных данных в Казенном учреждении города Омска «Управление по обеспечению деятельности Администрации города Омска» (далее - Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Администрации города Омска от 26.03.2021 № 188-п «Об обеспечении защиты информации, обрабатываемой в информационных системах Администрации города Омска», Постановлением Администрации города Омска от 26.03.2021 № 189-п «Об утверждении Положения об информационно-телекоммуникационной сети Администрации города Омска», Соглашением на обработку персональных данных в муниципальной информационной системе «Система электронного документооборота и делопроизводства Администрации города Омска», заключенным между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска» и Казенным учреждением города Омска «Управление информационно-коммуникационных технологий».

1.2. Политика определяет порядок и условия обработки персональных данных в Казенном учреждении города Омска «Управление по обеспечению деятельности Администрации города Омска» (далее – Оператор или по поручению Оператора) с использованием средств автоматизации и без использования таких средств, а также организацию мероприятий по защите персональных данных.

1.3. Обработка персональных данных в учреждении осуществляется в целях:

а) осуществления основной деятельности учреждения, ведения кадрового делопроизводства, обеспечения соблюдения федеральных законов и иных нормативных правовых актов Российской Федерации, субъектов РФ и органов местного самоуправления, организации процесса трудовых отношений с работниками, обеспечения личной безопасности работников, контроля количества

и качества выполняемой работы, ведения бухгалтерского учёта;

б) исполнения возложенных на Учреждение полномочий и обязанностей в части организации предоставления муниципальных услуг в соответствии с административными регламентами предоставления муниципальных услуг на основании поручений, заключенных с органами, оказывающими предоставление муниципальных услуг в Администрации города Омска;

в) рассмотрения обращений граждан (жалоб), в том числе от государственных органов, органов местного самоуправления и должностных лиц Администрации города Омска, иных уполномоченных юридических лиц.

2. Основные понятия, используемые в настоящей Политике

2.1. Настоящие основные понятия распространяются на Положение организации работы с персональными данными, Положение об обеспечении защиты персональных данных, Положение о системе межведомственного электронного взаимодействия при организации предоставления муниципальных услуг, Положение об осуществлении деятельности по созданию (замене) и выдаче простой электронной подписи с использованием сервисов Федеральной государственной информационной системы «Единая система идентификации аутентификации инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА).

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Передача персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных (сегменте) и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту

персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Поручение оператора персональных данных - обработка персональных данных другим лицом с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого Оператором с этим лицом договора (поручения), в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего нормативного акта.

Информация – сведения (сообщения, данные) независимо от формы их представления;

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

Обработка информации – вся совокупность действий (операций), включая сбор, ввод, запись, преобразование, считывание, хранение, уничтожение, регистрацию, передачу (распространение, предоставление, доступ), осуществляемых с помощью технических и программных средств;

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональным предназначениям и техническим характеристикам;

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Сегмент информационной системы (далее – сегмент) – компонент (составная часть) информационной системы, предназначенный для обработки информации и решения функциональных задач;

Центральный сегмент информационной системы – компонент (составная часть) информационной системы, предназначенный для обеспечения взаимодействия сегментов информационной системы, включая возможность хранения основных баз данных;

Защищаемый ресурс информационной системы (сегмента) – техническое средство, узел сети, линия (канал) связи, программа, том, каталог, файл и иные объекты, доступ к которым регламентируется правилами разграничения доступа принятыми в информационной системе (сегменте);

Оператор информационной системы (сегмента) – подразделение, осуществляющее деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

Пользователь информационной системы (сегмента) (далее – пользователь) – лицо, участвующее в функционировании информационной системы (сегмента) при обработке информации или использующее результаты ее функционирования;

Ответственный за организацию обработки персональных данных – лицо,

ответственное за разработку, внедрение и поддержание в актуальном состоянии комплекса организационных и технических мер, направленных на защиту персональных данных, а также осуществляющее контроль за исполнением указанных мер и организацию реагирования на инциденты информационной безопасности, связанные с нарушением данных мер;

Администратор безопасности информационной системы (сегмента) – лицо, ответственное за защиту информационной системы (сегмента) от несанкционированного доступа к информации;

Ответственный за эксплуатацию информационной системы (сегмента) – ответственное лицо, обеспечивающее правильное использование и функционирование системы защиты информации;

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Администратор сегмента Сети – подразделение или работник, ответственные за информатизацию в структурном подразделении, учреждении, осуществляющие контроль за функционированием сегмента Сети, а в отношении структурных подразделений и учреждений, в штатном расписании которых отсутствуют должности специалистов, обеспечивающих информатизацию соответствующих структурных подразделений, учреждений, в отношении должностных лиц Администрации – Казенное учреждение города Омска «Управление информационно-коммуникационных технологий»;

АРМ – автоматизированное рабочее место пользователя, с установленным программным обеспечением и периферийными устройствами подключенное к локальной сети;

Главный администратор Сети – Казенное учреждение города Омска «Управление информационно-коммуникационных технологий», которое осуществляет управление центральным сегментом Сети и предоставляет сервисы Сети структурным подразделениям, должностным лицам Администрации, учреждениям;

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Регламентные работы – плановая замена оборудования Сети и его техническое обслуживание, обновление программного обеспечения оборудования Сети, резервное копирование информации;

Ремонтные работы – работы по замене, ремонту оборудования Сети и восстановлению программного обеспечения в случае сбоя в функционировании Сети;

Сегмент Сети – локальная информационно-телекоммуникационная сеть (далее – локальная сеть) – единая технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники структурного подразделения, учреждения, находящихся в введении соответствующего структурного подразделения, учреждения;

Сервер – программно-аппаратный комплекс, предназначенный для централизованного хранения и обработки информации, функционирования Сети и информационных систем;

Сервисы Сети – совокупность услуг, предоставляемых посредством Сети;

Сетевое оборудование – совокупность устройств, необходимых для работы Сети и обеспечивающих подключение АРМ к Сети;

Сеть – единая технологическая система, объединяющая сегменты Сети, подключенные к центральному сегменту Сети, в состав которой входят АРМ, системы бесперебойного питания, периферийные устройства, кабельная система, сетевое оборудование, серверы, система внутренней телефонной связи;

Система бесперебойного питания – технологическая система, обеспечивающая защиту внутренних сетей электропитания от воздействия дестабилизирующих факторов, действующих в сетях электроснабжения;

Система внутренней телефонной связи – программно-аппаратный комплекс, обеспечивающий передачу голосовой информации с использованием сетевого оборудования и технических средств передачи и приема данных, включая линии связи, а также средства программного обеспечения;

Центральный сегмент Сети – комплекс оборудования, обеспечивающий передачу информации между сегментами Сети и предоставляющий сервисы Сети.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на законной основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.

3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператором (по поручения Оператора) обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных осуществляется в форме, позволяющей

определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

3.8. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Условия обработки персональных данных

4.1. Обработка персональных данных осуществляется с соблюдением принципов, требований и правил, предусмотренных законодательством Российской Федерации и нормативно-правовыми актами муниципальных органов.

4.2. Обработка персональных данных допускается в следующих случаях:

а) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

б) обработка персональных данных необходима для достижения целей, предусмотренных для осуществления и выполнения возложенных на Оператора (по поручению Оператора) функций, полномочий и обязанностей;

в) обработка персональных данных необходима для исполнения полномочий структурных подразделений Администрации города Омска, а также учреждений, участвующих в предоставлении муниципальных услуг Администрации города Омска, включая регистрацию субъекта персональных данных на Едином портале предоставления государственных и муниципальных услуг.

4.3. В случае, если Оператор поручает обработку персональных данных другому лицу (Казенному учреждению города Омска «Управлению по обеспечению деятельности Администрации города Омска»), ответственность перед субъектом персональных данных за действия указанного лица несет Оператор.

В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

4.4. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

4.5. Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренных Федеральным законодательством.

5. Конфиденциальность персональных данных

5.1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6. Право субъекта персональных данных на доступ к его персональным данным

6.1. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения субъекту персональных данных должны быть предоставлены Оператором (лицом по поручению Оператора) в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных

6.3. Сведения предоставляются субъекту персональных данных или его представителю Оператором (лицом по поручению Оператора) при обращении либо при получении запроса субъекта персональных данных или его представителя.

6.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

а) подтверждение факта обработки персональных данных Оператором (по поручению Оператора);

б) правовые основания обработки персональных данных;

в) цели и применяемые Оператором способы обработки персональных данных;

г) наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которые могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

е) сроки обработки персональных данных, в том числе сроки их хранения;

ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

з) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7. Право на обжалование действий или бездействий Оператора

7.1. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8. Обязанности Оператора при сборе персональных данных

8.1. Обработка персональных данных Оператором (по поручению Оператора) осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

8.2. При определении объема и содержания обрабатываемых персональных данных Оператор (по поручению Оператора) должен руководствоваться действующим законодательством РФ.

8.3. Оператор (по поручению Оператора) осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

8.4. К обработке персональных данных допускаются работники Оператора (по поручению Оператора), в должностные обязанности, которых входит обработка персональных данных.

8.5. Обработка персональных данных осуществляется путем:

-получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;

-получения персональных данных из общедоступных источников;

-внесения персональных данных в журналы, реестры и информационные системы Оператора;

-ввода данных, направления запросов по сбору персональных данных, получение персональных данных из различных государственных, муниципальных и иных уполномоченных органов и учреждений по поручению Оператора, в порядке межведомственного документооборота (в том числе электронного);

-приема, обработки, регистрации поступивших обращений граждан (в том числе при рассмотрении жалоб и подготовке ответов), перенаправления по компетенции, содержащие персональные данные заявителей;

-приема, обработки, регистрации поступивших обращений граждан, содержащие персональные данные заявителей, поступивших посредством Единого и регионального портала предоставления государственных и муниципальных услуг;

-использования иных способов обработки персональных данных.

8.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

8.7. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

8.8. Все персональные данные следует получать у субъекта персональных данных.

8.9. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

8.10. Оператор не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных федеральными законами, а также по поручению оператора.

8.11. Оператор не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности.

8.12. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

8.13. Защита персональных данных работников от неправомерного их использования или утраты должна обеспечена за счет собственных средств, либо за счет мероприятий, реализуемых третьими лицами согласно договора о технической защите информации.

8.14. Работники должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

8.15. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

8.16. Оператор, работники (и их представители) должны совместно вырабатывать меры защиты персональных данных работников.

8.17. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

8.18. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или

случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

-определяет угрозы безопасности персональных данных при их обработке;

-принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;

-назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;

-создает необходимые условия для работы с персональными данными;

-организует учет документов, содержащих персональные данные;

-организует работу с информационными системами, в которых обрабатываются персональные данные;

-хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

-организует обучение работников Оператора, осуществляющих обработку персональных данных.

8.19. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

9. Ответственность за нарушение норм, регулирующих обработку персональных данных

9.1. Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

9.2. Моральный вред, причиненный вследствие нарушения прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 № 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных убытков.

Приложение № 2 к приказу директора
от «11» 05 2021 № 18-ОД

ПОЛОЖЕНИЕ
об обработке персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, субъектов Российской Федерации, органов местного самоуправления, регламентирующими порядок обработки и защиты персональных данных.

1.2. Положение об обработке персональных данных определяет порядок и условия обработки персональных данных в Казенном учреждении города Омска «Управление по обеспечению деятельности Администрации города Омска» (далее – Учреждение), устанавливает процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, связанных с обработкой персональных данных.

1.3. Оператор - это 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.

1.4. Действие настоящего Положения не распространяется на отношения, возникающие при:

1) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных фондов;

2) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

3) предоставлении уполномоченными органами информации о деятельности Учреждения.

1.5. Способы обработки персональных данных:

- с использованием средств автоматизации;
- без использования средств автоматизации.

1.6. В соответствии с поставленными целями и задачами до начала обработки персональных данных в Учреждении должны быть назначены ответственное лицо (лица) за организацию обработки персональных данных, ответственные лица за эксплуатацию информационных систем (сегментов) в которых осуществляется обработка персональных данных, администраторы безопасности информации по каждой информационной системе (сегменту).

1.7. Работники, непосредственно осуществляющие обработку персональных данных, должны быть ознакомлены под роспись до начала

работы с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, с данным Положением и изменениями к нему.

1.8. При обработке персональных данных Оператор обязан применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.9. Оператор обязан обеспечить неразглашения сведений и персональных данных, работниками Учреждения, в обязанности которых входит обработка персональных данных ставших известных в ходе исполнения трудовых обязанностей.

1.10. Контроль за соблюдением работниками Оператора требований законодательства Российской Федерации и положений локальных актов Оператора должен быть организован в соответствии с требованиями настоящего Положения.

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

Контроль может также осуществляться учредителем - Управлением делами Администрации города Омска, ответственным за обеспечение безопасности персональных данных или сторонними организациями и Учреждениями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

1.11. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Оператором требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», определяется в соответствии со ст. ст. 15, 151, 152, 1101 Гражданского кодекса Российской Федерации.

1.12. Опубликование или обеспечение иным образом неограниченного доступа к настоящему Положению, иным документам, определяющим политику Оператора в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных Оператор проводит в соответствии с требованиями части второй ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.13. При осуществлении сбора персональных данных с использованием информационно-телекоммуникационных сетей Оператор до начала обработки персональных данных обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

1.14. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении в порядке, предусмотренном Положением о хранении персональных данных у Оператора (по поручению Оператора).

1.15. Взаимодействие с федеральными органами исполнительной власти по вопросам обработки и защиты персональных данных субъектов, персональные данные которых обрабатываются Оператором, осуществляется в рамках законодательства Российской Федерации.

2. Порядок обработки персональных данных

2.1. Порядок обработки персональных данных в Учреждении определён исходя из целей их обработки.

2.2. Порядок обработки персональных данных при осуществлении основной деятельности учреждения, ведение кадрового делопроизводства, обеспечение соблюдения федеральных законов и иных нормативных правовых актов Российской Федерации, субъектов РФ и органов местного самоуправления, организации процесса трудовых отношений с работниками, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, ведения бухгалтерского учёта.

2.2.1. Персональные данные работников Учреждения и граждан, претендующих на вакантные должности в Учреждении обрабатываются в целях обеспечения кадровой работы, в том числе в целях обеспечения трудовой деятельности, содействия в трудоустройстве, обеспечения личной безопасности сотрудников и членов их семей, условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества, а также в целях противодействия коррупции.

2.2.2. Обрабатываются следующие категории персональных данных:

1) Фамилия, имя, отчество, дата и место рождения, гражданство;

2) Адрес и дата регистрации по месту проживания;

3) Паспортные данные (серия, номер, кем и когда выдан);

4) Идентификационный номер налогоплательщика;

5) Номер страхового свидетельства обязательного пенсионного страхования;

6) Сведения об образовании и (или) о квалификации, наличии специальных знаний (подготовки);

7) Прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

8) Сведения о трудовой деятельности (включая военную и приравненную к ней службу, работу по совместительству, предпринимательскую деятельность и т.п.);

9) Государственные награды, иные награды и знаки отличия (кем

награжден и когда);

10) При необходимости подтверждения степени родства - фамилии, имена, отчества, даты и место рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

11) Номера телефонов;

12) Номера расчетных счетов, банковских карт;

13) Сведения о наличии/отсутствии судимости ;

14) Сведения о доходах;

15) Сведения о социальных льготах, и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения);

16) Фотографии;

17) Иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.2 настоящего Положения.

2.2.3. Обработка персональных данных работников Учреждения, а также граждан, претендующих на вакантные должности в Учреждении, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 2.2 настоящего Положения в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных».

2.2.4. Обработка специальных категорий персональных данных работников Учреждения, граждан, претендующих на вакантные должности Учреждения, лиц, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 2.2 настоящего Положения, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и нормами Трудового кодекса Российской Федерации, за исключением случаев получения персональных данных работника у третьей стороны (в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации требуется письменное согласие).

2.2.5. Обработка персональных данных работников Учреждения, граждан, претендующих на вакантные должности Учреждения, осуществляется при условии получения согласия указанных лиц в следующих случаях:

-при передаче (распространении, предоставлении) персональных данных третьим лицам;

-при трансграничной передаче персональных данных;

-при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

В этих случаях согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.2.6. Обработка персональных данных работников Учреждения, граждан, претендующих на вакантные должности Учреждения,

осуществляется сектором муниципального заказа, правовой и кадровой работы Учреждения и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.2.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных работников Учреждения, граждан, претендующих на вакантные должности Учреждения, осуществляется путем:

-получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, анкета, иные документы, предоставляемые в кадры Учреждения);

-внесения сведений в учетные формы (на бумажных и электронных носителях);

-формирования персональных данных в ходе кадровой работы;

-внесения персональных данных в информационные системы, используемые сектором муниципального заказа, правовой и кадровой работы.

2.2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от работников Учреждения, граждан, претендующих на вакантные должности.

2.2.9. В случае возникновения необходимости получения персональных данных работника Учреждения у третьей стороны, следует известить об этом работника, заранее получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

2.2.10. Запрещается получать, обрабатывать и приобщать к личному делу работника Учреждения, персональные данные, не предусмотренные целями настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.2.11. При сборе персональных данных работник сектора муниципального заказа, правовой и кадровой работы, осуществляющий сбор (получение) персональных данных непосредственно от работников Учреждения, граждан, претендующих на вакантные должности Учреждения, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.2.12. Передача (распространение, предоставление) и использование персональных данных работников Учреждения, граждан, претендующих на вакантные должности Учреждения, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

2.2.13. Обработка персональных данных для достижения целей, предусмотренных пунктом 2.2 настоящего Положения осуществляется посредством информационной системы «1С: Предприятие».

2.2.14. Оператором информационной системы «1С: Предприятие» являются работники сектора бухгалтерского учета и отчетности и работники сектора муниципального заказа и сектора правовой и кадровой работы Учреждения, техническое сопровождение информационной системы осуществляется ООО «Бизнес системы» на основании муниципального контракта.

2.2.15. Работникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах Учреждения, предоставляется уникальный логин и пароль для доступа к соответствующей к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными инструкциями сотрудников Учреждения.

Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Учреждения, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

-определение угроз безопасности персональных данных при их обработке в информационных системах (сегментах) персональных данных;

-применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах (сегментах) персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

-применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

-оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

-учет машинных носителей персональных данных;

-обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

-восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

-установление правил доступа к персональным данным, разрабатываемым в информационных системах персональных данных Учреждения, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Учреждения;

-контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

2.2.16. В случае выявления нарушений порядка обработки персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и

их устранению.

2.2.17. Для сохранности информации и персональных данных работников Учреждения сектором бухгалтерского учета и отчетности должно производиться резервное копирование данных информационной системы «1С:Предприятие» ежедневно, в конце рабочего дня, на внешний носитель информации. Внешний носитель информации должен храниться в сейфе, расположенном в помещении сектора бухгалтерского учета и отчетности.

Входная дверь помещения сектора бухгалтерского учета и отчетности должна быть оборудована замком и пломбирным устройством с пеналом.

Должен быть определен перечень лиц, имеющих право вскрытия помещения.

Хранение ключей от помещения сектора бухгалтерского учета и отчетности должно осуществляться на посту охраны здания Администрации города Омска.

Выдача и прием ключей подлежит обязательной регистрации в журнале, с подписью ответственных лиц.

2.2.18. Сроки обработки и хранения персональных данных сотрудников Учреждения, граждан, претендующих на вакантные должности Учреждения, определяются в соответствии с законодательством Российской Федерации.

С учетом положений законодательства Российской Федерации устанавливаются следующие сроки обработки и хранения персональных данных сотрудников Учреждения:

а) персональные данные, содержащиеся в приказах по личному составу сотрудников Учреждения (о приеме, перемещении, переводе, увольнении), подлежат хранению в секторе муниципального заказа, правовой и кадровой работы Учреждения в течение двух лет с последующим формированием и передачей указанных документов в архив Учреждения или муниципальный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение (75) 50 лет;

б) персональные данные, содержащиеся в личных делах сотрудников, хранятся в секторе муниципального заказа, правовой и кадровой работы Учреждения в течение трудовой деятельности работника. В последующим (при расторжении трудового договора) сформированное в течении двух лет личное дело передается в архив Учреждения или муниципальный архив, в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение (75) 50 лет;

в) персональные данные, содержащиеся в приказах о поощрениях, отпусках по беременности и родам, отпусках по уходу за ребенком, отпусках без сохранения заработной платы, совмещении, изменении фамилии, назначении надбавки за стаж работы, подлежат хранению в течении двух лет в секторе муниципального заказа, правовой и кадровой работы Учреждения с последующим формированием и передачей указанных документов в архив Учреждения или муниципальный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение (75) 50 лет;

г) персональные данные, содержащиеся в приказах о ежегодных оплачиваемых отпусках, отпусках в связи с обучением, о командировках подлежат хранению в секторе муниципального заказа, правовой и кадровой работы Учреждения в течение пяти лет с последующим уничтожением;

д) персональные данные, содержащиеся в приказах о дисциплинарных взысканиях подлежат хранению в секторе муниципального заказа, правовой и кадровой работы Учреждения в течении трех лет с последующим уничтожением;

е) персональные данные, содержащиеся в Карточках-справках по заработной плате подлежат хранению в течении двух лет в секторе бухгалтерского учета и отчетности Учреждения с последующим формированием и передачей указанных документов в архив Учреждения или муниципальный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение (75) 50 лет;

ж) персональные данные, содержащиеся в расчетах платежей по страховым взносам подлежат хранению в течении двух лет в секторе бухгалтерского учета и отчетности Учреждения с последующим формированием и передачей указанных документов в архив Учреждения или муниципальный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течение (75) 50 лет;

з) персональные данные, содержащиеся в сведениях о доходах физических лиц подлежат хранению в секторе бухгалтерского учета и отчетности Учреждения в течении пяти лет с последующим уничтожением;

и) персональные данные, содержащиеся в документах (списки застрахованных лиц, сведения, описи и др.) по персонифицированному учету работников учреждения, подлежат хранению в секторе бухгалтерского учета и отчетности Учреждения в течении пяти лет с последующим уничтожением;

к) персональные данные, содержащиеся в документах (заявления, справки, протоколы) о выплате пособий, оплате листков нетрудоспособности подлежат хранению в секторе бухгалтерского учета и отчетности Учреждения в течении пяти лет с последующим уничтожением;

л) персональные данные, содержащиеся в исполнительных листах. подлежат хранению в секторе бухгалтерского учета и отчетности Учреждения в течении пяти лет с последующим уничтожением.

2.2.19. Персональные данные должны храниться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

2.2.20. Документы, содержащие персональные данные, обрабатываемые в секторе муниципального заказа, правовой и кадровой работы, а также съемные носители информации, электронные подписи должны храниться в сейфе либо в металлических шкафах, которые должны быть оборудованы исправными запирающими устройствами.

Доступ к ключам от сейфов или металлических шкафов должен иметь ограниченный круг лиц.

2.2.21. Резервное копирование документов, содержащих персональные данные в секторе муниципального заказа, правовой и кадровой работы не осуществляется.

2.2.22. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом (пункт 7 статьи 5 Федерального закона «О персональных данных»).

2.2.23. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

2.2.24. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений (отделов, секторов) Учреждения.

2.2.25. Уполномоченными лицами Учреждения, ответственными за обеспечение безопасности персональных данных должен осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению (удалению, стиранию).

2.2.26. Вопрос об уничтожении выделенных документов, содержащих персональные данные, должен рассматривается на заседании экспертной комиссии Учреждения, которая производит экспертизу ценности документов, в порядке требований Положения об экспертной комиссии.

2.2.27. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

2.2.28. Уничтожение выделенных документов на бумажных носителях производиться с помощью бумагорезательной машины путем измельчения документов на куски, гарантирующего невозможность восстановления текста либо путем сжигания.

2.2.29. Категорически запрещается утилизация документов, содержащие персональные данные путем утилизации в мусор, передачи третьим лицам для утилизации, повторного использования в качестве черновиков.

2.2.30. Категорически запрещается предоставлять доступ к документам и информационным системам (обрабатываемому сегменту), содержащие персональные данные не уполномоченным на то лицам (не работникам Учреждения, участвующих в обработке персональных данных), в том числе

специалистам структурных подразделений Администрации города Омска, иных подведомственных учреждений, практикантам и иным лицам.

2.3. **Порядок обработки персональных данных при исполнении возложенных на Учреждение полномочий и обязанностей в части организации предоставления муниципальных услуг в соответствии с административными регламентами предоставления муниципальных услуг на основании поручений, заключенных с органами, оказывающими предоставление муниципальных услуг в Администрации города Омска.**

2.3.1. Обработка персональных данных граждан с целью организации предоставления государственных и муниципальных услуг, в том числе в электронной форме, осуществляется отделом «Служба одного окна» Учреждения в соответствии с Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», постановлением Администрации города Омска от 05.09.2011 № 977-п «Об организации работы по предоставлению документов по принципу «одного окна», административными регламентами предоставления муниципальных услуг, иными нормативными правовыми актами, определяющими предоставление государственных услуг и исполнение государственных функций в установленной сфере ведения Учреждения.

2.3.2. Обработка персональных данных, в данном случае осуществляется посредством муниципальной информационной системы «Система электронного документооборота и делопроизводства Администрации города Омска» на основании распоряжения Администрации города Омска от 09.04.2010 № 162-р «О внедрении системы электронного документооборота и делопроизводства Администрации города Омска», распоряжения Администрации города Омска от 27.10.2011 № 504-р «О системе электронного документооборота и делопроизводства Администрации города Омска», распоряжения Администрации города Омска от 18.09.2012 № 337-р «О Порядке работы в системе электронного документооборота и делопроизводства Администрации города Омска».

2.3.3. Согласно Постановления Администрации города Омска от 26.03.2021 № 188-п, операторами информационной системы (сегмента) являются должностные лица, структурных подразделений Администрации города Омска и подведомственных учреждений, участвующие в функционировании сегмента информационной системы при обработке информации или использующие результаты ее функционирования.

Администратором муниципальной информационной системы «Система электронного документооборота и делопроизводства Администрации города Омска» является Казенное Учреждение города Омска «Управление информационно-коммуникационных технологий».

2.3.4. Персональные данные граждан, обратившихся за государственной или муниципальной услугой лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения

указанных обращений с последующим уведомлением заявителей о результатах рассмотрения на основании поручения, в порядке ст. 19 Федерального закона «О персональных данных».

2.3.5. Структурные подразделения Администрации города Омска, подведомственные Учреждения, участвующие в предоставлении муниципальных услуг Администрации города Омска по принципу «одного окна» (Оператор) обязаны поручить обработку персональных данных работникам отдела «Служба одного окна» Учреждения *(заключить соглашение на обработку персональных данных)* в целях исполнения отделом возложенных полномочий и обязанностей по организации предоставления муниципальных услуг (далее - поручение оператора).

2.3.6. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться работниками отдела «Служба одного окна» Учреждения, цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, обеспечение безопасности персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

Существенным условием такого поручения является наличие права у работников отдела «Служба одного окна» Учреждения на обработку персональных данных и обязанность обеспечения указанными лицами конфиденциальности и безопасности персональных данных при их обработке.

2.3.7. В согласии на обработку персональных данных субъект обработки должен указать своё согласие на обработку персональных данных третьими лицами - работникам отдела «Служба одного окна» Учреждения.

2.3.8. Перечень действий, совершаемых с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), удаление, уничтожение персональных данных.

2.3.9. Объем и категории обрабатываемых персональных данных:

1) фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2) число, месяц, год рождения;

3) место рождения;

4) информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

5) вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

6) адрес места жительства (адрес регистрации, фактического проживания);

7) номер контактного телефона или сведения о других способах связи;

8) реквизиты страхового свидетельства государственного пенсионного страхования;

9) идентификационный номер налогоплательщика;

10) реквизиты страхового медицинского полиса обязательного медицинского страхования;

11) реквизиты свидетельства государственной регистрации актов гражданского состояния;

12) семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

13) фотография

14) иные персональные данные, необходимые для достижения целей.

2.3.10. Работникам отдела «Служба одного окна» Учреждения, осуществляющие обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными инструкциями работников отдела.

2.3.11. Информация может вноситься как в автоматическом режиме при получении персональных данных с Единого портала государственных услуг, Регионального портала государственных услуг, официального сайта Администрации города Омска, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

2.3.12. Категорически запрещается предоставлять доступ к документам и информационным системам (обрабатываемому сегменту), содержащие персональные данные не уполномоченным на то лицам (не работникам Учреждения, участвующих в обработке персональных данных), в том числе специалистам структурных подразделений Администрации города Омска, иных подведомственных учреждений, практикантам и иным лицам.

2.3.13. Документы, содержащие персональные данные в отделе «Служба одного окна», а также съемные носители информации, электронные подписи должны храниться в сейфе, в металлических шкафах, либо ящиках или шкафах и оборудованы исправными запирающими устройствами. Доступ к ключам от сейфов или металлических шкафов, ящиков, шкафов должен иметь ограниченный круг лиц.

2.3.14. Резервное копирование информации, содержащей персональные данные в отделе «Служба одного окна» не осуществляется.

2.3.15. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных (сегменте) отдела «Служба одного окна», достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

-определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

-применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения, необходимых для выполнения требований к защите персональных данных, исполнение которых

обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

-применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

-оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

-учет машинных носителей персональных данных;

-обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

-восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

-установление правил доступа к персональным данным, разрабатываемым в информационных системах персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Учреждения;

-контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

2.3.16. Общий срок использования персональных данных определяется периодом времени, в течение которого Учреждение осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки.

Персональные данные должны храниться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Персональные данные граждан, обратившихся за получением государственной или муниципальной услугой лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, подлежат уничтожению либо обезличиванию после достижения цели обработки (после выдачи документов о результатах обращения граждан, направления решения почтовым отправлением, на электронную почту, в личный кабинет портала заявителя).

2.3.17. Работник отдела «Служба одного окна» (иное уполномоченное лицо) при выдаче заявителю документов о предоставлении муниципальной услуги, обязан сделать отметку о дате и способе выдаче документа в регистрационно-контрольной карточке базы данных «Служба одного окна» МИС «Система электронного документооборота и делопроизводства Администрации города Омска» (далее - СЭДД), что подтверждает достижение цели обработки, вследствие чего, доступ к персональным данным у работника прекращается.

2.3.18. Персональные данные заявителей удаляются или обезличиваются в порядке, установленном в структурных подразделениях Администрации города Омска, которые оказывали предоставление муниципальной услуги.

2.3.19. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом (пункт 7 статьи 5 Федерального закона «О персональных данных»).

2.3.20. Персональные данные, предоставляемые субъектами на бумажном носителе в связи с организацией предоставления муниципальных услуг на бумажных носителях должны храниться в архиве отдела «Служба одного окна». Помещение архива должно иметь запорное устройство, доступ в которое иметь ограниченный круг лиц.

2.3.21. Персональные данные, содержащиеся на бумажных носителях, подлежат хранению в архиве отдела «Служба одного окна» в течение пяти лет с последующим уничтожением.

2.3.22. Вопрос об уничтожении выделенных документов, содержащих персональные данные, должен рассматривается на заседании экспертной комиссии Учреждения, которая производит экспертизу ценности документов, в порядке требований Положения об экспертной комиссии.

2.3.23. Уничтожение выделенных документов на бумажных носителях производиться с помощью бумагорезательной машины путем измельчения документов на куски, гарантирующего невозможность восстановления текста либо путем сжигания.

2.3.24. Категорически запрещается утилизация документов, содержащие персональные данные путем утилизации в мусор, передачи третьим лицам для утилизации, повторного использования в качестве черновиков.

2.3.25. Категорически запрещается предоставлять доступ к документам и информационным системам (обрабатываемому сегменту), содержащие персональные данные не уполномоченным на то лицам (работникам Учреждения не участвующих в обработке персональных данных), в том числе специалистам структурных подразделений Администрации города Омска, иных подведомственных учреждений, практикантам и иным лицам.

2.3.26. Обработка персональных данных при осуществлении межведомственного электронного взаимодействия (далее - СМЭВ) осуществляется на основании Соглашения от 05.09.2011 № 243-с о взаимодействии при обеспечении предоставления (исполнения) государственных (муниципальных) услуг (функций) в электронной форме заключенного между Министерством промышленной политики, транспорта и связи Омской области и Администрацией города Омска.

2.3.26.1. Персональные данные граждан, обратившихся за муниципальной услугой посредством государственной информационной системой Омской области «Региональный портал предоставления

государственных и муниципальных услуг Омской области» поступают в СЭДД на основании актов ввода в эксплуатацию, составленными между Казенным Учреждением Омской области «Государственное Учреждение информационных технологий и коммуникаций», структурными подразделениями Администрации города Омска, Администрациями округов города Омска, Казенным Учреждением города Омска «Управление информационно-коммуникационных технологий».

2.3.26.2. Право осуществлять обработку персональных данных в рамках электронного информационного взаимодействия с применением системы межведомственного электронного взаимодействия, отделу «Служба одного окна» делегировано постановлением Администрации города Омска от 5 сентября 2011 года № 977-п «Об организации работы по предоставлению документов по принципу «одного окна».

2.3.26.3. Работники отдела «Служба одного окна» на основании поручения Оператора направляют запросы, и принимают информацию, включающую персональные данные субъектов на основании поступивших в СЭДДе запросов от специалистов структурных подразделений Администрации города Омска, уполномоченных на прием документов по принципу «одного окна».

2.3.26.4. Перечень лиц, имеющих право на обработку персональных данных, в том числе имеющих вправо направить запросы о предоставлении информации в СМЭВе, включающей персональные данные субъектов (заявителей) должен быть определен приказом директора Учреждения.

Прекращение действия соглашения с другим оператором является основанием для уничтожения Оператором обработанных персональных данных.

2.3.26.6. При осуществлении деятельности по созданию (замене) и выдаче простой электронной подписи с использованием сервисов Федеральной государственной информационной системы «Единая система идентификации аутентификации инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА), на основании принятия при регистрации условий участников информационной системы в отделе «Служба одного окна» должны быть назначены ответственные лица для участия в информационном взаимодействии, кроме того, действия данных лиц должны быть строго регламентированы, в соответствии с регламентом использования ЕСИА для создания (замены) и выдаче ключей простой электронной подписи.

2.3.27. В случае выявления нарушений порядка обработки персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

2.4. Порядок обработки персональных данных при рассмотрении обращений граждан (жалоб), в том числе от государственных органов,

органов местного самоуправления и должностных лиц Администрации города Омска, иных уполномоченных юридических лиц.

2.4.1. Обработка персональных данных, в данном случае осуществляется посредством муниципальной информационной системы «Система электронного документооборота и делопроизводства Администрации города Омска» на основании распоряжения Администрации города Омска от 09.04.2010 № 162-р «О внедрении системы электронного документооборота и делопроизводства Администрации города Омска», распоряжения Администрации города Омска от 27.10.2011 № 504-р «О системе электронного документооборота и делопроизводства Администрации города Омска», а также распоряжения Администрации города Омска от 18.09.2012 № 337-р «О Порядке работы в системе электронного документооборота и делопроизводства Администрации города Омска».

2.4.2. Операторами информационной системы (сегмента), согласно Постановления Администрации города Омска от 26.03.2021 № 188-п, являются должностные лица, структурных подразделений Администрации города Омска и подведомственных учреждений, участвующие в функционировании сегмента информационной системы при обработке информации или использующие результаты ее функционирования.

2.4.3. Администратором муниципальной информационной системы «Система электронного документооборота и делопроизводства Администрации города Омска» является Казенное учреждение города Омска «Управление информационно-коммуникационных технологий».

2.3.4. При рассмотрении обращений граждан (жалоб), структурным подразделением Администрации города Омска, зарегистрировавшим обращение (жалобу) на основании Постановления Администрации города Омска от 07.02.2013 № 121-п «Об утверждении Порядка организации работы с обращениями граждан в Администрации города Омска» предоставляется доступ к персональным данным граждан.

2.3.5. Работникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными инструкциями сотрудников Учреждения.

2.3.6. Информация может вноситься как в автоматическом режиме при получении персональных данных с Единого портала государственных услуг, Регионального портала государственных и муниципальных услуг или официального сайта Администрации города Омска, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

2.4.7. Обрабатываются следующие категории персональных данных:

1) фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

2) число, месяц, год рождения;

3) место рождения;

4) информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

5) вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

6) адрес места жительства (адрес регистрации, фактического проживания);

7) номер контактного телефона или сведения о других способах связи;

8) реквизиты страхового свидетельства государственного пенсионного страхования;

9) идентификационный номер налогоплательщика;

10) реквизиты страхового медицинского полиса обязательного медицинского страхования;

11) реквизиты свидетельства государственной регистрации актов гражданского состояния;

12) семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

13) фотография;

14) иные персональные данные, необходимые для достижения целей.

2.4.8. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Учреждения, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

-определение угроз безопасности персональных данных при их обработке в информационных системах (сегментах) персональных данных;

-применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах (сегментах) персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

-применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

-оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

-учет машинных носителей персональных данных;

-обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

-восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

-установление правил доступа к персональным данным, разрабатываемым в информационных системах персональных данных

Учреждения, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных Учреждения;

-контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

2.4.9. В случае выявления нарушений порядка обработки персональных данных уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

2.4.10. При обработке персональных данных, вследствие поступивших обращений граждан (жалоб, поручений) резервное копирование не осуществляется.

2.4.11. Доступ в помещение, где производиться обработка персональных данных, должен быть ограничен.

2.4.12. После достижения целей обработки поручения рассмотрения обращения граждан (жалоб) работник Учреждения обязан сделать отметку об исполнении, вследствие чего, работникам Учреждения прекращается доступ к персональным данным.

2.4.13. Категорически запрещено утилизировать документы, содержащие персональные данные путем утилизации в мусор, передачи третьим лицам для утилизации, повторного использования в качестве черновиков.

2.4.14. Категорически запрещается предоставлять доступ к документам и информационным системам (обрабатываемому сегменту), содержащие персональные данные не уполномоченным на то лицам (не работникам Учреждения, участвующих в обработке персональных данных), в том числе специалистам структурных подразделений Администрации города Омска, иных подведомственных учреждений, практикантам и иным лицам.

3. Порядок обеспечения прав субъекта персональных данных

3.1. Сведения предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения Учреждения, осуществляющим обработку соответствующих персональных данных, при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:

-номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

-сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Учреждением, либо сведения, иным образом подтверждающие факт обработки персональных данных в Учреждении, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской

Федерации.

3.2. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

3.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

3.4. Субъекты персональных данных или их представители обладают правами, предусмотренными Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими нормативно-правовыми актами, регламентирующими обработку персональных данных.

3.5. Оператор обеспечивает права субъектов персональных данных в порядке, установленном главами 3 и 4 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.6. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в ч. 1 ст. 15 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.7. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами Российской Федерации, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

3.8. При трансграничной передаче персональных данных их перевод на другие языки осуществляется в порядке, согласованном Оператором с иностранным контрагентом.

4. Обязанности работников оператора

4.1. Работники Оператора:

- осуществляют обработку персональных данных в объеме возложенных на них трудовых обязанностей;

- незамедлительно доводят до сведения ответственного за эксплуатацию информационной системы (сегмента) и администратора безопасности информационной системы (сегмента), ответственного за обработку персональных данных сведения о предполагаемых нарушениях законодательства Российской Федерации, в том числе нормативных правовых актов уполномоченного федерального органа исполнительной власти, и внутренних документов Оператора другими сотрудниками Оператора или контрагентами Оператора.

5. Контроль, ответственность за нарушение или неисполнение Положения

5.1. Контроль за исполнением настоящего Положения возлагается на лицо ответственное за организацию обработки персональных данных.

5.2. Ответственный за обеспечение безопасности обработки персональных данных в Учреждении назначается приказом директора Учреждения.

5.3. Ответственный за организацию обработки персональных данных Учреждения в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящими Положением.

5.4. Ответственный за организацию обработки персональных данных обязан:

-организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Учреждении, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

-осуществлять внутренний контроль за соблюдением работниками Учреждения требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

-в случае нарушения в Учреждении требований к обеспечению защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

5.5. Ответственный за обработку персональных данных вправе:

-иметь доступ к информации, касающейся обработки персональных данных в Учреждении и включающей:

-цели обработки персональных данных;

-категории обрабатываемых персональных данных;

-категории субъектов, персональные данные которых обрабатываются;

-правовые основания обработки персональных данных;

-перечень действий с персональными данными, общее описание используемых в Учреждении способов обработки персональных данных;

-описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии

шифровальных (криптографических) средств и наименования этих средств;

-дату начала обработки персональных данных;

-срок или условия прекращения обработки персональных данных;

-сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

-сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

-привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Учреждении, сотрудников других Учреждений, путем заключения соответствующих договоров, с возложением на них соответствующих обязанностей и закреплением ответственности.

5.6. Ответственный за организацию обработки персональных данных в Учреждении несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в Учреждении в соответствии с Положениями законодательства Российской Федерации в области персональных данных.

5.7. Руководители структурных подразделений Учреждения несут персональную ответственность за неисполнение обязанностей по обработке персональных данных их подчиненными.

Приложение № 3 к приказу директора
от «11» 05 2021 №18-ОД

ПОЛОЖЕНИЕ
об обеспечении защиты информации, обрабатываемой в информационных системах

1. Общие положения

1.1 Настоящее Положение об обеспечении защиты информации, обрабатываемой в информационных системах (далее – Положение), разработано с целью определения единого порядка организации и проведения мероприятий по защите информации, обрабатываемой в Казенном учреждении города Омска «Управление по обеспечению деятельности Администрации города Омска» (далее – Учреждение).

1.2. Положение разработано на основании Постановления Администрации города Омска от 26.03.2021 № 188-п «Об обеспечении защиты информации, обрабатываемой в информационных системах Администрации города Омска», Постановления Администрации города Омска от 26.03.2021 № 189-п «Об утверждении положения об информационно-телекоммуникационной сети Администрации города Омска», Политики Казенного учреждения города Омска «Управление по обеспечению деятельности Администрации города Омска» в отношении обработки и защиты персональных данных, законодательных и иных нормативно правовых актов Российской Федерации, субъектов Российской Федерации, органов местного самоуправления, регламентирующими порядок обработки и защиты персональных данных.

1.3. Администратор безопасности информационной системы (сегмента) – лицо, ответственное за защиту информационной системы (сегмента) от несанкционированного доступа к информации.

1.4. Ответственный за эксплуатацию информационной системы (сегмента) – ответственное лицо, обеспечивающее правильное использование и функционирование системы защиты информации.

2. Цели защиты информации

2.1. Основными целями защиты информации являются:

- исключение неправомерного доступа, копирования, предоставления или распространения информации;
- исключение неправомерного уничтожения или модифицирования информации;
- исключение неправомерного блокирования информации.

3. Меры по обеспечению защиты информации

3.1. Лицом, ответственным за обеспечение защиты информации (администратором безопасности информационной системы) в Учреждении приказом директора назначается работник, в функции которого входят вопросы обеспечения информационной безопасности, контроль за соблюдением норм и правил обработки информации в подразделениях, планирование и организация работ по защите информации, организация обучения пользователей правилам работы на средствах вычислительной техники.

3.2. Для каждой эксплуатируемой в Учреждении информационной системы (сегмента) приказом директора назначается администратор безопасности информационной системы, ответственный за защиту информационной системы (сегмента) от несанкционированного доступа к информации.

3.3. Ответственный за эксплуатацию информационной системы назначается приказом директора из числа работников подразделения и обеспечивает правильное использование и функционирование системы защиты информации.

3.4. Меры защиты информации информационной системы (сегмента) определяются в зависимости от класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации, в соответствии с нормативными правовыми актами Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службы безопасности Российской Федерации.

3.5. Классификацию информационной системы проводит комиссия по классификации информационной системы, созданная в Учреждении.

3.6. Классификация информационной системы проводится в зависимости от значимости обрабатываемой в ней информации и масштаба информационной системы. Класс защищенности определяется для информационной системы в целом и при необходимости для ее отдельных сегментов. Класс защищенности сегмента не должен быть выше класса защищенности центрального сегмента информационной системы. Результаты классификации информационной системы (сегмента) оформляются актом классификации, который утверждается руководителем подразделения.

3.7. Для проведения классификации необходимо руководствоваться постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3.8. Модель угроз безопасности информации разрабатывается на основе определения угроз безопасности информации, реализация которых

может привести к нарушению безопасности информации в информационной системе (сегменте), и утверждается директором Учреждения в соответствии с методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 14.02.2008.

3.9. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы (сегмента), возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

3.10. При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

3.11. Обеспечение защиты информации осуществляется с помощью комплекса организационных и технических мер.

3.12. К организационным мерам обеспечения защиты информации относятся:

1) разработка и утверждение в Учреждении следующих организационно-распорядительных документов по защите информации информационной системы (сегмента):

- инструкция администратора безопасности;
- инструкция пользователя;
- инструкция по организации парольной защиты;
- инструкция по проведению антивирусного контроля;
- инструкция ответственного за эксплуатацию;
- инструкция о порядке технического обслуживания средств обработки информации;
- порядок проведения проверки в случае наступления инцидента информационной безопасности;
- порядок учета съемных носителей информации;
- порядок резервного копирования данных;

2) ведение учета программных, программно-аппаратных средств защиты информации, включая криптографические средства защиты;

3) создание комиссии по классификации информационной системы и разработка указанной комиссией акта классификации, его утверждение директором Учреждения;

4) разработка рабочей группой по обеспечению защиты информации, созданной в Учреждении и утверждение директором Учреждения для каждой

информационной системы (сегмента):

- модели угроз безопасности информации;
- описания технологического процесса обработки защищаемой информации;
- перечней разрешенного к использованию программного обеспечения;
- перечней защищаемых ресурсов;
- списка лиц, допущенных к самостоятельной работе (пользователей) в информационной системе (сегменте);
- списка лиц, имеющих право доступа в помещение, в котором проводится обработка защищаемой информации;
- списка лиц, допущенных к техническому обслуживанию;
- списка установленных прав доступа пользователей к защищаемым ресурсам.

3.13 Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности в соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации», Федеральным законом «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», методическим документом ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».

На основании Договора № 9 от 20.08.2012, заключенного между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска» и Казенным учреждением города Омска «Управление информационно-коммуникационных технологий» по проведению мероприятий по технической защите информационной системы персональных данных 1С Предприятие, Договора № 125 от 08.11.2012, заключенным между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска и Казенным учреждением города Омска "Управление информационно-коммуникационных технологий" на оказание услуг по техническому сопровождению и обслуживании информационно-коммуникационных систем и их компонентов, программного обеспечения и аппаратных средств, договора № 141 от 10.12.2012, заключенного между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска» и Казенным учреждением

города Омска «Управление информационно-коммуникационных технологий» по проведению работ по технической защите сегмента «Службы одного окна» муниципальной информационной системе «Система электронного документооборота и делопроизводства Администрации города Омска» Учреждение реализуют следующие технические меры:

- применение лицензионного программного обеспечения, а также сертифицированных по требованиям безопасности информации программных и технических средств защиты информации;
- аттестация средств вычислительной техники и информационных систем, в случае, если информационные системы является муниципальными информационными системами;
- исключение несанкционированного доступа к информации, обрабатываемой в информационных системах, путем идентификации и аутентификации пользователей;
- опломбирование средств вычислительной техники с целью предотвращения несанкционированного доступа, изъятия и замены комплектующих элементов и узлов;
- исключение использования в информационно-коммуникационной сети систем обмена мгновенными сообщениями, не сертифицированными по требованиям безопасности, через сеть Интернет (WhatsApp, Skype, Viber и т.п.);
- исключение публичных адресов сети Интернет в информационно-телекоммуникационной сети;
- обеспечение доступа к сети Интернет с использованием прокси-сервера с ведением журнала фиксации событий по учетным записям пользователей и IP-адресам;
- мониторинг и анализ зарегистрированных событий, связанных с обеспечением безопасности, включая запросы к ресурсам в сети Интернет, а также электронной почты;
- создание в локальной вычислительной сети контроллера домена;
- обнаружение (предотвращение) вторжений, направленных на преднамеренный несанкционированный доступ к информации, а также реагирование на эти действия (пресечение), и последующее документирование информации об инциденте информационной безопасности;
- защита среды виртуализации;
- защита машинных носителей информации (средств обработки (хранения) информации, съемные машинные носители информации);
- проведение списания и утилизации средств вычислительной техники только после удаления содержащейся в них информации без возможности ее восстановления и последующего прочтения;
- резервное копирование информации;
- антивирусный контроль программного обеспечения, получаемой и передаваемой информации, а также обновление антивирусных программных средств;

- обновление используемого программного и прикладного обеспечения, включая обновление программного обеспечения средств защиты информации;

- осуществление передачи защищаемой информации по открытым каналам связи только с использованием средств криптографической защиты информации;

- создание в служебных целях защищенного удаленного соединения для дистанционного подключения к информационным системам.

3.15. Подключение к ресурсам информационно-телекоммуникационной сети регламентируется Положением об информационно-телекоммуникационной сети Администрации города Омска, утвержденным Постановлением Администрации города Омска от 26.03.2021 № 189-п.

В Учреждении осуществление функций по обеспечению организационных мер защиты возлагается на лицо, ответственное за обеспечение защиты персональных данных.

В соответствии с Договором № 9 от 20.08.2012, заключенным между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска» и Казенным учреждением города Омска «Управление информационно-коммуникационных технологий» по проведению мероприятий по технической защите информационной системы персональных данных 1С Предприятие, Договором № 125 от 08.11.2012, заключенным между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска и Казенным учреждением города Омска "Управление информационно-коммуникационных технологий" на оказание услуг по техническому сопровождению и обслуживании информационно-коммуникационных систем и их компонентов, программного обеспечения и аппаратных средств, Договором № 141от 10.12.2012, заключенным между Казенным учреждением города Омска «Управление по обеспечению деятельности Администрации города Омска» и Казенным учреждением города Омска «Управление информационно-коммуникационных технологий» по проведению работ по технической защите сегмента «Службы одного окна» муниципальной информационной системе «Система электронного документооборота и делопроизводства Администрации города Омска» обеспечение технических мер защиты информации возлагается на работников Казенного учреждения города Омска "Управление информационно-коммуникационных технологий".

4. Контроль за обеспечением защиты информации

4.1. Контроль за обеспечением защиты информации осуществляется с целью предотвращения несанкционированного доступа к защищаемой информации, оценки полноты и эффективности применяемых мер и средств защиты информации.

4.2. Организация и контроль за обеспечением защиты информации,

обрабатываемой в информационных системах (сегментах) в Учреждении, осуществляется самостоятельно.

4.3. По итогам осуществления контроля за обеспечением защиты информации в Учреждении в срок до 1 ноября текущего года готовится справка, в которой отображается:

- общее состояние обеспечения защиты информации информационных систем (сегментов) учреждений;
- количество проведенных проверок;
- основные недостатки, выявленные в ходе проверок;
- укомплектованность учреждений специалистами по обеспечению защиты информации;
- предложения по совершенствованию системы обеспечения защиты информации.

Приложение № 4 к приказу директора от
«11» 05 2021 №18 -ОД

ПОЛОЖЕНИЕ
о системе межведомственного электронного взаимодействия

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Постановлением Администрации города Омска от 26.03.2021 № 188-п «Об обеспечении защиты информации, обрабатываемой в информационных системах Администрации города Омска», Постановлением Администрации города Омска от 26.03.2021 № 189-п «Об утверждении положения об информационно-телекоммуникационной сети Администрации города Омска», Решением Коллегии Государственной технической комиссии России № 7.2/02.03.2001 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Политикой Казенного учреждения города Омска «Управление по обеспечению деятельности Администрации города Омска», утвержденной приказом директора.

1.2. Положение определяет назначение и правила использования государственной информационной системы Омской области «Система межведомственного электронного взаимодействия» в отделе «Служба одного окна» Казенного учреждения города Омска «Управление по обеспечению деятельности Администрации города Омска», а также порядок осуществляемого с ее применением информационного обмена между государственными органами, органами местного самоуправления, государственными и муниципальными учреждениями, многофункциональными центрами, иными органами и организациями, в целях предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме по принципу «одного окна».

1.3. В настоящем Положении используются следующие термины и определения:

- межведомственное электронное взаимодействие - обмен информацией, а также регламентированное предоставление доступа к информационным системам, подключенным к государственной информационной системе Омской области «Система межведомственного электронного взаимодействия» с использованием средств электронной подписи, в результате применения которых можно однозначно определить (идентифицировать) участников межведомственного электронного взаимодействия, правомочность действий, дату и время осуществления такого взаимодействия, а также гарантировать идентичность информации, отправленной одним участником межведомственного электронного взаимодействия и полученной другим;

- участники межведомственного электронного взаимодействия - органы и организации, включенные в государственную информационную систему Омской области «Система межведомственного электронного взаимодействия»;

- электронный сервис - регламентированный вид автоматического обмена информацией, обеспечивающий возможность доступа через государственную информационную систему Омской области «Система межведомственного электронного взаимодействия» к информационным системам других государственных органов, органов местного самоуправления, государственных и муниципальных учреждений, многофункциональными центрами, иными органами и организациями;

- основные виды электронных сервисов, предоставляемых системой межведомственного взаимодействия:

- получение запрашиваемой информации из информационной системы, подключенной к государственной информационной системе Омской области «Система межведомственного электронного взаимодействия»;

- передача информации в информационную систему, подключенную к государственной информационной системе Омской области «Система межведомственного электронного взаимодействия»;

- передача запроса на получение информации и обработка данных;

- регламент (порядок) функционирования государственной информационной системы Омской области «Государственный удостоверяющий центр Омской области» – описание технологического процесса межведомственного электронного взаимодействия с поддержкой автоматического и автоматизированных режимов в рамках оказания государственных и муниципальных услуг с использованием государственной информационной системы Омской области «система межведомственного электронного взаимодействия»;

- обладатель информации - лицо, самостоятельно создавшее информацию.

- доступ к информации - возможность получения информации и ее использования;

- конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам;

-предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

- распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

- электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

- электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или

обработки в информационных системах;

- электронная подпись - реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи, а в случае успешной проверки подтвердить факт подписания электронного документа;

- служебная информация ограниченного распространения - несекретная информация, касающаяся деятельности учреждения, ограничения, на распространение которой диктуются необходимостью при оказании государственных и муниципальных услуг;

- безопасность информации - состояние защищенности информации, характеризуемое способностью работников учреждения, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами;

- сертификат ключа проверки электронной подписи – электронный документ и (или) документ на бумажном носителе, выданные удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

- средства криптографической защиты информации – программное обеспечение или программно аппаратный комплекс, с помощью которых происходит шифрование информации и передача их по сети интернет;

- удостоверяющий центр – организация, подтверждающая принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2. Обязанности пользователей информационной системы

2.1. Пользователь информационной системы обязан:

- запрашивать с использованием государственной информационной системы Омской области «Система межведомственного электронного взаимодействия» (далее – СМЭВ) информацию в строго установленном объеме, предусмотренными Постановлением Администрации города Омска от 05.09.2011 № 977-п «Об организации работы по предоставлению документов по принципу «одного окна», регламентом работы по предоставлению документов по принципу «одного окна» от 15.09.2011, утвержденным исполняющим обязанности управляющего делами Администрации города Омска, председателем рабочей группы Администрации города Омска по организации работы по принципу «одного окна», иными Административными регламентами;

- обеспечивать достоверность сведений при подаче заявлений, запросов и обращений;

- в случае установления недостоверности сведений или ошибке обеспечивать их изменение и информировать об этом изменении заинтересованных участников межведомственного электронного взаимодействия;

- обеспечивать сохранность, целостность и неизменность полученных ответов на запросы, выписки и иные документы;

- обеспечивать работоспособность и безопасность вверенных пользователю информационной системы программно-аппаратных средств, необходимых для функционирования электронных сервисов СМЭВ, в соответствии с требованиями регламента СМЭВ;

- обеспечивать строгое соблюдение установленного законодательством Российской Федерации порядка ограниченного доступа к отдельным видам информации, получаемой и передаваемой при помощи СМЭВ, в том числе к персональным данным граждан;

- не производить действия, направленные на нарушение информационной безопасности электронных сервисов СМЭВ, или информационных систем иных органов и организаций (деструктивные действия).

3. Права пользователей информационной системы

3.1. Пользователь информационной системы имеет право:

- получать с использованием СМЭВ информацию о статистике использования электронных сервисов пользователем, о ходе предоставления государственных (муниципальных) услуг и исполнения государственных (муниципальных) функций, выполнения электронных регламентов от оператора СМЭВ;

- вносить предложения о необходимых улучшениях в части функционирования СМЭВ;

- обращаться в сервис технической поддержки СМЭВ через работников сектора развития отдела информационных систем Казенного учреждения города Омска «Управление информационной-коммуникационных технологий».

4. Условия и порядок обращения пользователей информационной системы с электронной подписью и средствами криптографической защиты информации

4.1. Носители, содержащие сертификат ключа проверки электронной подписи, относятся к материальным носителям, содержащим служебную информацию ограниченного распространения.

При обращении с ними должны выполняться требования регламента удостоверяющего центра и иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения.

4.2. При работе со средствами криптографической защиты информации и электронной подписи пользователям информационной системы запрещается:

– снимать несанкционированные копии с носителей ключевой информации или переписывать с них файлы на иные носители информации (ленты стримера, лазерные диски, жесткие диски, флеш-карты и т.п.);

– передавать носители ключевой информации или знакомить с их содержанием посторонних лиц;

– выводить закрытые ключи электронной подписи на монитор или принтер;

– оставлять без присмотра носители ключевой информации;

– использовать электронные носители ключевой информации на неисправных устройствах считывания информации;

– устанавливать носители ключевой информации в считывающие устройства в режимах, не предусмотренных технологическим процессом формирования электронного документа, а также в другие рабочие станции, не задействованные в системе электронного документооборота;

– записывать на носитель ключевой информации постороннюю информацию.

5. Порядок и условия использования ключей электронной подписи пользователями информационной системы

5.1. Владельцы электронной подписи несут персональную ответственность за безопасность собственных ключей электронной подписи и обязаны обеспечивать их сохранность и неразглашение.

5.2. Пользователи информационной системы обязаны хранить носители ключевой информации в хранилищах (сейфах, ящиках, шкафах, столах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.3. Дата ввода электронной подписи в обращение указывается в сертификате ключа проверки электронной подписи.

5.4. Пользователь информационной системы получает право использования соответствующего закрытого ключа электронной подписи для подписи электронного документа с момента регистрации сертификата ключа проверки электронной подписи, но не ранее даты ввода в обращение, указанной в сертификате проверки ключа электронной подписи.

5.5. Сертификат пользователя информационной системы доступен всем участникам системы электронного документооборота после его опубликования в реестре сертификата проверки ключа электронной подписи.

5.6. Формирование новых ключей электронной подписи и сертификата ключа проверки электронной подписи осуществляется в соответствии с регламентом удостоверяющего центра.

5.7. После окончания срока действия сертификата ключа проверки электронной подписи его владелец прекращает использование соответствующих закрытых ключей электронной подписи.

6. Порядок действий при компрометации закрытых ключей электронной подписи

6.1. К случаям компрометации закрытых ключей электронной подписи относятся:

– потеря носителей ключевой информации;

– потеря носителей ключевой информации с их последующим обнаружением;

– носители ключевой информации стали на время доступными постороннему лицу без контроля со стороны владельца или ответственного за хранение ключевой информации.

6.2. В случае компрометации ключей электронной подписи администратор безопасности информации проводит служебное расследование с оформлением акта. Акт проверки совместно с заявлением об аннулировании сертификата ключа проверки электронной подписи предоставляется в удостоверяющий центр.

6.3. К случаям подозрения на компрометацию закрытых ключей электронной подписи относятся:

– возникновение подозрений утечки информации или ее искажения в СМЭВ или муниципальной информационной системе «Система электронного документооборота и делопроизводства Администрации города Омска;

– наличие следов повреждений запорных устройств помещений, где производится обработка персональных данных в информационных системах с носителями ключевой информации и (или) наличие следов несанкционированного проникновения в данные помещения.

6.4. Дата и время, когда сертификат ключа проверки электронной подписи считается недействительным в СМЭВ, устанавливается равной дате и времени публикации списка отозванных сертификатов ключей проверки электронной подписи, в который был включен отзываемый сертификат.

6.5. При получении электронного документа, подписанного скомпрометированным закрытым ключом электронной подписи, данный электронный документ считается недействительным.

6.6. В случае компрометации закрытого ключа электронной подписи проводятся мероприятия по формированию нового ключа в соответствии с Регламентом (порядком) функционирования государственной информационной системы Омской области «Государственный удостоверяющий центр Омской области».

7. Обязанности администратора безопасности информации

7.1. Основными задачами администратора безопасности информации являются:

- организация эксплуатации технических и программных средств защиты информации;

- текущий контроль работы средств и систем защиты информации;

- контроль за работой пользователей информационных систем, выявление и регистрация попыток несанкционированного доступа к информационным системам и защищаемым информационным ресурсам.

7.2. Администратор информационной безопасности обязан:

- организовать обеспечение и поддержание в работоспособном состоянии средств и систем защиты информации;
- совместно со специалистами подразделения по технической защите информации принимать меры по восстановлению работоспособности средств и систем защиты информации;
- оказывать содействие работникам подразделения по технической защите информации в проведении работ по анализу защищенности автоматизированных систем;
- проводить инструктаж пользователей информационной системы по правилам работы с используемыми средствами и системами защиты информации;
- после окончания срока действия сертификата электронной подписи, произвести стирание записанной на них ключевой информации или уничтожить ключевые носители информации, при необходимости, составить акт уничтожения (стирания) ключевых носителей информации;
- при подозрении компрометации или компрометации закрытого ключа электронной подписи пользователя информационной системы немедленно прекратить использование владельцем соответствующего закрытого ключа и сообщить об этом уполномоченному лицу удостоверяющего центра;
- в случае компрометации закрытых ключей электронной подписи провести служебное расследование с оформлением акта, который, совместно с заявлением об аннулировании сертификата ключа проверки электронной подписи предоставить в удостоверяющий центр;
- несет персональную ответственность за наличие на средствах вычислительной техники пользователей информационной системы программно – технически и криптографических средств защиты информации, а также их исправное функционирование.

8. Права администратора безопасности информации

8.1. Администратор безопасности информации имеет право:

- обращаться в сервис технической поддержки СМЭВ с просьбой об оказании технической и методической помощи в работе по обеспечению технической защиты информации;
- вносить предложения о необходимых улучшениях в части функционирования СМЭВ;
- обращаться к руководителю с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;

- докладывать непосредственному руководителю о выявленных нарушениях и несанкционированных действиях пользователей информационной системы, принимать необходимые меры по устранению нарушений.

9. Ответственность

9.1. За неисполнение или ненадлежащее исполнение обязанностей пользователь информационной системы несет ответственность в установленном действующим законодательством порядке.

9.2. За разглашение служебной информации ограниченного распространения ставшей известными в соответствии с родом работы пользователь информационной системы несет ответственность в установленном действующим законодательством порядке.

Приложение № 5 к приказу директора
от «11» 05 2021 № 18 -ОД

ПОЛОЖЕНИЕ
об осуществлении деятельности по созданию (замене) и выдаче простой электронной подписи с использованием сервисов Федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА)

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральным законом Российской Федерации от 05.05.2014 № 110-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации»;
- Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральным законом Российской Федерации от 04.07.2014 № 149-ФЗ «О внесении изменений в Закон Российской Федерации «Об организации страхового дела в Российской Федерации» и отдельные законодательные акты Российской Федерации»;
- Государственной программой Российской Федерации «Информационное общество (2011 – 2020 годы)», утвержденной распоряжением Правительства Российской Федерации от 20.10.2010 № 1815-р;
- Постановлением Правительства Российской Федерации от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;
- Постановлением Правительства Российской Федерации от 28.12.201 № 1184 «О мерах по обеспечению перехода федеральных органов исполнительной власти и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде»;
- Постановлением Правительства Российской Федерации от

09.02.2012 № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке её использования, а также об установлении требований к обеспечению совместимости средств электронной подписи»;

- Постановлением Правительства Российской Федерации от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг»;

- Постановлением Правительства Российской Федерации от 10.07.2013 № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно - технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;

- Распоряжением Правительства Российской Федерации от 15.09.2009 № 1475-р «Об определении ОАО «Ростелеком» единственным исполнителем работ по эксплуатации инфраструктуры электронного правительства – единым национальным оператором инфраструктуры электронного правительства»;

- Регламентом информационного взаимодействия Участников с Оператором ЕСИА и Оператором эксплуатации инфраструктуры электронного правительства (Приложение 18 к протоколу заседания Подкомиссии по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 13.05.2016 № 168пр).

Положение об информационном взаимодействии участников с оператором ЕСИА и оператором эксплуатации инфраструктуры электронного правительства предназначено для формализации ответственности участников, задействованных в обеспечении и поддержании процессов в рамках информационно -технологического взаимодействия информационных систем с использованием.

2. Термины и сокращения

Термин	Определение
Администратор профиля государственной организации	Уполномоченное должностное лицо Заявителя, которое является пользователем ЕСИА и обладает полномочиями по ведению профиля государственной организации в ЕСИА
Аутентификация	Процедура идентификации и установления подлинности источника информации
ДЛ	Должностное лицо
ДУЛ	Документ, удостоверяющий личность

ЕПГУ	Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг
ЕСИА	Федеральная государственная информационная система «Единая система идентификации аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ИНН	Идентификационный номер налогоплательщика
ИС	Информационная система Заявителя
ИСПДн	Информационная система персональных данных
ИС ГУЦ	Федеральная государственная информационная система «Информационная система головного удостоверяющего центра»
КЭП	Усиленная квалифицированная электронная подпись
Метаданные	Специальный файл, описывающий конфигурационные данные ИС. Для описания используется язык XML
Оператор выдачи ключа ПЭП	Орган или организация, обладающая правом создания (замены) ключа ПЭП в соответствии с постановлением Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг». В соответствии с указанным постановлением Правительства, в качестве Операторов выдачи ключа ПЭП могут выступать: а) федеральные органы исполнительной власти; б) государственные внебюджетные фонды; в) органы исполнительной власти субъектов Российской Федерации; г) органы местного самоуправления; д) государственные и муниципальные учреждения; е) многофункциональные центры предоставления государственных и муниципальных услуг; ж) иные организации, определенные федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации (а также уполномоченные ими организации), осуществляющие оказание государственных или муниципальных услуг и подключенные к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме. Также в качестве Операторов выдачи ПЭП могут выступать организации, определенные Федеральными законами Российской Федерации от 0 5.05.2014 № 110-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» и от 4 июня 2014 г. № 149-ФЗ «О внесении изменений в Закон Российской Федерации «Об

ОГВ	Орган государственной власти
ОГРН	Основной государственный регистрационный номер
Оператор ЕСИА	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Оператор ИС	Организация, осуществляющая регистрацию и управление ИС. В качестве операторов ИС, включенных в регистр информационных систем ЕСИА, могут быть организации, обеспечивающие решение следующих задач: - предоставление государственных и муниципальных услуг; -исполнение государственных и муниципальных функций; - формирование БГИР; - межведомственное электронное взаимодействие; - иные задачи, предусмотренные федеральными законами, актами Президента РФ и актами Правительства РФ. В качестве Операторов ИС могут выступать: а) федеральные органы исполнительной власти; б) государственные внебюджетные фонды; в) органы исполнительной власти субъектов Российской Федерации; г) органы местного самоуправления; д) государственные и муниципальные учреждения; е) многофункциональные центры предоставления государственных и муниципальных услуг; ж) иные организации, определенные федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации (а также уполномоченные ими организации), осуществляющие оказание государственных или муниципальных услуг и подключенные к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме. Также в качестве Операторов ИС могут выступать организации, определенные Федеральными законами Российской Федерации от 05.05.2014 № 110-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» и от 0 4.06.2014 № 149-ФЗ «О внесении изменений в Закон Российской Федерации «Об организации страхового дела в Российской Федерации» и отдельные законодательные акты Российской Федерации»
Оператор эксплуатации ИЭП	Единый национальный оператор эксплуатации инфраструктуры электронного правительства – ОАО «Ростелеком» (в соответствии с распоряжением Правительства Российской Федерации от 15.10.2009 №1475-р)
ПО	Программное обеспечение
Пользователь ЕСИА	Пользователь информационно-телекоммуникационной сети «Интернет», зарегистрированный в ЕСИА в качестве физического лица. Может иметь роли индивидуального предпринимателя, сотрудника юридического лица, должностного лица государственного учреждения

Поставщик услуг	ИС, интегрированная с ЕСИА и осуществляющая предоставление пользователям ЕСИА данных и услуг, в частности, государственных и муниципальных услуг в электронной форме
ПЭП	Простая электронная подпись
Регистр ЕСИА	Перечень учетных записей, хранящихся в ЕСИА. В ЕСИА предусмотрены следующие регистры: а) физических лиц; б) юридических лиц; в) должностных лиц органов и организаций; г) органов и организаций; д) органов и организаций, имеющих право создания (замены) и выдачи ключа ПЭП; е) информационных систем
Регламент	Регламент взаимодействия участников информационного взаимодействия с оператором ЕСИА и оператором инфраструктуры электронного правительства при организации информационно-технологического взаимодействия информационных систем с использованием ЕСИА
СМЭВ	Федеральная государственная информационная система «Единая система межведомственного электронного
СНИЛС	Страховой номер индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда России
Специалист центра обслуживания	Сотрудник Оператора выдачи ключа ПЭП, осуществляющий подтверждение личности пользователей ЕСИА
УЛ	Уполномоченное лицо, наделенное правом от лица организации формировать и направлять заявки в целях подключения к инфраструктуре взаимодействия (в соответствие с Постановлением Правительства РФ от
Участник информационного взаимодействия	Орган или организация имеющая право использования ЕСИА в соответствии с требованиями действующих нормативных правовых актов
Заявитель	Заявитель – это организация, использующая или планирующая использовать ЕСИА одним из предусмотренных способов. В роли Заявителя могут выступать следующие органы и организации: а) федеральные органы исполнительной власти, б) государственные внебюджетные фонды, в) органы исполнительной власти субъектов Российской Федерации, г) органы местного самоуправления, д) государственные и муниципальные учреждения, многофункциональных центров предоставления государственных и муниципальных услуг, е) иные организации, определенные федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации Также в качестве Заявителей (в целях проведения идентификации физических лиц) могут выступать организации, ФЗ «О внесении изменений в Закон Российской Федерации «Об организации страхового дела в Российской Федерации» и

Учетная запись	Набор сведений о пользователе, организации или информационной системе, хранимый в ЕСИА в электронном виде
ФИО	Фамилия, имя, отчество
ФРГУ	Федеральный реестр государственных и муниципальных услуг
Центр обслуживания (ЦО)	Центр обслуживания органа или организации, имеющей право создания (замены) и выдачи ключа ПЭП. В Центре обслуживания специалистами Центра обслуживания осуществляется регистрация и/или подтверждение личности пользователей

3. Условия использования ЕСИА с целью создания (замены) и выдачи ключей простой электронной подписи

3.1. Отдел «Служба одного окна» Казенное учреждение города Омска «Управление по обеспечению деятельности Администрации города Омска» осуществляя деятельность по созданию (замене) и выдаче ПЭП с использованием сервисов ЕСИА является Центром обслуживания пользователей ЕСИА (далее – Центр обслуживания пользователей ЕСИА).

3.2. Участник информационного взаимодействия гарантирует, что групповое использование КЭП, выданного на одно должностное лицо иными работниками Центра обслуживания пользователей ЕСИА запрещено.

3.3. При работе с ЕСИА работниками Центра обслуживания пользователей ЕСИА осуществляется проверка подлинности и действительности ДУЛ предъявленного заявителем (в том числе проверка документа техническими средствами на соответствие требованиям, утвержденным МВД к паспорту гражданина РФ, а также проверка на подлинность для паспортов иностранных граждан на предмет целостности и наличия на нем защитных средств).

3.4. Во всех случаях, если имеется основания полагать, что ДУЛ недействителен (в том числе его просрочка), либо в случаях, когда не представляется возможным достоверно сопоставить принадлежность паспорта к заявителю, то в оказании услуги должно быть отказано.

3.5. Ввод в ЕСИА данных заявителей вноситься в полном соответствии с оригиналом предоставленных документов, внесение сведений на основании заявления без сличения соответствия сведений не осуществляется.

3.6. Услуги по созданию (замене) и выдаче ПЭП (регистрация в ЕСИА) заявителям оказывается бесплатно.

3.7. За несоблюдение требований настоящего Положения работники Центра обслуживания пользователей ЕСИА подлежат привлечению к ответственности согласно требованиям действующего законодательства.

3.8. В случае выявления оператором ЕСИА признаков нарушения пунктов Регламента ЕСИА, Методических рекомендаций, а также руководства пользователей и сервиса ЕСИА в СМЭВ участник должен провести внутреннюю проверку.

3.9. Работники Центра обслуживания пользователей ЕСИА должны ознакомиться с нормативно-правовыми актами электронного правительства,

ЕСИА, ЕПГУ, владеть действующей документацией.

3.10. Лица, участвующие в регистрации ЕСИА или выдачи ПЭП должны быть работниками Отдел «Служба одного окна» Казенное учреждение города Омска «Управление по обеспечению деятельности Администрации города Омска».

3.11. Для обеспечения безопасности данных, обрабатываемых при информационном взаимодействии с ФГИС ЕСИА необходимо использовать средства криптографической информации класса КС1 и выше, прошедшие сертификацию на соответствие требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27.12.2010 № 796, а также средства антивирусной защиты, прошедшие сертификацию на соответствие требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК России от 20.03.2012 № 28.

3.12. Нарушение требований и условий, содержащихся в настоящем разделе, может повлечь отключение от сервисов и интерфейсов ЕСИА.

3.13. Право выдачи ПЭП может быть отозвано по усмотрению Оператора эксплуатации ИЭП или оператора ИЭП, если имеются признаки нарушений требований, действующих нормативных правовых актов, в том числе Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 27.07.2006 № 152-ФЗ « О персональных данных», Постановления Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг», Приказа Минкомсвязи России от 13.04.2012 № 107 «Об утверждении Положения о федеральной государственной информационной системе « Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

3.14. Участник информационного взаимодействия обязуется не хранить, не обрабатывать, не передавать и не собирать (в том числе от самих пользователей) информацию о паролях пользователей ЕСИА.

3.15. Участник информационного взаимодействия обязуется принимать заявления от заявителей исключительно силами Отдела «Служба одного окна» Казенного учреждения города Омска «Управление по обеспечению деятельности Администрации города Омска».

3.16. Создание, выдача (замена) ПЭП работниками Оператора выдачи ПЭП за пределами офисов (помещений) Центра обслуживания пользователей ЕСИА выдачи ПЭП запрещены.

3.17. Центр обслуживания пользователей ЕСИА не в праве:

- Выполнять операции без Личного присутствия заявителя, в том числе по телефону, email и т.д.;

- Использовать недокументированные в РП функции предоставляемого ПО и сервисов;

- Использовать функционал ЕСИА для получения доступа к

персональным данным пользователя;

- Регистрировать пользователя с использованием контактов, полученных от иного лица (не являющегося владельцем указываемых при обращении к ЕСИА персональных данных);

- Предоставлять доступ к предоставляемому Оператором ЕСИА ПО, интерфейсам и сервисам ЕСИА третьим лицам;

- Осуществлять передачу функции приёма заявлений, подтверждения личности, доступа к АРМ ЕСИА и сервису ЕСИА в СМЭВ, функцию открытия ЦО или выполнение иных операций в рамках регистрации в ЕСИА или выдачи ПЭП в иные организации, ИП, подведомственные учреждения или иным лицам, не являющимися работниками зарегистрированного действующего оператора выдачи ПЭП.

3.18. Минкомсвязь России, как оператор ИС, имеет право заблокировать Центр обслуживания ЕСИА на время проведения расследования в случае, если в рамках плановых работ по аудиту безопасности учетных записей (или Центров обслуживания, выполняющих операции регистрации/восстановления доступа) ЕСИА была зафиксирована подозрительная активность с учетными записями или при обращении к сервисам ЕСИА.

3.19. В случае не согласия Участника информационного взаимодействия с требованиями настоящего раздела, он обязан прекратить взаимодействие с ЕСИА и направить в установленном порядке в Минкомсвязь России и Оператору эксплуатации ИЭП уведомление о несогласии.

4. Распространённые задачи и сценарии их решения

Задача	Шаги
Зарегистрировать учетную запись органа государственной власти (ОГВ)	Зарегистрировать ОГВ согласно п. 4 Регламента[1].
Подключиться к ЕСИА с целью идентификации и аутентификации пользователей своей системы (вход через Госуслуги)	– зарегистрировать в промышленной среде ЕСИА орган/организацию согласно п. 4 Регламента; – зарегистрировать в промышленной ЕСИА ИС согласно п. 6 Регламента; – подключить ИС к тестовой среде ЕСИА согласно п. 9 Регламента и произвести интеграцию с тестовой средой ЕСИА[2]. Обращаем внимание на то, что регистрация ИС в тестовой среде ЕСИА и загрузка сертификата ИС в профиль системы выполняется сотрудниками СТП в рамках выполнения заявки на подключение; – подключить ИС к промышленной среде ЕСИА согласно п. 10 Регламента

Подключиться к ЕСИА с целью внесения информации о выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключа проверки электронной подписи (только для удостоверяющих центров)	– зарегистрировать удостоверяющий центр в ЕСИА согласно п. 4 Регламента; – зарегистрировать ИС в промышленной ЕСИА согласно п. 6 Регламента; – подключить ИС к тестовой среде ЕСИА согласно п. 9 Регламента и провести интеграцию с тестовой средой ЕСИА; Обращаем внимание на то, что регистрация ИС в тестовой среде ЕСИА и загрузка сертификата ИС в профиль системы выполняется сотрудниками СТП в рамках выполнения заявки
	– подключить ИС к промышленной среде ЕСИА согласно п. 9.4 Регламента
Подключиться к промышленной и тестовой среде ЕСИА для регистрации пользователей ЕСИА в Центрах обслуживания	– зарегистрировать орган/организацию согласно п. 4 Регламента; – зарегистрировать ИС согласно п. 6 Регламента; – получить согласование права использования ЕСИА и обеспечить включение своей организации в регистр органов и организаций, имеющих право создания (замены) и выдачи ключа ПЭП согласно п. 12 Регламента; – зарегистрировать свои центры обслуживания согласно п. 14 Регламента. Обращаем внимание на то, что в рамках выполнения заявки на предоставление доступа к сервису выдачи ПЭП, организация получает доступ к сервисам как в промышленной, так и в тестовой средах, а также получает инструкцию по работе с сервисом в тестовой среде. Подача заявок на подключение в соответствии с п. 9, 10 Регламента не требуется
Подключиться к Единому сервису упрощенной идентификации в промышленной и тестовой средах (только для субъектов исполнения Федеральным законом 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»)	– зарегистрировать организацию согласно Руководству пользователя ЕСИА[3]; – зарегистрировать ИС согласно п. 6 Регламента; – получить согласование права использования Единого сервиса упрощенной идентификации согласно п. 13 Регламента. Обращаем внимание на то, что в рамках выполнения заявки на предоставление доступа к Единому сервису упрощенной идентификации,
Подключиться к промышленной и тестовой среде ЕСИА для обеспечения возможности импорта в ЕСИА учетных записей других ИС	– зарегистрировать в промышленной среде ЕСИА орган/организацию согласно п. 4 Регламента; – зарегистрировать в промышленной среде ЕСИА ИС согласно п. 6 Регламента; – получить согласование права использования ЕСИА и обеспечить включение своей организации в регистр органов и организаций, имеющих право создания (замены) и выдачи ключа ПЭП согласно п. 12 Регламента;

	– подключить ИС к тестовой среде ЕСИА согласно п. 9 Регламента[4] и произвести интеграцию с тестовой средой ЕСИА[5]. – подключить ИС к промышленной среде ЕСИА согласно п. 9.4 Регламента[6]. Обращаем внимание на то, что регистрация ИС в тестовой среде ЕСИА и загрузка сертификата ИС в профиль системы выполняется сотрудниками СТП в рамках выполнения заявки на подключение.