ПОЛИТИКА
в области обеспечения безопасности персональных данных, обрабатываемых в МКУ «Дирекция Наукограда» города Фрязино

1. Общие положения

1.1. Настоящая Политика в области обеспечения безопасности персональных данных (далее – Политика), обрабатываемых в МКУ «Дирекция Наукограда» города Фрязино (далее - Дирекция), разработана в соответствии с положениями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящая Политика устанавливает правила и процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований, правила рассмотрения запросов субъектов персональных данных или их представителей, а также правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.3. Обработка персональных данных в Дирекции осуществляется в целях: обеспечения кадровой работы и соблюдения трудовых прав сотрудников Дирекции; реализации прав и обязанностей Дирекции как юридического лица.

1.4. Обработка персональных данных в Дирекции выполняется с использованием средств автоматизации или без использования таких средств и включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в Дирекции.

1.5. Субъектами персональных данных являются лица, замещающие должности Дирекции; граждане, претендующие на замещение вакантных должностей Дирекции; контрагенты (возможные контрагенты) по гражданско-правовым сделкам.

1.6. Положения настоящей Политики подлежат исполнению всеми сотрудниками Дирекции, принимающими участие в обработке персональных данных.

1.7. В целях выполнения требований статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», распоряжением руководителя Дирекции назначаются лица, ответственные за организацию обработки персональных данных, а также за обеспечение безопасности персональных данных. Ответственные назначаются из числа сотрудников Дирекции, имеющих достаточный уровень полномочий и квалификации для проведения указанных работ.

2. Процедуры и принципы обработки персональных данных

2.1. Обработка персональных данных в Дирекции осуществляется на основе принципов:

– законности и справедливости целей и способов обработки персональных данных, соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Дирекции;

– соответствия объема и характера обрабатываемых персональных данных, способам и целям обработки персональных данных;

– достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

– хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

– уничтожения по достижении целей обработки персональных данных и в случае утраты необходимости в их достижении.

2.2. В целях выявления и предотвращения нарушений законодательства Российской Федерации в сфере персональных данных, обеспечения прав субъектов персональных данных устанавливаются следующие процедуры:

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов несанкционированного доступа к персональным данным;

– недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль за обеспечением уровня защищенности персональных данных;

– определение для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения.

2.3. Процедуры по предотвращению несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

2.3.1. Процедура доступа в помещения, в которых осуществляется обработка персональных данных, заключается в запрете оставления помещений с незакрытыми на ключ дверями, в запрете проведения уборки помещений в отсутствие хотя бы одного сотрудника из числа работающих в этом помещении. Двери помещений оборудуются замками. Ключи от помещений хранятся у сотрудников, работающих в этих помещениях.

2.3.2. Процедура обращения электронных носителей информации заключается в выдаче и получении носителей информации информационной системы персональных данных (далее – ИСПДн), под роспись в соответствующем журнале учета. При этом под носителями понимаются как съемные носители (Flash-накопители и компакт-диски), так и жесткие диски персональных ЭВМ. Передача электронных носителей посторонним лицам запрещена. При необходимости ремонта средств вычислительной техники, пользователь ИСПДн, должен сообщить специалисту, ответственному за обеспечение безопасности персональных данных, о необходимости резервирования данных, хранящихся на жестком диске ПЭВМ, а при передаче средства вычислительной техники для осуществления ремонта в сторонней организации, также о необходимости удаления данных в соответствии с техническими требованиями, действующими для конкретной ИСПДн.

2.3.3. Процедура доступа к ресурсам ИСПДн пользователями ИСПДн заключается в соблюдении правил идентификации и аутентификации пользователей в соответствии с требованиями инструкции по парольной защите. Каждый пользователь ИСПДн должен осуществлять обработку персональных данных под своей учетной записью. Передача идентификаторов допускается только в случае замещения сотрудника, оформленного в установленном порядке. Передача идентификаторов и парольной информации посторонним лицам запрещена.

2.3.4. Процедура доступа к ресурсам ИСПДн сотрудников сторонних организаций, осуществляющих обслуживание и техническое сопровождение программных и технических средств ИСПДн, заключается в обязательстве сторонней организации и ее сотрудников о неразглашении сведений, ставших им известными в ходе выполнения обслуживания и (или) технического

сопровождения. Указанные обязательства должны быть закреплены в соответствующем разделе договора, при этом список сотрудников сторонней организации, имеющих возможность доступа к ресурсам ИСПДн, должен прилагаться к договору. Удаленный доступ сотрудников сторонних организаций, осуществляющих обслуживание и техническое сопровождение программных и технических средств ИСПДн, осуществляется при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите персональных данных (наличие аттестата соответствия требованиям по безопасности информации). Удаленный доступ должен осуществляться с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

2.3.5. Процедура доступа к информации, выводимой на средства отображения (печати) (мониторы персональных ПЭВМ, принтера) и сетевые печатающие устройства заключается в размещении средств отображения и сетевых печатающих устройств таким образом, чтобы неконтролируемый доступ к ним был исключен. Мониторы персональных ЭВМ должны блокироваться пользователем вручную, либо автоматически, при оставлении им рабочего места.

2.4. Процедуры по своевременному обнаружению фактов несанкционированного доступа к персональным данным.

2.4.1. Процедура обнаружения несанкционированного доступа к ресурсам ИСПДн заключается в ведении файлов журналирования (log-файлов) средств защиты информации, фиксирующего доступ учетных записей пользователей ИСПДн к соответствующему ресурсу, а также периодической проверки файлов журналирования (log-файлов) специалистом, ответственным за обеспечение безопасности персональных данных, на предмет выявления записей, свидетельствующих о попытках несанкционированного доступа. Периодичность проверки устанавливается не реже одного раза в день. В случае обнаружения попыток несанкционированного доступа, специалист, ответственный за обеспечение безопасности персональных данных, сообщает о данных фактах руководителю, для принятия им решения о дальнейшем разбирательстве.

2.4.2. Процедура обнаружения несанкционированного доступа вредоносных программ к ресурсам ИСПДн заключается в применении средства антивирусной защиты, средства анализа защищенности, выявляющих уязвимости штатного программного обеспечения ИСПДн. Периодичность применения и обновления баз данных указанных средств, содержащих сигнатуры вредоносных программ, должны быть установлены в автоматическом режиме. При обнаружении попыток несанкционированного доступа вредоносных программ к ресурсам ИСПДн, технические (программные) средства защиты должны осуществлять их блокировку и извещать специалиста, ответственного за обеспечение безопасности персональных данных в автоматическом режиме.

2.5. Процедуры по недопущению воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.5.1 Процедура по недопущению физического воздействия на технические средства автоматизированной обработки персональных данных заключается в предотвращении несанкционированного доступа к техническим средствам обработки путем контроля доступа, предусмотренного в пунктах 2.3.1.

2.5.2 Процедура по недопущению воздействия на средства обеспечения ИСПДн, таких как система электропитания, заключается в контроле обслуживания систем обеспечения. Доступ к системам обеспечения в целях их регламентного обслуживания должен осуществляться под контролем специалиста, ответственного за обеспечение безопасности персональных данных. Проведение регламентного обслуживания должно осуществляться квалифицированным персоналом в установленные сроки. Проведение ремонта, подразумевающего вывод из эксплуатации средств и систем обеспечения, должно производиться в согласованные сроки таким образом, чтобы не нарушить работоспособность технических средств обработки информации. При длительном выводе из эксплуатации должны приниматься меры по замене узлов, устройств и систем обеспечения, вышедших из строя.

2.5.3 Процедура по недопущению случайного воздействия на технические средства обработки и съемные носители заключается в соблюдении пользователями правил эксплуатации технических средств. Технические средства обработки должны применяться пользователями только по прямому назначению. Установка и подключение к персональным ЭВМ нештатных периферийных устройств (сотовых телефонов, коммуникаторов, смартфонов, иных средств) запрещены. Использование бытовых приборов, создающих электромагнитные поля большой мощности, в непосредственной близости от технических средств и съемных электронных носителей информации не допускается. Условия эксплуатации технических средств обработки информации должны исключать воздействие агрессивных сред (пыли, пара, жидкостей) и высоких температур.

2.6. Процедуры по обеспечению возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.6.1. Процедура резервного копирования файлов баз данных, содержащих персональные данные, заключается в создании их резервной копии с заданной периодичностью. Периодичность резервного копирования устанавливается в зависимости от времени обработки данных и длительности периода актуальности сведений.

2.6.2. Процедура восстановления утраченных или ошибочно удаленных файлов осуществляется специалистом, ответственным за обеспечение безопасности персональных данных.

2.7. Процедуры по контролю за обеспечением уровня защищенности персональных данных.

2.7.1. Процедура контроля работоспособности технических средств автоматизированной обработки персональных данных пользователей осуществляется ежедневно непосредственно пользователями и заключается в проверке функционирования при включении системного блока, монитора, клавиатуры и манипулятора «мышь». При выявленных неисправностях пользователю необходимо обратиться к специалисту, ответственному за обеспечение безопасности персональных данных.

2.7.2. Процедура контроля работоспособности коммутационного оборудования осуществляется ежедневно специалистом, ответственным за обеспечение безопасности персональных данных и заключается в проверке функционирования всех систем ИСПДн. При выявленных неисправностях необходимо обратиться к эксплуатационным документам для выяснения причин и принятия решения об устранении.

2.7.3. Процедура контроля за действиями пользователей осуществляется ежедневно специалистом, ответственным за обеспечение безопасности персональных данных путем просмотра файлов журналирования (log-файлов) и сообщений программного обеспечения средств защиты информации. При возникновении сообщений о попытках несанкционированного доступа к ресурсам ИСПДн, либо ошибочных действий пользователей, специалист, ответственный за обеспечение безопасности персональных данных сообщает об указанных фактах руководителю для принятия им решения о дальнейшем разбирательстве. Дополнительно необходимо ежедневно проверять исправность функционирования всех технических средств обработки путем визуального осмотра и контролировать отсутствие нештатных периферийных устройств, подключенных к персональным ЭВМ пользователей.

2.7.4. Процедура контроля за рассмотрением обращений субъектов персональных данных осуществляется руководителем Дирекции, либо по его поручению руководителем соответствующего структурного подразделения, по мере поступления обращений и в сроки, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2.7.5. Процедура оценки соответствия применяемых программных (технических) средств защиты информации заключается в использовании средств защиты, прошедших в установленном порядке сертификацию в системе сертификации ФСТЭК России или ФСБ России (по принадлежности), а также в своевременном продлении срока действия сертификатов соответствия.

2.7.6. Процедура оценки эффективности принимаемых мер по обеспечению безопасности персональных данных проводится не реже одного раза в три года. Оценка эффективности производится с учетом актуальных угроз безопасности персональных данных, определенных в Модели угроз и (или) Модели нарушителя (при необходимости), имеющих актуальную редакцию на момент проверки. Оценка эффективности проводится с применением специальных программных (технических) средств контроля,

прошедших в установленном порядке оценку соответствия (сертификацию) в системе сертификации ФСТЭК России или ФСБ России (по принадлежности).

2.8. Процедуры, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, сроки обработки и хранения персональных данных, порядок уничтожения.

2.8.1. Процедуры, определяющие для каждой цели обработки данных содержание персональных данных, категории субъектов персональных данных и сроки обработки персональных данных, а также сроки их хранения в ИСПДн, заключаются в доведении до каждого сотрудника – пользователя ИСПДн содержания, сроков обработки персональных данных, категории субъектов, необходимых для реализации целей обработки. Доведение осуществляется путем издания распоряжений (приказов) Дирекции и ознакомления сотрудников под роспись. Содержание, категории субъектов и сроки обработки персональных данных формируются исходя из требований законодательства Российской Федерации, а также производственной необходимости.

2.8.2. Процедура, определяющая порядок хранения персональных данных заключается в получении и выдаче носителей информации сотрудниками Дирекции, являющимися пользователями ИСПДн, под роспись в соответствующем журнале учета.

2.8.3. Процедура, определяющая порядок уничтожения персональных данных на электронных носителях заключается в физическом уничтожении носителя либо в применении специальных программных средств, обеспечивающих защиту от несанкционированного доступа для затирания областей пространств носителя таким образом, чтобы восстановление удаленной информации было невозможным. Программные средства, применяемые для этих целей, должны проходить процедуру сертификации в системе сертификации ФСТЭК России и входить в состав средств защиты ИСПДн.

3. Правила рассмотрения запросов субъектов персональных данных или их представителей

3.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

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

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

3.2. Запрос направляется в Дирекцию в письменном виде и должен содержать:

1) номер, серию документа, удостоверяющего личность субъекта персональных данных или его представителя, дату выдачи, наименование органа, выдавшего его;

2) информацию, подтверждающую участие субъекта персональных данных в правоотношениях с Дирекцией, либо информацию, иным образом подтверждающую факт обработки персональных данных в Дирекции, заверенную подписью субъекта персональных данных или его представителя.

3.3. Информация, предусмотренная пунктом 3.1, предоставляется субъекту персональных данных или его представителю сотрудником структурного подразделения Дирекции, осуществляющим обработку соответствующих персональных данных.

3.4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено федеральными законами.

4. Права и обязанности оператора и субъекта персональных данных

4.1. Дирекция как оператор персональных данных вправе:

– отстаивать свои интересы в суде;

– предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством;

– отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

– использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством.

4.2. Дирекция как оператор персональных данных обязана:

– принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от

27.07.2006 N 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

4.3. Субъект персональных данных имеет право:

– требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

– требовать перечень своих персональных данных, обрабатываемых Дирекцией и источник их получения;

– получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

– требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

– на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5. Доступ к обрабатываемым персональным данным

5.1. Доступ к обрабатываемым в Дирекции персональным данным имеют лица, уполномоченные распоряжением руководителя Дирекции, лица, которым Дирекция поручила обработку персональных данных на основании заключенного договора, а также лица, чьи персональные данные подлежат обработке.

5.2. В целях разграничения полномочий при обработке персональных данных полномочия по реализации каждой определенной законодательством функции или услуги Дирекции закрепляются за соответствующими структурными подразделениями Дирекции.

Доступ к персональным данным, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Дирекции, могут иметь только сотрудники этого структурного подразделения. Доступ сотрудников к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями.

Допущенные к обработке персональных данных сотрудники под роспись знакомятся с документами Дирекции, структурного подразделения, устанавливающими порядок обработки персональных данных.

6. Сроки обработки и хранения персональных данных

6.1. Сроки обработки и хранения персональных данных определяются и устанавливаются в соответствии с законодательством Российской Федерации. Персональные данные граждан, обратившихся в Дирекцию лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет.

6.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

6.3. 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 Дирекции.

6.4. Срок хранения персональных данных, внесенных в автоматизированные информационные системы, должен соответствовать сроку хранения бумажных оригиналов.

7. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

7.1. Дирекция и ее структурные подразделения осуществляют систематический контроль за обеспечением сохранности документов, содержащих персональные данные, и по истечению сроков хранения организуют отбор документов, содержащих персональные данные, к уничтожению в соответствии с действующим законодательством в области архивного дела.

7.2. Отобранные к уничтожению документы, содержащие персональные данные, включаются в акт и после согласования акта экспертной комиссией по вопросам делопроизводства и архивного дела Дирекции уничтожаются.

7.3. 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.