Приложение 1 к приказу учреждения

от 13.09.2017г. № 138/ОД

ИНСТРУКЦИЯ

по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных

1. Настоящая инструкция разработана в соответствии с требованиями подпункта «в» пункта 13 постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах.
2. Основанием для допуска и прекращения допуска сотрудника к персональным данным (далее - ПДн) в информационных системах персональных данных (далее - ИСПДн) муниципального автономного учреждения Центра физкультурной и спортивной работы Тюменского муниципального района (далее - учреждение), является приказ руководителя учреждения, основанный на письменном ходатайстве руководителя структурного подразделения, согласованном с ответственным за организацию обработки персональных данных учреждения.
3. Для учета лиц, допущенных к работе с ПДн в ИСПДн, ведется «Журнал учета лиц, допущенных к работе с персональными данными в ИСПДн».
4. «Журнал учета лиц, допущенных к работе с персональными данными в ИСПДн» учитывается в соответствии с правилами ведения делопроизводства и ведется администратором безопасности информации в ИСПДн.

Приложение 2 к приказу учреждения

от 13.09.2017г. № 138/ОД

ИНСТРУКЦИЯ

ответственному за эксплуатацию информационной системы персональных данных

1. Общие положения

1. Настоящая инструкция определяет основные обязанности, права и ответственность ответственного за эксплуатацию информационной системы персональных данных (далее - ИСПДн) муниципального автономного учреждения Центра физкультурной и спортивной работы Тюменского муниципального района (далее - учреждение) по вопросам защиты информации в ИСПДн, используемой в работе учреждения.
2. Ответственный за эксплуатацию ИСПДн назначается из числа руководителей структурных подразделений учреждения, эксплуатирующих ИСПДн, и осуществляет контроль за соблюдением порядка работы пользователей ИСПДн, установленного соответствующей инструкцией, на которых проводится обработка персональных данных, дополнительно к своим непосредственным обязанностям. Ответственный за эксплуатацию ИСПДн назначается приказом учреждения.
3. Ответственный за эксплуатацию ИСПДн непосредственно подчиняется ответственному за организацию обработки ПДн учреждения в части, касающейся защиты информации в информационной системе персональных данных учреждения, и осуществляет контроль за выполнением требований организационно-распорядительных документов по обеспечению безопасности информации при ее обработке в ИСПДн структурных подразделений учреждения.
4. **Обязанности ответственного за эксплуатацию ИСПДн**

2.1. Ответственный за эксплуатацию ИСПДн обязан знать перечень автоматизированных рабочих мест (далее - АРМ), входящих в состав ИСПДн и перечень задач, решаемых с их использованием.

2.2. Ответственный за эксплуатацию ИСПДн обязан обеспечивать постоянный контроль за выполнением пользователями ИСПДн требований инструкций по обеспечению безопасности обработки персональных данных.

2.3. Ответственный за эксплуатацию ИСПДн обязан немедленно сообщать ответственному за организацию обработки персональных данных (далее - ПДн) учреждения в части, касающейся защиты информации, об обнаруженных фактах (попытках) несанкционированного доступа к информации и АРМ, и принимать необходимые меры по пресечению нарушений.

2.4. Ответственный за эксплуатацию ИСПДн обязан организовать ведение «Журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, храненияи транспортировки информации».

2.5. Ответственный за эксплуатацию ИСПДн обязан осуществлять контроль за правильностью использования и хранениямашинных носителей информации и документов, содержащих персональные данные.

2.6. Ответственный за эксплуатацию ИСПДн обязан осуществлять контроль за правильностью использования и хранения персональных идентификаторов и личных паролей пользователями.

2.7. Ответственный за эксплуатацию ИСПДн обязан разъяснять работникам структурного подразделения учреждения вопросы обеспечения информационной безопасности и правила работы с используемыми средствами зашиты информации.

2.8. Ответственный за эксплуатацию ИСПДн обязан требовать от работников структурного подразделения учреждения соблюдения правил организации парольной защиты (в соответствии с «Инструкцией по организации парольной защиты в информационных системах персональных данных муниципального автономного учреждения Центр физкультурной и спортивной работы Тюменского муниципального района»).

2.9. Ответственный за эксплуатацию ИСПДн обязан контролировать использование сотрудниками отдела средств зашиты информации, установленных на АРМ, входящих в ИСПДн.

2.10. Ответственный за эксплуатацию ИСПДн обязан контролировать прохождение антивирусного контроля (в соответствии с «Инструкцией по организации антивирусной защиты в информационных системах персональных данных муниципального автономного учреждения Центра физкультурной и спортивной работы Тюменского муниципального района») при применении машинных носителей информации.

2.11. Ответственный за эксплуатацию ИСПДн обязан контролировать наличие защитных пломб на корпусах АРМ, входящих в ИСПДн.

2.12. Ответственный за эксплуатацию ИСПДн обязан немедленно прекращать работы на АРМ при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

1. Права ответственного за эксплуатацию ИСПДн

3.1. Ответственный за эксплуатацию ИСПДн имеет право требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации (в соответствии с документом «Описание технологического процесса обработки персональных данных в информационных системах персональных данных муниципального автономного учреждения Центр физкультурной и спортивной работы Тюменского муниципального района») и выполнения инструкций по обеспечению безопасности информации в ИСПДн.

3.2. Ответственный за эксплуатацию ИСПДн имеет право инициировать проведение служебных расследований по фактам нарушения требований защиты информации, утвержденных соответствующими инструкциями, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.3. Ответственный за эксплуатацию ИСПДн имеет право подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты на своем участке работы.

Приложение 3 к приказу учреждения

от 13.09.2017г. № 138/ОД

**ИНСТРУКЦИЯ**

по организации парольной защиты в информационных

системах персональных данных

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее - ИСПДн), а также контроль за действиями пользователей при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на администратора безопасности информации в ИСПДн.
2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 6 символов;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры или специальные символы (@, #, $, &, \*, % и тому подобное);
* символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и так далее), а также общепринятые сокращения (ЭВМ, ЛВС, USER и тому подобное);
* при смене пароля новое значение должно отличаться от предыдущих;
* пользователь не имеет права сообщать личный пароль другим лицам;
* все используемые пароли должны ежемесячно сменяться на новые.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

1. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и тому подобное, либо при наличии технологической необходимости использования имен и паролей сотрудников (пользователей ИСПДн) в их отсутствие, сотрудники обязаны при первой   
   же возможности сменить разглашенный пароль на новый в соответствии с требованиями настоящей инструкции. Также, сразу же после смены своих паролей, их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение администратору безопасности информации в ИСПДн или руководителю структурного подразделения. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у пользователей).
2. Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.
3. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и тому подобное) должна производиться администратором безопасности информации в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.
4. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности информации в ИСПДн.
5. В случае компрометации (утеря, передача другому лицу) личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с пунктом 5 или пунктом 6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.
6. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности информации в ИСПДн.

Приложение 4 к приказу учреждения

от 13.09.2017г. № 138/ОД

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах персональных данных

1. Общие требования

1.1. Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее - ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений муниципального автономного учреждения Центр физкультурной и спортивной работы Тюменского муниципального района (далее - учреждение), эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Настоящая Инструкция распространяется на все ИСПДн существующие и вновь разрабатываемые учреждением. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы ИСПДн.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля осуществляется администратором безопасности информации в ИСПДн.

1.4. Данные требования не распространяются на автоматизированные рабочие места (далее - АРМ) с установленными операционными системами, для которых отсутствуют какие-либо средства антивирусного контроля.

1. Применение средств антивирусного контроля
   1. При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся   
      в автозагрузке, реестра операционной системы.
   2. Полному антивирусному контролю АРМ в учреждении должны подвергаться не реже одного раза в неделю.
   3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и тому подобное). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
   4. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.
   5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения АРМ, администратором безопасности информации в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ ИСПДн.
   6. При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и тому подобное) работник структурного подразделения учреждения самостоятельно или вместе с администратором безопасности информации в ИСПДн
   7. должен провести внеочередной антивирусный контроль своего АРМ.
   8. В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, работника учреждения обязаны:

* приостановить работу в ИСПДн;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения учреждения и администратора безопасности информации в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
* совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* администратору безопасности информации в ИСПДн провести лечение или уничтожение зараженных файлов.

1. Ответственность
   1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на руководителя структурного подразделения учреждения, эксплуатирующего ИСПДн.
   2. Ответственность за проведение мероприятий антивирусного контроля в структурных подразделениях учреждения и соблюдение требований настоящей Инструкции возлагается на администратора безопасности информации в ИСПДн и всех работников структурных подразделений учреждения, являющихся пользователями ИСПДн.
   3. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется ответственным за организацию обработки ПДн.

Приложение 5 к приказу учреждения

от 13.09.2017г. № 138/ОД

ИНСТРУКЦИЯ

**работнику муниципального автономного учреждения Центр физкультурной и спортивной работы Тюменского муниципального района, ведущему обработку персональных данных без использования средств автоматизации**

1. Общие положения

1. Настоящая инструкция включает основные обязанности, права и ответственность пользователя, допущенного к обработке персональных данных и иной конфиденциальной информации на средствах вычислительной техники.
2. Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
3. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
4. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.
5. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, муниципальными нормативными правовыми актами, а также локальными нормативными актами учреждения, должны применяться с учетом требований настоящего Положения.
6. Особенности организации обработки персональных данных без средств автоматизации
   1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации   
      их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).
   2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
   3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники учреждения или лица, осуществляющие такую обработку по договору с учреждением), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки,
   4. установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, муниципальными нормативными правовыми актами, а также локальными нормативными актами учреждения (при их наличии).
   5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

* типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
* типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
* типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
* типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.
  1. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится учреждение, или в иных аналогичных целях, должны соблюдаться следующие условия:
* необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом учреждением, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию учреждения, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
* копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
* персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию учреждения.
  1. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:
* при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное
* копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

* 1. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
  2. Правила, предусмотренные настоящей Инструкцией, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.
  3. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

1. **Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации**
   1. Обработка персональных данных без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
   2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
   3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются учреждением.

Приложение 6 к приказу учреждения

от 13.09.2017г. № 138/ОД

ИНСТРУКЦИЯ

о порядке работы пользователей со средствами криптографической защиты информации

1. **Общие положения**
   1. Настоящая Инструкция определяет порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну (далее - крипто средство) в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее - информационная система).
   2. Пользователь - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.
   3. Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.
   4. Шифровальные (криптографические) средства - криптосредства:
      1. средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа (далее - НСД) при ее обработке и хранении;
      2. средства имитозащиты-аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
      3. средства электронной цифровой подписи (далее - ЭЦП) - аппаратные, программные   
         и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание ЭЦП с использованием закрытого ключа ЭЦП, подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП, создание закрытых и открытых ключей ЭЦП;
      4. Средства кодирования -средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;
      5. Средства изготовления ключевых документов (независимо от вида носителя ключевой информации);
      6. Ключевые документы (независимо от вида носителя ключевой информации).
2. **Обязанности пользователей криптосредств**
   1. Пользователи криптосредств обязаны:
      1. Не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;
      2. Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;
      3. Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;
      4. Немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных;
      5. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкции, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

**3. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей.**

1. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.
2. Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.
3. Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.
4. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.
5. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.
6. Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.
7. Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят   
   (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться   
   в техническом (аппаратном) журнале, ведущемся непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства   
   не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).
8. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.
9. Пользователи криптосредств хранят инсталлирующие криптосредства
10. носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
11. Пользователи криптосредств предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения   
    в случае компрометации действующих ключевых документов.
12. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.
13. Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными оператором ответственными пользователями криптосредств и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки.
14. Эксплуатационную и техническую документацию к криптосредствам допускается пересылать заказными или ценными почтовыми отправлениями.
15. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).
16. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), DataKey, SmartCard, TouchMemory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).
17. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).
18. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин.
19. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.)» разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).
20. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.
21. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах уничтожаются пользователями этих криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.
22. Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и тому подобное) ответственного пользователя криптосредств для списания уничтоженных документов с их лицевых счетов.
23. Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.
24. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя криптосредств, согласованного с оператором, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.
25. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств и (или) оператору.
26. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).
27. В случаях недосдачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.
28. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет оператор.

Приложение 7 к приказу учреждения

от 13.09.2017г. № 138/ОД

ИНСТРУКЦИЯ

по организации резервирования и восстановления программного обеспечения

и баз персональных данных в информационных системах

персональных данных

1. Общие положения

1. Настоящая инструкция разработана в соответствии с требованиями подпункта «б» пункта 13 постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», с целью обеспечения возможности незамедлительного восстановления персональных данных (далее - ПДн), модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее - ИСПДн) муниципального автономного учреждения Центра физкультурной и спортивной работы Тюменского муниципального района (далее - учреждение).
3. Резервируемое программное обеспечение и базы персональных данных
   1. В ИСПДн резервированию подлежит:

* общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и тому подобное), поставляемые с компонентами автоматизированных рабочих мест (далее - АРМ), входящими в состав ИСПДн);
* прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и тому подобное);

базы ПДн (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

* программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

1. Порядок резервирования и хранения резервных копий
   1. Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора безопасности информации в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.
   2. Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора безопасности информации в ИСПДн.
   3. Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях учреждения, эксплуатирующих ИСПДн.
   4. Резервирование баз ПДн, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.
   5. Резервирование осуществляется ежемесячно назначенными приказом учреждения работниками учреждения, под контролем ответственных за эксплуатацию ИСПДн.
   6. Резервные носители ПДн хранятся в структурных подразделениях учреждения, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации ПДн.
   7. К резервному носителю ПДн должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.
   8. Резервные носители ПДн не могут быть переданы за пределы структурных подразделений учреждения, эксплуатирующих ИСПДн.
   9. Копирование информации с резервных носителей ПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.
2. Порядок восстановления работоспособности ИСПДн
   1. Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.
   2. Данные работы осуществляются администратором безопасности информации в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.
   3. Восстановление ПДн, созданных после их последнего резервирования, осуществляется структурным подразделением, осуществляющим эксплуатацию ИСПДн.
   4. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с ПДн. Ответственность за выполнение данного требования возлагается на администратора безопасности информации в ИСПДн и руководителя структурного подразделения учреждения, обеспечивающего ее эксплуатацию.
3. Типовая форма учетной карточки резервного носителя персональных данных № \_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| дата резервного копирования | объект копирования | кто производил копирование | подпись |
| 1 | 2 | 3 | 4 |
|  |  |  |  |
|  |  |  |  |

Приложение 8 к приказу учреждения

от 13.09.2017г. № 138/ОД

ИНСТРУКЦИЯ

о порядке работы пользователей информационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

1. Настоящая инструкция определяет порядок действий пользователей информационных систем персональных данных (далее - ИСПДн) в части обеспечения безопасности персональных данных (далее - ПДн) при их обработке в ИСПДн.
2. Допуск пользователей для работы за автоматизированным рабочим местом (далее - АРМ) осуществляется на основании утверждаемого «Списка работников учреждения, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных обязанностей» в муниципальном автономном учреждении Центре физкультурной и спортивной работы Тюменского муниципального района (далее - учреждение).
3. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в «Журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения, транспортировки информации».
4. Пользователь несет ответственность за правильность включения и выключения АРМ, входа в систему и все действия при работе в ИСПДн.
5. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.
6. Запись информации, содержащей ПДн, может, осуществляется пользователем ИСПДн на съемные машинные носители информации, соответствующим образом учтенные в «Журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения, транспортировки информации».
7. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями Инструкции по организации антивирусной защиты.
8. Каждый сотрудник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:
   1. Строго соблюдать установленные соответствующими Инструкциями правила обеспечения безопасности информации ИСПДн.
   2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ.
   3. Хранить в тайне свой пароль (пароли). Выполнять требования Инструкции по организации парольной защиты в полном объеме.
   4. Хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу).
   5. Выполнять требования Инструкции по организации антивирусной защиты в полном объеме
   6. Немедленно известить администратора безопасности информации в ИСПДн в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

* нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих компонентах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к АРМ;
* несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ ИСПДн;
* отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

некорректного функционирования установленных на АРМ технических средств защиты;

* непредусмотренных отводов кабелей и подключенных устройств.

1. Пользователю АРМ категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

* самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;
* осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
* записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и тому подобное);
* оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
* оставлять без личного присмотра на рабочем месте или в ином месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;
* умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
* размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.