УТВЕРЖДАЮ
Заведующий МАДОУ ДСКВ
_____ Н.А. Пайму
Приказ от «01» 09 201

ПОЛИТИКА
в области обеспечения безопасности персональных данных в МАДОУ ДСКВ «Рябинушка»

1. Общие положения

1.1. В целях обеспечения безопасности персональных данных при их информационных системах персональных данных МАДОУ ДСКВ в соответствии с требованиями Федерального закона от 27 июля 2006 определяется политика в области обеспечения безопасности персональ содержащая основные правила и порядок обработки персональных данных гра

1.2. Политика заключается в выполнении требований и нор персональных данных, установленных в Постановлении Правительства Федерации от 1 ноября 2012 года № 1119.

2. Лица, ответственные за обеспечение безопасности персональных данных

2.1. В МАДОУ ДСКВ «Рябинушка» производится назначение ответственных лиц:

2.1.1. Ответственный за организацию работ по обеспечению персональных данных, на которого приказом заведующего ДОУ возлагается:

• утверждение списка лиц, доступ которых к персональным данным, выполнения служебных (трудовых) обязанностей, а также изменений к нему;

• принятие решения о распространении (передаче) персональных данны

• проведение разбирательств по фактам несоблюдения условий хране персональных данных, использования средств защиты информации, ко привести к нарушению конфиденциальности персональных данных нарушениям, приводящим к снижению уровня защищенности персональных д

• приостановка предоставления персональных данных информационной системы при обнаружении нарушений порядка п персональных данных;

• руководство работами по обеспечению безопасности персональных д обработке в информационных системах персональных данных.

2.1.2. Ответственного пользователя криптосредств.

2.1.3. Ответственного за выполнение работ по обеспечению персональных данных, на которого приказом заведующего ДОУ возлагается:

• организация парольной защиты;

• организация учета средств защиты информации, эксплуатационной

- учет лиц, допущенных к работе с персональными данными в информационных системах;
- учет носителей персональных данных, используемых в информационных системах персональных данных (как с использованием средств автоматизации, так и без их использования);
- периодическая (не реже одного раза в квартал) проверка электронного журнала обращений пользователей информационных систем к персональным данным;
- инструктаж пользователей информационных систем персональных данных о порядке и правилах использования средств защиты информации, включая средства антивирусной защиты;
- контроль за соблюдением условий использования средств защиты информации (за исключением средств криптографической защиты информации).

3. Организация резервирования и восстановления программного обеспечения, баз персональных данных информационных систем персональных данных

3.1. В информационных системах персональных данных резервированию подлежат:
- базы персональных данных;
- специальное программное обеспечение;
- средства защиты информации;
- общее программное обеспечение;
- средства вычислительной техники;
- средства обеспечения функционирования информационных систем.

3.2. Резервные носители персональных данных хранятся в подразделении, эксплуатирующем ИСПДн.

3.3. Резервные носители персональных данных не могут быть переданы за пределы подразделения, эксплуатирующего ИСПДн.

3.4. Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, ***запрещается***.

3.5. Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения машинных носителей дистрибутивов данных программ и машинных носителей обновлений к ним в подразделениях, отвечающих за их установку, настройку и сопровождение.

3.6. Машинные носители обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны быть маркированы датой их получения (датой выхода обновления).

3.7. В случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения осуществляется обязательное восстановление работоспособности ИСПДн.

4. Учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных

4.1. Лица, допущенные к работе с персональными данными в информационных системах персональных данных утверждаются соответствующим приказом.

4.2. Основанием для допуска сотрудника к персональным данным, обрабатываемым в информационных системах персональных данных, является необходимость обработки персональных данных в связи с выполнением должностных обязанностей, а также соответствующий приказ, утвержденный заведующим ДОУ.

4.3. Основанием для прекращения допуска сотрудника к персональным данным, обрабатываемым в информационных системах персональных данных, может служить приказ об его увольнении (переводе на другую должность, не требующую работы с персональными данными).

5. Организация парольной защиты в информационных системах персональных данных

5.1. Защите паролем подлежит доступ к:

- базовым системам ввода вывода компьютеров;
- настройкам сетевого оборудования;
- настройкам операционных систем;
- настройкам средств защиты информации (в том числе средств антивирусной защиты);
- запуску специализированного программного обеспечения, предназначенного для обработки персональных данных;
- ресурсам АРМ и баз данных ИСПДн.

5.2. Базовые системы ввода вывода, сетевое оборудование, операционные системы, средства защиты информации и файловые массивы (далее – объекты парольной защиты) должны быть настроены таким образом, чтобы:

- исключить возможность просмотра ранее вводимых паролей;
- блокировать доступ пользователей после пятикратной ошибки при вводе пароля и сигнализировать о наступлении данного события.

5.3. 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 сотрудников отдела инженерно-технического обеспечения, отдела информационных технологий и администраторов баз данных в территориальных отделах в соответствии с возложенными обязанностями.

5.4. Пользователь обязан запомнить личные пароли и никому их не передавать, и не записывать их на местах, где их могут увидеть другие лица.

5.5. Информация о паролях пользователей является информацией ограниченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к ресурсам ИСПДн согласно разрешительной системы доступа.

5.6. **ЗАПРЕЩАЕТСЯ:**

- умышленное и неумышленное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;
- передача личного пароля сослуживцам или посторонним лицам;
- запись личного пароля на бумагу и хранение его в потенциально доступном для ознакомления посторонними лицами и другими сотрудниками месте;
- вход в систему с использованием чужих идентификаторов или паролей;
- оставление без присмотра рабочего места при работе в ИСПДн.

5.7. 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.

5.8. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора.

6. Антивирусная защита в информационных системах персональных данных

6.1. К использованию в ИСПДн допускаются только лицензионные и сертифицированные по требованиям безопасности информации антивирусные средства.

6.2. Установка и настройка средств антивирусного контроля на компьютерах осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

6.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

6.4. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в 3 месяца.

6.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения, должна быть выполнена антивирусная проверка на всех компьютерах ИСПДн.

6.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно должен провести внеочередной антивирусный контроль своего компьютера.

6.7. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на сотрудников отдела инженерно-технического обеспечения и администраторов баз данных в территориальных отделах.

6.8. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на сотрудников отдела инженерно-технического обеспечения и администраторов баз данных в территориальных отделах и всех сотрудников, являющихся пользователями ИСПДн.

6.9. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований по антивирусной защите осуществляется ответственным за организацию работ по обеспечению безопасности персональных данных при их обработке в ИСПДн.

7. Перечень персональных данных, обрабатываемых в информационных системах персональных данных и подлежащих защите

7.1. В информационных системах персональных данных защите подлежит:

- любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:
  - фамилия, имя, отчество;
  - год рождения;
  - месяц рождения;
  - дата рождения;
  - адрес;
  - образование;
  - профессия;
  - доходы;
  - фотография;
  - контактный номер;
  - сведения о документе, удостоверяющем личность;
  - реквизиты ИНН, СНИЛС, пенсионного удостоверения, расчетных счетов.

Фамилия, имя и отчество не являются информацией, позволяющей определить субъекта персональных данных.

8. Порядок предоставления персональных данных

8.1. Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц.

8.2. Персональные данные могут быть распространены только на основании решения субъекта персональных данных.

8.3. До передачи любых персональных данных за пределы организации от каждого субъекта персональных данных должно быть получено письменное согласие на распространение его персональных данных, оформленное в соответствии с требованиями статьи 9 Федерального закона «О персональных данных», в каждом конкретном случае.

8.4. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта

персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8.5. Решение на предоставление персональных данных принимается ответственным за организацию обработки персональных данных.

8.6. Персональные данные, обрабатываемые в ИСПДн, могут быть предоставлены органам власти и органам местного самоуправления без согласия субъекта персональных данных, если данные действия осуществляются в соответствии с федеральными законами Российской Федерации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом решение на распространение персональных данных должно содержать ссылку на соответствующую статью федерального закона Российской Федерации.

9. Порядок приостановки предоставления персональных данных, в случае обнаружения нарушений порядка их предоставления, и порядок разбирательств по фактам, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям

9.1. При обнаружении нарушений порядка предоставления персональных данных предоставление персональных данных пользователям информационной системы незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

9.2. Принятие решения на приостановку обработки персональных данных принимается ответственным за организацию обработки персональных данных.

9.3. Основаниями для приостановки обработки ПДн в ИСПДн и проведения разбирательства являются:

- выявление недостоверных персональных данных в информационных системах персональных данных;
- предоставление персональных данных в нарушение установленных правил;
- допуск к ИСПДн лица, не имеющего на то разрешения;
- утрата носителя персональных данных;
- нарушение правил хранения носителей персональных данных;
- нарушение правил эксплуатации средств защиты информации;
- нарушение правил парольной защиты;
- нарушение правил антивирусной защиты;
- нарушение правил резервирования и восстановления общего и специального программного обеспечения, а также баз персональных данных;
- выявление в ИСПДн вредоносных программ (вирусов);
- выявление в электронных журналах средств защиты информации несанкционированных действий пользователей, нарушающих безопасность персональных данных или целостность (неизменность) программного обеспечения ИСПДн;
- выявление несанкционированного внесения изменений в состав технических средств и (или) программного обеспечения ИСПДн.

9.4. Разбирательство проводится структурным подразделением или должностным лицом (работником), ответственным за обеспечение безопасности персональных данных, с обязательным привлечением руководителя структурного подразделения, осуществляющего эксплуатацию ИСПДн.

9.5. В ходе разбирательства составляется заключение, в котором отражается:

- состав группы проводившей разбирательство;
- период времени, в который проводилось разбирательство;
- основание для проведения разбирательства;
- факты, выявленные в ходе разбирательства и имеющие значение в определении наличия нарушений конфиденциальности персональных данных или нарушений правил использования средств защиты информации, а также иные факты, которые могут привести к нарушению конфиденциальности персональных данных или к снижению уровня защищенности персональных данных;
- вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;
- рекомендации по совершенствованию обеспечения безопасности персональных данных, исключающие в дальнейшем подобные нарушения.

9.6. Заключение представляется ответственному за организацию обработки персональных данных, который принимает решение на возобновление обработки персональных данных и принятие дополнительных мер защиты.

10. Порядок взаимодействия по вопросам обеспечения безопасности персональных данных

10.1. Взаимодействие по вопросам обеспечения безопасности персональных данных может осуществляться с:

- Администрацией города Покачи;
- организациями, оказывающими услуги по обеспечению безопасности персональных данных;
- подчиненными организациями и обособленными структурными подразделениями.

10.2. Взаимодействие по вопросам обеспечения безопасности персональных данных с Администрацией города Покачи осуществляется в части методического обеспечения и контроля, а также в целях определения единой стратегии и технической политики в области обеспечения безопасности персональных данных.. Методическое обеспечение в части методов и способов защиты информации в информационных системах осуществляется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

10.3. Взаимодействие с организациями, оказывающими услуги по обеспечению безопасности персональных данных, осуществляется на договорной основе. Такие организации в обязательном порядке должны иметь лицензию Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации, а в случае оказания ими

услуг в области криптографической защиты информации – лицензии Федеральной службы безопасности Российской Федерации.

10.4. Существенным условием договора с организацией, оказывающей услуги по обеспечению безопасности персональных данных, является требование соблюдения конфиденциальности сведений о степени защищенности информационных систем персональных данных (внедренных методах и способах защиты и их эффективности).

10.5. Взаимодействие с подчиненными организациями и обособленными структурными подразделениями осуществляется в части методического руководства и контроля за полнотой и эффективностью принятых мер обеспечения безопасности персональных данных. Контрольные мероприятия в подчиненных организациях и обособленных структурных подразделениях осуществляются ответственным за организацию работ по обеспечению безопасности персональных данных, ответственным пользователем криптосредств (в части использования средств криптографической защиты информации) и сотрудниками отдела инженерно-технического обеспечения, осуществляющими работы по обеспечению безопасности персональных данных.

УТВЕРЖДАЮ
Заведующий МАДОУ ДСКВ «Рябинушка»
_____ Н.А. Паймухина
Приказ от «___»_____ 2017 №_____

ПОЛОЖЕНИЕ
о порядке выявления и реагирования на инциденты информационной безопасности МАДОУ ДСКВ «Рябинушка»

1. Общие положения

1.1. Настоящее Положение устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационных систем МАДОУ ДСКВ «Рябинушка» (далее – Организация) и (или) возникновению угроз безопасности конфиденциальной информации Организации (далее – инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима коммерческой тайны (далее – служебное расследование) в Организации.

1.2. Настоящее Положение разработано в соответствии с Положением по организации и проведению работ по обеспечению безопасности конфиденциальной информации при ее обработке в информационных системах Организации.

1.3. Процесс управления инцидентами ИБ включает:

- учет и регистрацию инцидентов ИБ;
- оповещение ответственного лица о возникновении инцидентов ИБ;
- расследование обнаруженных инцидентов ИБ;
- устранение причин и последствий инцидентов ИБ;
- определение плана корректирующих и превентивных мероприятий.

1.4. Требования настоящего Положения являются обязательными для выполнения всеми работниками Организации.

2. Учет и регистрация инцидентов информационной безопасности

2.1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем Организации.

2.2. В обязательном порядке должны регистрироваться следующие события безопасности:

- попытки входа (выхода) пользователей в операционную систему (из операционной системы);
- загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;
- попытка доступа к средствам виртуализации;
- факт изменения конфигурации средств виртуализации;
- запуск и остановка служб (системных сервисов) средств виртуализации;
- попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

2.3. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

- тип события;
- дата и время события;
- результат события;
- источник события;
- идентификатор пользователя информационной системы, предъявленный при попытке доступа.

2.4. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.

2.5. Учет инцидентов ИБ осуществляется администратором информационной безопасности информационных систем Организации (далее – администратор ИБ), назначенным приказом по Организации. Допускается ведение учета инцидентов ИБ в электронном виде.

2.6. При обнаружении инцидента ИБ администратор ИБ проводит его классификацию в соответствии с приложением №1 к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

3. Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности

Средства защиты информации должны обеспечивать возможность информирования администратора ИБ о критических событиях безопасности в информационной системе по электронной почте или посредством смс.

В случае, если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», администратор ИБ обязан незамедлительно сообщить о выявленном инциденте ИБ ответственному за обеспечение безопасности конфиденциальной информации по электронной почте или иному средству связи.

Ответственный за обеспечение безопасности конфиденциальной информации должен провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным данным Положением.

4. . Порядок расследования обнаруженных инцидентов информационной безопасности

Проведение служебного расследования инициируется приказом заместителя заведующего Организации, ответственного за вопросы разработки, принятия и внедрения мер защиты информации (далее – заместитель заведующего). В этом же приказе устанавливается состав Комиссии для проведения служебного расследования (далее – Комиссия).

Служебное расследование может быть возбуждено:

- по решению заместителя заведующего Организации;
- по инициативе любого работника Организации на основании служебной записки в произвольной форме на имя заместителя заведующего Организации;
- по устному докладу.

В состав Комиссии входят следующие работники Организации:

4.1.1. В обязательном порядке:

- Председатель Комиссии – ответственный за обеспечение безопасности конфиденциальной информации;
- администратор ИБ.

4.1.2. В случае необходимости Комиссия вправе привлекать к расследованию:

- администратора информационных систем Организации;
- руководителя структурного подразделения, в котором произошел инцидент ИБ;
- непосредственного руководителя работника, в отношении которого проводится служебное расследование;
- экспертов из других структурных подразделений и, при необходимости, представителей сторонних организаций.

Комиссия для проведения служебного расследования в рабочем порядке в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное расследование.

Результаты работы Комиссии оформляются в виде аналитического экспертного заключения на имя заведующего Организации, с предложениями:

- по внесению изменений в организационные и (или) технические меры по защите конфиденциальной информации;
- по внесению изменений и улучшений в комплект организационно - распорядительной документации Организации;
- по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

В аналитическом экспертном заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.

Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами Организации.

5. . Устранение причин и последствий инцидентов информационной безопасности

5.1. Для инициирования работ по устранению причин и последствий инцидентов ИБ ответственный за обеспечение безопасности конфиденциальной информации направляет аналитическое экспертное заключение по электронной почте заместителю заведующего и ответственным за выполнение запланированных работ.

Если ответственный за выполнение запланированных работ не согласен с установленными сроками, он вправе обратиться к ответственному за обеспечение безопасности конфиденциальной информации с просьбой перенести срок с обоснованием причин переноса.

При изменении сроков реализации действий, ответственный за обеспечение безопасности конфиденциальной информации вносит необходимые изменения в экспертное заключение и информирует о них по электронной почте ответственного за выполнение запланированных работ и заместителя заведующего.

5.2. После реализации запланированных работ ответственное лицо должно направить по электронной почте ответственному за обеспечение безопасности конфиденциальной информации подтверждение выполнения работ, не позднее срока реализации, установленного в экспертном заключении.

5.3. Ответственный за обеспечение безопасности конфиденциальной информации вправе запросить у назначенного лица информацию о выполнении в случае, если ему не поступило подтверждение выполнения работ в течение 2 (Двух) рабочих дней с даты, установленной в экспертном заключении.

5.4. Оценку результативности предпринятых мер осуществляет ответственный за обеспечение безопасности конфиденциальной информации ежемесячно на основании

анализа информации, содержащейся в отчетах о проведении служебного расследования и в сводном отчете об инцидентах ИБ.

5.5. О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

6. Определение плана корректирующих и превентивных мероприятий

Ежемесячно администратор ИБ готовит сводный отчет по инцидентам ИБ, предоставляемый ответственному за обеспечение безопасности конфиденциальной информации Организации.

В сводном отчете администратор ИБ должен провести анализ выявленных инцидентов ИБ, в качестве приложения к отчету должен быть предложен перечень корректирующих и превентивных мероприятий, направленных на устранение причин и последствий инцидентов ИБ и на предотвращение подобных нарушений в будущем. Данный перечень должен устанавливать сроки реализации и ответственных за проведение указанных мероприятий.

После согласования указанного перечня с ответственным за обеспечение безопасности конфиденциальной информации, данная информация доводится администратором ИБ до всех работников, назначенных ответственными за проведение корректирующих и превентивных мероприятий.

Контроль за своевременным и качественным выполнением работ по проведению корректирующих и превентивных мероприятий осуществляет ответственный за обеспечение безопасности конфиденциальной информации.

6. . Ответственность

7.5. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный за обеспечение безопасности конфиденциальной информации.

7.6. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор ИБ, назначенный приказом по Организации.

7.7. Ответственность за выделение требуемых ресурсов (в том числе финансовых и трудовых) для реализации положений настоящего документа несет заместитель руководителя, ответственный за вопросы разработки, принятия и внедрения мер защиты информации (далее – заместитель руководителя).

Приложение №1
к Положению о порядке выявления и реагирования
на инциденты информационной безопасности

ПЕРЕЧЕНЬ
инцидентов информационной безопасности
Организации

№ п/п	Описание инцидента информационной безопасности
1	2
1. Текущие нарушения	
1.1.	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (однократная)
1.2.	Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам
1.3.	Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры Организации
1.4.	Выполнение производственных обязанностей с использованием компьютерного оборудования в нерабочее время
1.5.	Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
1.6.	Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания
1.7.	Нецелевое использование элементов информационной инфраструктуры Организации (печать, сервисы сети Интернет, электронная почта, и т.п.)
2. Значимые нарушения	
2.1.	Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная)
2.2.	Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время
2.3.	Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации
2.4.	Утрата носителя информации с резервной копией
2.5.	Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная)
2.6.	Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.)
2.7.	Нерегламентированная очистка журналов событий безопасности информационных систем Организации
2.8.	Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации
2.9.	Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования

№ п/п	Описание инцидента информационной безопасности
1	2
2.10.	Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет
2.11.	Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах Организации
2.12.	Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем Организации (повышение уровня прав доступа, получение прав на отладку программ и т.п.)
2.13.	Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное)
2.14.	Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения
2.15.	Нерегламентированное использование анализаторов протоколов (снифферов)
2.16.	Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите)
2.17.	Несанкционированное проведение обновления версий системного и прикладного программного обеспечения
3. Нарушения, имеющие признаки преступления	
3.1.	Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры Организации
3.2.	Несанкционированное изменение конфигурации элементов информационной инфраструктуры Организации
3.3.	Утрата резервных копий
3.4.	Утечка конфиденциальной информации (баз данных информационных систем и др.)
3.5.	Подозрение в умышленном нарушении работоспособности информационной сети Организации, элементов информационной инфраструктуры Организации, системного и прикладного программного обеспечения
3.6.	Юридически необоснованная передача (распространение) конфиденциальной информации
3.7.	Несанкционированное внесение изменений в базы данных информационных систем Организации
3.8.	Несанкционированное уничтожение конфиденциальной информации
3.9.	Проведение обновления версии информационных систем Организации (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации
3.10.	Намеренное заражение информационных систем Организации вредоносным кодом

УТВЕРЖДАЮ
Заведующий МАДОУ ДСКВ
«Рябинушка»
_____ Н.А. Паймухина
Приказ от «___»_____ 2017 №_____

Инструкция
пользователя информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) МАДОУ ДСКВ «Рябинушка» (далее – Организация).

1.2. Субъектами доступа к ресурсам ИСПДн являются администратор безопасности (далее – АБ), пользователи и обслуживающий персонал.

1.3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4. Машинные носители информации имеют пометку «ПДн».

1.5. Пользователи получают свои права на доступ к ресурсам ИСПДн через АБ.

1.6. Пользователи имеют право письменно вносить предложения по изменению и дополнению данной Инструкции.

1.7. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.8. Право толкования положений настоящей Инструкции возлагается на Руководителя Организации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Муниципальные информационные системы – информационные системы, созданные на основании решения органа местного самоуправления.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

Распространение персональных данных − действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление 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 и (или) в результате которых уничтожаются материальные носители персональных данных.

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 функциональному предназначению и техническим характеристикам.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

3. ОБЯЗАННОСТИ

Пользователь обязан:

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

3.2. Выполнять на АРМ только те процедуры, которые определены технологическим процессом обработки ПДн.

3.3. Знать и соблюдать установленные требования к обработке ПДн, учету и хранению носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

3.4. Соблюдать требования парольной политики в соответствии с «Инструкцией по организации парольной защиты».

3.5. Получить уникальное имя и персональный идентификатор (при его наличии) от АБ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.

3.6. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи на окнах должны быть закрыты.

3.7. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ ИСПДн провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

3.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

3.8.1. приостановить обработку данных;

3.8.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ ИСПДн, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

3.8.3. совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

3.8.4. произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ ИСПДн).

3.9. Немедленно вызывать АБ ИСПДн и поставить в известность руководителя структурного подразделения при обнаружении:

3.9.1. нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

3.9.2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

3.9.3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

3.9.4. некорректного функционирования установленных на АРМ технических средств защиты;

3.9.5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.10.При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБ.

3.11.Обо всех выявленных нарушениях, связанных с информационной безопасностью Организации, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.

3.12.При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

3.13.Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

3.14.Пользователям **запрещается**:

разглашать **защищаемую информацию** посторонним лицам;

копировать защищаемую информацию на неучтенные внешние носители;

самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;

подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПДн;

сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;

оставлять без присмотра и передавать другим лицам персональный идентификатор;

привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности ПДн;

оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

4. ПОРЯДОК РАБОТЫ ПОЛЬЗОВАТЕЛЯ С РЕСУРСАМИ ИСПДН

4.1. Начало работы на АРМ

При включении АРМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее – СЗИ) и операционной системы (далее – ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИСПДн пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБ.

4.2. Завершение работы на АРМ

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения АРМ), либо завершить работу АРМ стандартным способом (при этом выключить АРМ).

4.3. Требования к распечатыванию информации

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПДн, все документы, содержащие ПДн, должны быть недоступны для просмотра и иного их использования.

5. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям АБ или создаются самостоятельно.

5.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 12 месяцев.

5.3. Правила формирования пароля:

- пароль должен состоять не менее чем из 6 символов;
- в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);
- запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения пользователей ИСПДн и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.

5.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

5.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

5.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать АБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

6. ОТВЕТСТВЕННОСТЬ

6.1. Пользователь несет персональную ответственность за:

– сохранность носителей информации и содержащейся на них информации (в рабочее время);

– соблюдение требований данной Иинструкции, неправомерное использование ресурсов ИСПДн и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. За разглашение ПДн и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

УТВЕРЖДАЮ
Заведующий МАДОУ ДСКВ
«Рябинушка»
_____ Н.А. Паймухина
Приказ от «___»_____ 2017 №_____

Инструкция
по организации антивирусной защиты

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации, и определяет требования к организации защиты информационной системы персональных данных (далее – ИСПДн) МАДОУ ДСКВ «Рябинушка» (далее – Организация) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора безопасности (далее – АБ) и других должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИСПДн, за выполнение указанных требований.

1.2. К использованию в Организации допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

1.3. Установка средств антивирусного контроля на компьютеры и сервера ИСПДн Организации осуществляется АБ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты персональных данных

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Муниципальные информационные системы – информационные системы, созданные на основании решения органа местного самоуправления.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

Распространение персональных данных − действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление 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 и (или) в результате которых уничтожаются материальные носители персональных данных.

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 функциональному предназначению и техническим характеристикам.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

3. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

3.1. Антивирусный контроль должен осуществляться в режиме постоянной антивирусной защиты. Ежедневно в начале работы при загрузке компьютера (для

серверов – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль дисков и файлов АРМ.

3.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

3.3. Процедура обновления баз данных средства антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИСПДн, работающих в сети, не реже одного раза в неделю для всех АРМ ИСПДн, работающих автономно.

3.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено АБ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверах и АРМ ИСПДн.

3.5. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПДн Организации в соответствии с требованиями настоящей Инструкции возлагается на АБ и всех должностных лиц, настраивающих и сопровождающих средства антивирусной защиты в ИСПДн Организации.

4.2. Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а так же проверка работоспособности средств антивирусной защиты) в ИСПДн Организации, осуществляется АБ и всеми должностными лицами, настраивающими и сопровождающими средства антивирусной защиты в ИСПДн Организации.

УТВЕРЖДАЮ
Заведующий МАДОУ ДСКВ
«Рябинушка»
_____ Н.А. Паймухина
Приказ от «___»_____ 2017 №_____

Инструкция
администратора безопасности информационных
систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности (далее – АБ) в информационных системах персональных данных (далее – ИСПДн) МАДОУ ДСКВ «Рябинушка» (далее – Организация).

1.2. Субъектами доступа к ресурсам ИСПДн являются пользователи, АБ и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт), в соответствии с утвержденным перечнем.

1.3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные.

1.4. Машинные носители с защищаемой информацией имеют пометку «ПДн».

1.5. АБ назначается Приказом Руководителя и получает неограниченные права на доступ к ресурсам ИСПДн.

1.6. АБ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИСПДн и обслуживающего персонала.

1.7. Методическое руководство по информационной безопасности объектов информатизации осуществляет АБ.

1.8. АБ имеет право вносить предложения по изменению и дополнению данной Инструкции, а также «Инструкции пользователя…» и «Инструкции обслуживающего персонала…».

1.9. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.10. Право толкования положений настоящей Инструкции возлагается на Руководителя.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Муниципальные информационные системы – информационные системы, созданные на основании решения органа местного самоуправления.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

Распространение персональных данных − действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление 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 и (или) в результате которых уничтожаются материальные носители персональных данных.

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 функциональному предназначению и техническим характеристикам.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

3. ТРЕБОВАНИЯ К АБ

3.1. АБ обязан знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

3.2. АБ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПДн не допускается.

3.3. АБ осуществляет учет съемных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

3.4. АБ обязан немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее – ОТСС и ВТСС), СЗИ, системного и прикладного программного обеспечения (далее – ПО) ИСПДн.

3.5. АБ обязан немедленно ставить в известность ответственного за обеспечение безопасности персональных данных Организации обо всех неисправностях аппаратно-программных средств ИСПДн.

3.6. АБ обязан ставить в известность ответственного за обеспечение безопасности персональных данных Организации о необходимости проведения работ по администрированию СЗИ.

3.7. АБ имеет право проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

3.8. АБ разрабатывает планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ИСПДн Организации.

3.9. АБ обязан в случае отказа технических средств или программного обеспечения элементов ИСПДн, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.10. АБ имеет право требовать прекращения обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

3.11. АБ присутствует при выполнении технического обслуживания элементов ИСПДн сторонними специалистами на территории Организации.

3.12. АБ осуществляет разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.13. В ходе управления (администрирования) системой защиты ИСПДн АБ обязан осуществлять:

3.14. заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИСПДн и поддержание правил разграничения доступа в ИСПДн;

3.15. управление СЗИ в ИСПДн, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

3.16. изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИСПДн;

3.17. установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

3.18. централизованное управление системой защиты информации ИСПДн (при необходимости);

3.19. регистрацию и анализ событий в ИСПДн, связанных с защитой информации;

3.20. информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПДн и отдельных СЗИ, а также их обучение;

3.21. сопровождение функционирования системы защиты информации ИСПДн в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

3.22. В ходе выявления инцидентов и реагирования на них АБ обязан осуществлять:

3.23. обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.24. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДн;

3.25. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

3.26. планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.27. планирование и принятие мер по предотвращению повторного возникновения инцидентов.

3.28. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн, АБ обязан осуществлять:

3.29. анализ и оценку функционирования системы защиты информации ИСПДн, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИСПДн;

3.30. проверку работоспособности и параметров настройки программного обеспечения, аппаратных и программных СЗИ ИСПДн;

3.31. проверку состава технических средств, программного обеспечения и СЗИ;

3.32. контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных;

3.33. еженедельное отслеживание появления новых видов уязвимостей ПО ИСПДн. По необходимости АБ производит устранение уязвимостей согласно рекомендациям разработчика;

3.34. периодический анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

3.35. контроль за событиями безопасности и действиями пользователей в ИСПДн. В частности, АБ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;

3.36. контроль (анализ) защищенности информации, содержащейся в ИСПДн;

3.37. документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн;

3.38. принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИСПДн, повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

4. ДОСТУП К РЕСУРСАМ ИСПДн

4.1. Обязательными условиями получения доступа к ресурсам ИСПДн АБ являются:

- право доступа в помещение;
- наличие допуска к персональным данным;
- право доступа к ИСПДн;
- знание технологии обработки информации в ИСПДн с учетом требований информационной безопасности.

4.2. Идентификация АБ в ИСПДн осуществляется по уникальному имени и персональному идентификатору (при его наличии).

4.3. Длина пароля АБ и всех пользователей – не менее 6 буквенно-цифровых символов.

4.4. Уникальное имя, персональный идентификатор (при его наличии) и пароль АБ получает в установленном порядке. АБ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

4.5. При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

4.6. Регистрация пользователя осуществляется АБ в соответствии с «Инструкцией по организации парольной защиты» и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

4.7. При заведении новой учетной записи, АБ должен проверить личность пользователя и его должностные обязанности.

4.8. Предоставление пользователям прав доступа к объектам доступа ИСПДн должно осуществляться на основании задач, решаемых пользователями.

4.9. АБ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

4.10. АБ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

5. ПОРЯДОК РАБОТЫ АБ С РЕСУРСАМИ ИСПДН

Ниже приводится перечень работ, производимых АБ с ресурсами ИСПДн.

5.1. **Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн**

АБ присваивает пользователям идентификационные данные к ресурсам ИСПДн. При этом должны выполняться следующие требования:

- АБ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;
- АБ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;
- изменение учетных данных пользователя производится АБ по требованию ответственного за обеспечение безопасности персональных данных Организации, а также периодически по утвержденному плану и в случае увольнения работника;
- АБ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АБ обязан потребовать у пользователя изменение пароля.

5.2. **Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ)**

АБ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить.

В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБ обязан приостановить обработку защищаемой информации до устранения неисправности. В случае производственной необходимости – отключить СЗИ и лично контролировать проведение работ пользователями.

5.3. **Антивирусная защита ресурсов ИСПДн**

АБ разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры антивирусной программы;
- контролирует работоспособность антивирусной программы;
- немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;
- имеет право на проведение внеплановой проверки на наличие вирусов;
- периодически (один раз в неделю) контролирует корректность процесса обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

5.4. **Хранение дистрибутивов программного обеспечения СЗИ**

АБ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИСПДн Организации в месте, исключающем доступ посторонних лиц.

a. **Проверка целостности системного и прикладного ПО**

Контролю целостности подлежат файлы ПО ИСПДн с расширениями: *.exe, *.com, *.dll, *.sys, *.vxd,*.drv.

5.5. **Резервное копирование и восстановление информации**

Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

- обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых машинных носителей (далее – МН);
- допускается обоснованное внеплановое резервное копирование информации как по инициативе пользователя, так и АБ, если это не нарушает технологию обработки информации;
- резервные копии пользовательской информации и информации операционной системы хранятся на учтенных внешних МН;
- ответственным лицом за хранение резервных копий является АБ.

По мере устранения неисправностей ПЭВМ АБ производит восстановление информации ограниченного доступа с резервных копий.

АБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5.6. **Конфигурирование ИСПДн**

Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

Управление изменениями конфигурации осуществляет ответственный за обеспечение безопасности. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБ.

В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации АБ обязан осуществлять:

– поддержание конфигурации ИСПДн и ее системы защиты информации (структуры системы защиты информации ИСПДн, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПДн и ее системы защиты информации);

– управление изменениями базовой конфигурации ИСПДн и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПДн и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПДн и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДн и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

– определение параметров настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИСПДн и ее системы защиты информации в документацию на систему защиты информации ИСПДн;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБ. При возникновении необходимости изменения конфигурации ИСПДн, аттестованной по требованиям безопасности информации, АБ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

5.7. **Вывод ресурсов ИСПДн из эксплуатации**

При невозможности ремонта различных ресурсов ИСПДн АБ обязан:

- физически уничтожать любые МН, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИСПДн;

- факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ИСПДн.

5.8. **Реагирование на сбои при регистрации событий безопасности**

Реагирование на сбои при регистрации событий безопасности осуществляется АБ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности, АБ обязан:

- немедленно уведомить Руководителя о данном факте;
- по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;
- восстановить работоспособность ИСПДн;
- по окончании работ по восстановлению работоспособности ИСПДн произвести запись в соответствующих журналах.

6. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

6.1. К попыткам несанкционированного доступа относятся:

- сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;
- действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

6.2.При выявлении факта несанкционированного доступа АБ обязан:

- пресечь дальнейший несанкционированный доступ к ИСПДн;
- доложить ответственному за обеспечение безопасности персональных данных Организации служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
- известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

7. ОТВЕТСТВЕННОСТЬ

7.1. АБ несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации в рабочее время;
- несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИСПДн;
- СЗИ, применяемые в ИСПДн Организации;
- качество проводимых работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени учетной записи АБ в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

7.2. АБ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

УТВЕРЖДАЮ
Заведующий МАДОУ ДСКВ
«Рябинушка»
_____ Н.А. Паймухина

Приказ от «___»_____ 2017 №_____

Инструкция
по организации парольной защиты

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) МАДОУ ДСКВ «Рябинушка» (далее – Организация), а также контроль над действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Муниципальные информационные системы – информационные системы, созданные на основании решения органа местного самоуправления.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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 (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

Распространение персональных данных − действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление 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 и (или) в результате которых уничтожаются материальные носители персональных данных.

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 функциональному предназначению и техническим характеристикам.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

3. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

3.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной 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 и специальные символы (@, #, $, &, *, % и т.п.);

− пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

− при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

3.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

3.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн.

3.4. Для обеспечения возможности использования имен и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями работников должны храниться в опечатанном сейфе, к которому исключен доступ других работников Организации и посторонних лиц. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии), либо печать администратора безопасности ИСПДн. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в «Журнале учета паролей пользователей…».

4. ВВОД ПАРОЛЯ

4.1 При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.2 При неверном вводе пароля более 5 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

5. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

5.1. Смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев, самостоятельно каждым пользователем.

5.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

5.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, администратора безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5.4. Администратор безопасности ИСПДн ведет «Журнал учета паролей пользователей...», в котором он отмечает причины внеплановой смены паролей пользователей.

5.5. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

6. ХРАНЕНИЕ ПАРОЛЯ

6.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

6.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

6.3. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

7. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ

7.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

8. ОТВЕТСТВЕННОСТЬ

8.1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

8.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за обеспечение безопасности персональных данных.

8.3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.